



Faculty of Law,  
Economics  
and Finance

---

**Law Working Paper Series**  
Paper number 2019-015

# **The EU Response to Criminal Misuse of Cryptocurrencies**

The young, already outdated 5th  
Anti-Money Laundering Directive

Valentina Covolo  
valentina.covolo@uni.lu

13/12/2019

# The EU Response to Criminal Misuse of Cryptocurrencies: The young, already outdated 5<sup>th</sup> Anti-Money Laundering Directive<sup>1</sup>

---

*Dr. Valentina Covolo  
Post-doctoral researcher  
University of Luxembourg*

## **Abstract**

*Combating criminal misuse of cryptocurrencies was at the core of the FATF agenda under the US Presidency, culminating in June 2019 with the thorough extension of international standards against money laundering over virtual assets' markets. This echoed the first legislative measure regulating virtual currencies adopted by the EU a year before. Directive 2018/843, better known as the 5<sup>th</sup> Anti-Money Laundering Directive, fails however to address key technological breakthroughs and new business models, which continuously make the ever-growing and fast-paced crypto economy evolve. Against this background, the present contribution investigates shortfalls and challenges that lay ahead in the light of the new FATF Recommendations. It ultimately argues that the preventive anti-money laundering measures cannot dispense with the establishment of a cross-border integrated supervisory and enforcement system.*

**Key words:** *Cryptocurrencies – Virtual Assets – Blockchain - Money laundering – AML Directives – FATF – Cybercrime*

## **TABLE OF CONTENTS**

I. Introduction.....	2
II. ‘Cryptocrimes’, a spreading phenomena .....	4
A. Understanding a disruptive technology .....	4
B. Mapping the dark side of the crypto-economy.....	6
III. The EU policy choice: when crime prevention and detection takes precedence over harmonized regulation.....	7
IV. Defining the new object of AML regulations: a legal conundrum .....	9
A. Virtual currencies, fiat and electronic money.....	9
B. Virtual currencies, digital tokens and virtual assets .....	11
V. Identifying obliged entities: transposing or reshaping the AML enforcement architecture? .....	13

---

<sup>1</sup> The present paper presents the findings of the CRYPTOCRIME study (Cryptocurrencies and Crime: Regulatory Needs and Enforcement Strategies’) led by Prof. Silvia Allegranza and supported by the Luxembourg National Research Fund (Project No O17/11757193). The author warmly thanks Prof. Silvia Allegranza and Dr. Sofia Mirandola for the invaluable support and feedbacks.

A.	Targeting the gatekeepers: exchanges and custodial wallet providers .....	13
B.	Users and minors, the excluded market players .....	16
C.	Further inclusion of virtual assets service providers .....	17
VI.	Implementing customer due diligence: collection, decryption and analysis of transactions data .....	18
A.	From ‘pseudonymity’ to privacy coins.....	18
B.	Mixers, tumbler and other anonymity-enhancing tools.....	20
C.	Expertise and analysis software.....	21
VII.	Conclusive remarks.....	23

## I. Introduction

*‘Virtual assets and related financial services have the potential to spur financial innovation and efficiency and improve financial inclusion, but they also create new opportunities for criminals and terrorists to launder their proceeds or finance their illicit activities’.*<sup>2</sup> Drawing on this, the Financial Action Task Force (FATF) published in October 2018 the last amendments to its recommendations,<sup>3</sup> with the aim to tackle a spreading phenomenon that is nowadays among its policy priorities: fighting against the use of cryptocurrencies for criminal purposes.<sup>4</sup> The new international standards thus echoed the legislative reform that a few month earlier modified the EU legal framework for combatting money laundering and terrorist financing (AML/CFT). The Directive 2018/843/EU, better-known as the 5<sup>th</sup> Anti-Money Laundering Directive (AML Directive), brings providers engaged in exchange services between virtual currencies and fiat currencies, as well as custodian wallet providers, under its scope of application, thereby imposing on them due diligence rules and reporting duties.<sup>5</sup> By doing so, the 5<sup>th</sup> AML Directive that the Member States will have to transpose into national law by January 2020 is the first EU legal instrument regulating a market, which generates as much enthusiasm among investors as it raises concerns among regulators and supervisory authorities.<sup>6</sup>

<sup>2</sup> FATF, ‘Regulation of Virtual Assets’, Paris, 19 October 2018, <<http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html>>.

<sup>3</sup> FATF (2012-2019), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France, <[www.fatf-gafi.org/recommendations.html](http://www.fatf-gafi.org/recommendations.html)>, hereinafter FATF Recommendations (updated June 2019).

<sup>4</sup> In response to the concerns expressed by the G20 in July 2018, the FATF prioritized the improvement in the regulation and supervision of virtual currencies and crypto-assets in the view of adapting its recommendations to the growing use of this new technology for money laundering and terrorism financing. See FATF Report to G20 Finance Ministers and Central Bank Governors (July 2018), Paris, France <[www.fatf-gafi.org/publications/fatfgeneral/documents/report-g20-fm-cbg-july-2018.html](http://www.fatf-gafi.org/publications/fatfgeneral/documents/report-g20-fm-cbg-july-2018.html)>.

<sup>5</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 [2018] OJ L 156/43.

<sup>6</sup> See, for instance, European Security and Markets Authority, European Banking Authority and European Insurance and Occupational Pension Authority, Joint Warning, ‘ESMA, EBA and EIOPA warn consumers on the

Bitcoin, the first and still most popular cryptocurrency, was designed in 2008 by a mysterious programmer under the pseudonym of Satoshi Nakamoto.<sup>7</sup> On January 3<sup>rd</sup> 2009, he unleashed the very first coin and marked the birth of a revolutionary peer-to-peer electronic cash system, with the ambition to create an alternative mean of payment in the wake of a growing distrust against banking institutions after the financial crisis.<sup>8</sup> Since then, the number of users, developers and investors skyrocketed, creating in just over a decade a market of more than 3000 different cryptocurrencies for a total market capitalization exceeding 223 billion US Dollars.<sup>9</sup> Two problematic aspects still tarnish, however, their popularity. On the one hand, public institutions worldwide constantly alert the users about the high volatility risks that expose them to significant and sudden losses.<sup>10</sup> Whilst the spectacular increase in the value of Bitcoins in 2017 highlighted its smashing speculative potential, the subsequent sharp drop of prices added another crash in the short history of cryptocurrencies markets.<sup>11</sup>

On the other hand, an increasing number of high profile cases draws attention to the criminogenic potential of cryptocurrencies. Lack of regulation and supervision, anonymity, global online access and non-face-to-face transactions make cryptocurrencies a new attractive tool that facilitates the perpetration of a wide range of criminal offences.<sup>12</sup> Drug trafficking via virtual market places such as Alphabay<sup>13</sup>, money laundering charges against the founder of Liberty Reserve,<sup>14</sup> scams on exchange platforms, such as for instance Mt.Gox, Coin.mx and Coincheck,<sup>15</sup> ransoms using cryptocurrencies such as Wannacry<sup>16</sup> or the Avalanche

---

risks of Virtual Currencies’, 12 February 2018  
<<https://www.eba.europa.eu/documents/10180/2139750/Joint+ESAs+Warning+on+Virtual+Currencies.pdf>>.

<sup>7</sup> S. Nakamoto, ‘Bitcoin: A Peer-to-Peer Electronic Cash System’ (2008) <<https://bitcoin.org/en/bitcoin-paper>>.

<sup>8</sup> *Ibid.*, p. 1.

<sup>9</sup> Figures reported by CoinMarketCap on October 21<sup>st</sup> 2019. An updated market analysis is available at <<https://coinmarketcap.com>>.

<sup>10</sup> See *inter alia* ESMA, EBA and EIOP, Joint Warning, *loc. cit.*; IMF Staff Discussion Note, ‘Virtual Currencies and Beyond : Initial Considerations’ (January 2016) SDN/16/03, pp. 31 ff; ECB, Report ‘Virtual currency Schemes – a further analysis’ (February 2015), p. 23, <<https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>>; EBA, Opinion on virtual currencies (4 July 2014), EBA/OP/2014/08, pp. 23 ff; A Blundell-Wignall, ‘The Bitcoin Question: Currency versus Trust-less Transfer Technology’ (2014) OECD Working Papers on Finance, Insurance and Private Pensions No. 37, <<http://dx.doi.org/10.1787/5jz2pwjd9t20-en>>, p. 11; ECB, Report ‘Virtual Currency Schemes’ (October 2012), p. 39, <<https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>>.

<sup>11</sup> ECB, ‘Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures’, Occasional Paper Series No 223 (May 2019) pp. 11 ff.

<sup>12</sup> Europol, ‘Internet Organised Crime Threat Assessment 2018’, <<https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018>>, p. 8. Hereinafter IOCTA 2018.

<sup>13</sup> Europol Press Release, *Massive blow to criminal dark web activities after globally coordinated operation*, 20 juillet 2017 [<https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation>].

<sup>14</sup> R Girasa, Regulation of Cryptocurrencies and Blockchain Technologies, National and International Perspectives (Palgrave MacMillan, 2018), 145

<sup>15</sup> Besides cybersecurity risks, the MtGox case casted light on deceptions and dishonest practices on the part of exchange platforms. See P. de Filippi, ‘Bitcoin: A Regulatory Nightmare to a Libertarian Dream’, 3(2) Internet Policy Review, pp. 8-9.

<sup>16</sup> Europol, ‘Internet Organised Crime Threat Assessment 2017’, <<https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017>>, pp. 19 ff.

network,<sup>17</sup> ICO's token fraud<sup>18</sup> and cryptojacking<sup>19</sup> are among the criminal cases reported by the newspapers around the world.

Against this background, policy-makers increasingly advocate the need for a regulatory framework capable to effectively prevent and sanction criminal misuse of cryptocurrencies, without however stifling technological developments and the undeniable beneficial growth of digital economy.<sup>20</sup> By adopting the 5<sup>th</sup> AML Directive, the EU intended precisely to move forward along this path.<sup>21</sup> At the time of implementation, however, the newly adopted measures are already lagging behind with respect to the fast technological and structural developments of the crypto-assets market. This is even more striking when considering the recent extension of the AML international standards resulting from an intense and productive work of the FATF under the US Presidency. In particular, the interpretative note to Recommendation 15<sup>22</sup> and the Guidance on Virtual Assets and Virtual Assets Service Providers published in June 2019<sup>23</sup> help identifying gaps and challenges that the implementation of the 5<sup>th</sup> AML Directive raises in this field. To do so, one should first understand what cryptocurrencies are and how this technology may be used for the perpetration of criminal offences.

## II. 'Cryptocrimes', a spreading phenomena

### A. Understanding a disruptive technology

The creation of Bitcoin was the first step of what is today largely recognized as the most disruptive technology in decades.<sup>24</sup> Its innovative character lies above all in the decentralized and trustless network on which the whole transaction system is based. Unlike traditional payment methods, cryptocurrencies do not resort to trusted intermediaries, such as banks or credit card companies, which maintain a central record of the transactions. On the contrary, copies of the transactions records are kept in multiple devices (also called 'nodes') throughout

---

<sup>17</sup> Europol Press Release, 'Avalanche network dismantled in international cyber operation', 1 December 2016, <<https://www.europol.europa.eu/newsroom/news/%E2%80%99avalanche%E2%80%99-network-dismantled-in-international-cyber-operation>>.

<sup>18</sup> D. Zetzsche et al., 'The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators', 63 Harvard International Law Journal (2019) forthcoming.

<sup>19</sup> C. Cornish, H. Kuchler, 'Cryptojackers steal computer power to mine digital coins', Financial Times (8 April 2018).

<sup>20</sup> See in particular European Parliament, Committee on Economic and Monetary Affairs, Report on virtual currencies (May 2016), PE575.277v02-00.

<sup>21</sup> Proposal for a Directive of the European Parliament and the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC, COM(2016) 450 final, p. 11.

<sup>22</sup> FATF (2019), Interpretative Note to Recommendation 15, in FATF Recommendations, p. 70. Hereinafter FATF, Interpretative Note to Recommendation 15.

<sup>23</sup> FATF, Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (2019), FATF, Paris, <<https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf>>. Hereinafter FATF, Guidance on Virtual Assets and Virtual Assets Service Providers.

<sup>24</sup> Whilst the sustainability of cryptocurrencies schemes as a large-scale accepted payment system still raise doubts, the underlying blockchain technology is seen to have revolutionary potential applications both in the public and private spheres. See M.C. Weldon, R. Epstein, 'Beyond Bitcoin: Leveraging Blockchain to Benefit Business and Society', 20 Transactions: The Tennessee Journal of Business Law, pp. 837 – 909.

the network, which form an openly maintained distributed ledger.<sup>25</sup> Trust in third parties to the transaction is no longer needed, but replaced by consensus protocols, such as ‘proof-of-work’ or ‘proof-of stake’.<sup>26</sup> These algorithms guarantee the reliability of the system, by achieving consensus across members of the network on the validity of the ledger.<sup>27</sup> As a result of this disintermediation process, users do not need to trust governments and institutions anymore, which traditionally guarantee the stability and proper functioning of the monetary system.<sup>28</sup> Thanks to the distributed ledger technology (DLT), cryptocurrencies schemes make the promise of a secure and self-sustained payment system, where transactions are irreversible and records immutable.<sup>29</sup>

More specifically, every user holds two cryptographic keys.<sup>30</sup> The public key may be assimilated to a bank account, a destination address known to everyone on the network where the assets are sent. The private key works as a digital signature required to validate the transaction.<sup>31</sup> Once the signed transaction is sent to the network, the system generates ‘cryptographic puzzles’, namely complex mathematical calculations that must be solved in order to validate and secure the transaction. As a result of this process called ‘mining’ or ‘forging’, key accounts, time and amounts of the transaction are recorded in this chain of blocks.<sup>32</sup> It is precisely the well-known blockchain that ensures the transactions’ security and prevents double-spending, i.e. that asset is transferred more than once without central controlling.<sup>33</sup> A smartphone with an internet connection is sufficient to access the network. The user can then easily buy Bitcoins with Euros on an online exchange platform and, to further facilitate the transactions, he can hold, store and transfer coins in a digital wallet.

This short overview is undoubtedly not sufficient to reflect the ever-growing complexity of the cryptocurrencies ecosystem. Whilst tech solutions seek to improve the privacy, speed and scalability of cryptocurrencies’ transactions, the blockchain wave gave rise to myriads of different crypto-assets that regulators still struggle to classify.<sup>34</sup> The physiological slowness of the law-making process preserved until now the crypto-economy from a consistent regulation and coordinated supervision both at the European and international level.<sup>35</sup> The resulting legal

---

<sup>25</sup> IMF, Staff Discussion Note ‘Virtual Currencies and Beyond : Initial Considerations’, January 2016, SDN/16/03, pp. 19 ff.

<sup>26</sup> R. Houben, A. Snyers, ‘Cryptocurrencies and blockchain. Legal context and implications for financial crime, money laundering and tax evasion’, Study requested by the TAX3 Committee, PE 619.024, July 2018, pp. 18 – 19.

<sup>27</sup> P. De Filippi, A. Wright, *Blockchain and the Law. The Rule of Code* (Harvard University Press, 2018) p. 24.

<sup>28</sup> On the libertarian roots of Bitcoin, Y. Zhang, ‘The Incompatibility of Bitcoin’s Strong Decentralization Ideology and Its Growth as a Scalable Currency’, 11 NYU JL & Liberty (2017) p. 556.

<sup>29</sup> P. De Filippi, B. Loveluck, ‘The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure’, 5(3) Internet Policy Review, p. 5.

<sup>30</sup> Every cryptocurrency presents its own technical features. For the sake of clarity, the following observations sketch out common basic characteristics that take as a reference the functioning of Bitcoin.

<sup>31</sup> R. Houben, A. Snyers, *loc. cit.*, pp. 16 – 17.

<sup>32</sup> *Ibid.*, pp. 18 – 19.

<sup>33</sup> ECB, Report ‘Virtual Currency Schemes’ (October 2012), *loc. cit.*, pp. 23 – 24.

<sup>34</sup> ECB, ‘Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures’ (May 2019) pp. 7 ff.

<sup>35</sup> This holds true for cryptocurrencies, as well as with regard to the regulatory status of crypto-assets. See respectively S. Fiedler et al., ‘Virtual Currencies, Monetary Dialogue July 2018, Report to the Committee of Economic and Monetary Affairs of the European Parliament’, PE 619.016, p. 17; ECB, ‘Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures’, *loc. cit.*, p. 7.

loopholes - compounded by the borderless nature of the Internet - did certainly contribute to the criminogenic attractiveness of cryptocurrencies.<sup>36</sup>

## B. Mapping the dark side of the crypto-economy

How bad is Bitcoin? According to empirical studies, the estimated rate of Bitcoin transactions linked to illicit activities ranges between 1%<sup>37</sup> and 46%.<sup>38</sup> Despite the uncertainties surrounding the dark figure of 'crypto-crimes', law enforcement agencies identified two clear trends: an increasing number of criminal cases involving cryptocurrencies and a shift by criminals towards currencies that guarantee stronger anonymity.<sup>39</sup> As for the typology of crimes, one may distinguish three main categories.

Firstly, cryptocurrencies are the target of criminal offences.<sup>40</sup> This first scenario encompasses cybercrimes in a narrower sense: crimes which require high technical expertise and raise cybersecurity issues.<sup>41</sup> Telling examples are the numerous cases of hacking, theft and embezzlement against cryptocurrencies exchanges, ransomware attacks and more recently cryptojacking. Secondly, cryptocurrencies become the object of criminal offences that aim to sanction infringements to existing regulations, such as unlicensed or illicit conduct of regulated activities, price manipulation and tax evasion. This second category typically involves cases in which the lack and confused regulatory provisions urged public authorities to clarify if and what law applies in order to determine whether non-compliance with that legal provisions is criminally sanctioned.<sup>42</sup> Thirdly, cryptocurrencies are also used instead of fiat or electronic money as a mean to perpetrate 'traditional crimes'. Indeed, the lack of monitoring and the greater anonymity characterizing the cryptocurrencies' market facilitates the perpetration of criminal offences,<sup>43</sup> in particular where payment, transfer, concealment of funds are among

---

<sup>36</sup> On the criminogenic features of virtual currencies and other online payment systems, T. Tropina, 'Fighting money laundering in the age of online banking, virtual currencies and internet gambling', 15 ERA Forum (2014), p. 72.

<sup>37</sup> S. Foley, J.R. Karlsen, T.J. Putniņš, 'Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?', 32 The Review of Financial Studies (May 2019), p. 1798.

<sup>38</sup> Chainalysis, Crypto Crime Report 'Decoding increasingly sophisticated hacks, darknet markets, and scams' (January 2019), <[https://uploads-ssl.webflow.com/5a9360f88433cb00018022c2/5c4f67ee7deb5948e2941fda\\_Chainalysis%20January%202019%20Crypto%20Crime%20Report.pdf](https://uploads-ssl.webflow.com/5a9360f88433cb00018022c2/5c4f67ee7deb5948e2941fda_Chainalysis%20January%202019%20Crypto%20Crime%20Report.pdf)>.

<sup>39</sup> Europol, IOCTA 2018, *loc. cit.*, p. 58.

<sup>40</sup> *Ibid.*, 7.

<sup>41</sup> On the definition of cybercrime in its narrow and broader sense, M. Chawki et al., *Cybercrime, Digital Forensic and Jurisdiction* (Springer, 2015), p. 6.

<sup>42</sup> For instance, in September 2018 a German criminal court dismissed the charges against a person accused of trading Bitcoins without a license because, contrary to the extensive interpretation of the BaFin, Bitcoins are not a unit of account and thus a financial instrument. See Kammergericht Berlin, Urteil v. 25.09.2018 - Az.: (4) 161 Ss 28/18 (35/18). Another example can be found in the Espinoza case, where the uncertainty as for the legal classification of Bitcoins lead a Circuit Court in Florida to dismiss money laundering charges. See B.M. Peck, 'The Value of Cryptocurrencies: How Bitcoin Fares in the Pockets of Federal and State Courts', 26 U. Miami Bus. L. Rev. (2017), p. 191.

<sup>43</sup> Some scholars pointed out that the over-regulation of the banking sector pushed criminals to look for new ways and tools for the laundering of their illicit proceeds. See B. Under, J. den Hertog, 'Water always finds its way: Identifying new forés of money laundering', 57 Crime Law Soc. Change (2012), pp. 287 – 304.

their constituent elements.<sup>44</sup> An illustration thereof are illegal trafficking notably via virtual market places, money laundering and terrorism financing.<sup>45</sup>

Despite the heterogeneity of the above-mentioned crimes, the EU chose as a first measure to extend the scope of AML/CTF regulations in order to include cryptocurrencies' transactions. The explanation is to be found in the 'follow the money' strategy that supported from the very beginning the criminalization of money laundering: by depriving criminals of the economic profits of their illicit activities, AML regulation incidentally tackle a wide range of predicate offences.<sup>46</sup> From this perspective, the 5<sup>th</sup> AML Directive does not solely target suspicious cryptocurrencies transactions that are likely to be part of a laundering or terrorism financing scheme. The resulting monitoring and reporting duties also help in detecting other forms of criminal activities, which take advantage of the cryptocurrencies ecosystem.

### **III. The EU policy choice: when crime prevention and detection takes precedence over harmonized regulation**

The implementation of the AML/CTF rules in the field of cryptocurrencies is not a novelty, however, for law enforcement authorities nor for the judiciary. Certain Member States have already taken some steps in order to clarify whether and to what extent entities operating on the cryptocurrencies market are subject to AML obligations. Some national legislatures had already included a reference to virtual currencies into the existing anti-money laundering legal instruments, such as for instance Italy.<sup>47</sup> Others extended the scope of AML/CTF regulation as part of transversal legal acts recently enacted with the aim to regulate the young crypto-economy, like the well-known Virtual Assets Financial Act in Malta.<sup>48</sup> A third group of countries adopted a case-by-case approach by imposing Know-your-customer (KYC) and due diligence requirements, reporting and cooperation duties as a direct consequence of licenses granted to companies engaged in a cryptocurrency business. An illustration thereof is Luxembourg, whose financial regulator was the first EU authority that in 2014 granted the status of payment service provider to an exchange platform.<sup>49</sup>

---

<sup>44</sup> This is all the more true where the transfer is part of a transnational illicit activity. For a criminological analysis of this aspect see C. Durrant, 'Understanding the Nexus between Cryptocurrencies and Transnational Crime Operations', CUNY Academic Works (2018), <[https://academicworks.cuny.edu/jj\\_etds/70](https://academicworks.cuny.edu/jj_etds/70)>.

<sup>45</sup> International organizations and scholars reported several case studies illustrating the way cryptocurrencies are used for the purpose of money laundering and terrorism financing. See notably FATF Report, 'Professional Money Laundering (July 2018)', <<https://www.fatf-gafi.org/publications/methodsandtrends/documents/professional-money-laundering.html>>, p. 25 and 46; FATF Report, 'Emerging Terrorist Financing Risks' (October 2015), <<https://www.fatf-gafi.org/documents/documents/emerging-terrorist-financing-risks.html>>, p. 35; D. Connel, 'Do EU Regulations Combating Money Laundering and the Financing of Terrorism adequately tackle Cryptocurrencies? The case of Ireland', 21 Irish Journal of European Law, pp. 74 ff.

<sup>46</sup> P. Alldrige, *What Went Wrong With Money Laundering Law?* (Palgrave Macmillan, 2016) p. 34.

<sup>47</sup> Legislative Decree No. 90 of 25 May 2017, OJ No 140, 19 June 2017.

<sup>48</sup> In 2018, Malta adopted comprehensive legal frameworks aimed to regulate the emerging blockchain economy. As for the consequent extension of AML rules, see Art. 57 (3) of the Virtual Financial Assets Act and Art. 8 (4) d, ii) of the Innovative Technology Arrangement and Services Act (ITAS).

<sup>49</sup> The Luxembourg financial supervisor (Commission de surveillance du secteur financier, CSSF) verifies whether the virtual assets service providers undertakes an activity that falls within the scope of the 2009 law transposing the PSD2 or whether the virtual assets qualifies as a financial instrument under the 1993 law on the financial sector. If so and only in that case, that regulated entity automatically becomes an obliged entity subject to the Luxembourg AML law. After Bitstamp, a second exchange platform, Bitflyer, was granted a license by the CSSF, which confirmed its case-by-case approach in March 2018. See CSSF, 'Avertissement sur les monnaies virtuelles', 14



Having regard to the different policy options adopted by the Member States, the question arose of whether the EU should have regulated first the virtual assets' market.<sup>50</sup> Notably, by extending the scope of application of the 2<sup>nd</sup> Payment Service Directive (PSD2),<sup>51</sup> the EU legislature could have both enhanced consumer protection under a harmonized legal framework and automatically imposed on the newly regulated entities obligations and duties stemming from the AML/CTF Directives.<sup>52</sup> Despite repeated calls by EU regulators, the decision-makers refused - at least in a first stage - to take this path.<sup>53</sup> The Commission clearly pointed out that such a policy option could not have reached a consensus among the Member States, which feared that a regulatory act 'would give too much legitimacy to VCs [virtual currencies] and drive consumers to believe VCs are safe and sound products in contrast to the list of risks' pointed out by the banking and financial regulators across the EU.<sup>54</sup>

Although regulation of crypto-assets still is a key issue of the European Fintech Action Plan,<sup>55</sup> the EU preferred, as a first step, to focus on criminal misuses of cryptocurrencies<sup>56</sup> without however undermining the competitiveness of the European economy.<sup>57</sup> As a result, less than eight months after the reform which led to the adoption of the 4<sup>th</sup> Anti-Money Laundering Directive (4<sup>th</sup> AML Directive),<sup>58</sup> the Commission decided to re-open the text for amendments. The proposal presented in July 2016 intended to implement *inter alia* the Guidance for a risk-based approach in the field of virtual currencies published in June 2015 by the FATF.<sup>59</sup> Few months later, the terrorist attacks in Paris and Brussels urged the Parliament and the Council to step up the legislative process and to adopt, after the first reading, Directive 2018/843/EU.<sup>60</sup>

It is worth emphasizing that the 5<sup>th</sup> AML Directive did not need to amend the definition of money laundering provided under Article 1(3) Directive 2015/849/EU in order to include

---

March 2018; CSSF, 'Avertissement sur les Initial Coin Offerings (ICOs)', 14 March 2018. Both documents are available at <<https://www.cssf.lu/consommateur/avertissements/news-cat/90/>>.

<sup>50</sup> This was notably suggested by EBA, Opinion on 'virtual currencies', EBA/Op/2014/08, 4 July 2014.

<sup>51</sup> Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, OJ [2015] L 337/3.

<sup>52</sup> Among the policy options considered by the Commission was the possibility to bring exchange platforms and custodian wallet providers under the scope of the 2PSD. See Commission Staff Working Document, Impact Assessment Accompanying the document Proposal for a Directive of the European Parliament and the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC, SWD (2016) 223 final, pp. 30 and 51.

<sup>53</sup> On the political context that led the Commission to present the proposal for a 5th AML Directive, N Vandezande, 'Virtual currencies under EU anti-money laundering law', 33 Computer Law and Security Review (2017), p. 344.

<sup>54</sup> SWD (2016) 223 final, p. 31.

<sup>55</sup> Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions, Fintech Action plan: For a more competitive and innovative European financial sector, COM (2018) 109 final.

<sup>56</sup> Besides the 5<sup>th</sup> AML Directive, the EU also included virtual currencies within the scope of Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA, OJ [2019] L 123/18.

<sup>57</sup> COM(2016) 450 final, p. 11.

<sup>58</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, OJ [2015] L 141/73, hereinafter 4<sup>th</sup> AMLD.

<sup>59</sup> FATF, Guidance for a risk-based Approach on Virtual Currencies (June 2015), FATF, Paris, <<https://www.fatf-gafi.org/documents/documents/guidance-rba-virtual-currencies.html>>.

<sup>60</sup> SWD (2016) 223 final, p. 7

transactions in cryptocurrencies aimed at concealing the illicit origin of proceeds of crimes.<sup>61</sup> In a similar way, the offence defined in the 6<sup>th</sup> AML Directive criminalizes such acts, since it broadly refers to ‘property’, a term that includes ‘assets of any kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such assets’.<sup>62</sup> Likewise, virtual currencies also fall within the definition of funds, referred to in the constituent elements of terrorism financing.<sup>63</sup> In this regard, EU law is clearly in line with the FATF Recommendations.<sup>64</sup>

The challenges that the implementation of the AML rules raise in the crypto-assets market do not relate so much to substantive criminal law. They primarily concern the enforcement of those measures that were designed to prevent and detect money laundering within the traditional banking and financial circuits. Among the goals of the 5<sup>th</sup> AML Directive is precisely the extension of the AML/CTF enforcement system to cryptocurrencies schemes, which unlike banking and financial institutions remain – at the time of writing - mostly unregulated and thereby exempted from any monitoring or supervisory activity by States’ authorities. Hence, in order to impose due diligence rules and reporting duties on entities operating on this new market, the 5<sup>th</sup> AML Directive provides the first harmonized legal definition of virtual currencies.

#### **IV. Defining the new object of AML regulations: a legal conundrum**

##### **A. Virtual currencies, fiat and electronic money**

Over the last years, international organizations and most particularly standard-setting bodies endeavored to identify the distinguishing features of cryptocurrencies. Rather than establishing common legal definitions, this led first to a classification exercise, where the terminology used varies depending on the time, the author and the context in which they are used. The various reports and opinions published by international and European bodies refer indeed to different but overlapping terms, ranging from digital tokens,<sup>65</sup> through cryptocurrencies<sup>66</sup> to crypto-assets,<sup>67</sup> from virtual assets<sup>68</sup> to virtual currencies.<sup>69</sup> The 5<sup>th</sup> AML

---

<sup>61</sup> R. Houben, A. Snyers, *loc. cit.*, p. 62.

<sup>62</sup> Art 2(2) Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law, OJ [2018] L 284/22.

<sup>63</sup> Art 1(5) Directive 2015/849/EU.

<sup>64</sup> FATF, Interpretative Note to Recommendation 15, pt. 1.

<sup>65</sup> ESMA, Advice on Initial Coin Offering and Crypto Assets (January 2019), ESMA50-157-1391.

<sup>66</sup> FATF, ‘Virtual Currencies, Key Definitions and Potential AML/CFT Risks’ (June 2014), < <https://www.fatf-gafi.org/documents/documents/virtual-currency-definitions-aml-cft-risk.html>>.

<sup>67</sup> Financial Stability Board Report, Crypto-asset markets Potential channels for future financial stability implications (10 October 2018); EBA, Report with Advice for the European Commission on Opinion on Crypto-assets (January 2019); ESMA, Advice on Initial Coin Offering and Crypto Assets (January 2019).

<sup>68</sup> FATF Recommendations.

<sup>69</sup> ECB, Virtual currency schemes (October 2012); EBA, Opinion on Virtual Currencies (July 2014); ECB, Virtual currency schemes – a further analysis (February 2015); IMF Staff Discussion Note, SDN/16/03 (January 2016); ESMA, EBA, EIOPA, Joint Warning on the Risks of Virtual Currencies (February 2018).

Directive uses the latter term while adopting the first harmonized legal definition of virtual currencies<sup>70</sup> that draws heavily on the one elaborated by the EBA in its 2014 Opinion.<sup>71</sup>

Both texts provide first negative definitional elements that evoke the distinction between virtual currencies and other means of payment on the regulated markets. Indeed, pursuant Article 3 (18) Directive 2015/849/EU, a virtual currency is ‘*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*’. Thus, unlike fiat currencies, virtual currencies are not issued by central banks or public authorities. They might be controlled by a single private administrator (centralized virtual currencies) or generated and distributed through math-based peer-to-peer systems without centralized oversight (decentralized virtual currencies, such as crypto-currencies).<sup>72</sup> In addition, virtual currencies do not have – in principle - legal tender status in any jurisdiction.<sup>73</sup> Indeed, natural and legal persons are not under the obligation to accept virtual currencies for all kind of payments. They are only used on a voluntary basis within a given online community.<sup>74</sup> Thus, acceptance of virtual currencies varies from one scheme to another<sup>75</sup> and ultimately depends on the market participants.<sup>76</sup>

Most importantly, the 5<sup>th</sup> AML Directive clarifies the distinction between virtual currencies and electronic money.<sup>77</sup> Considering that both are not physically represented through banknotes and coins but hold a digital form,<sup>78</sup> some doubts were raised as to whether certain virtual currencies, in particular Bitcoins, fall under the legal definition of e-money.<sup>79</sup> According to Directive 2009/110/EC, electronic money consists in an ‘*electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions (...) and which is accepted by a natural or legal person other than the electronic money issuer*’.<sup>80</sup> Hence, e-money is a digital equivalence of fiat currency (Euro, US dollars) and must be redeemed at par value.<sup>81</sup> For instance, a customer may purchase an electronic purse (smart card), which represents a claim on the issuer and can exchange such claim for goods and services with the seller who accepts it as payment. Thus, the electronic money issued corresponds with an amount ‘*not less in value than the monetary value issued*’.<sup>82</sup> Exception made for certain stablecoins<sup>83</sup> that some national

---

<sup>70</sup> Art 3 (18) Directive 2015/849/EU.

<sup>71</sup> EBA Opinion on virtual currencies (4 July 2014), EBA/OP/2014/08.

<sup>72</sup> FATF Report, ‘Virtual currencies. Key Definitions and Potential AML/CFT Risks’ (June 2014), p. 5.

<sup>73</sup> ECB Report, Virtual currency Schemes – a further analysis (February 2015), p. 24.

<sup>74</sup> *Ibid*, p. 25.

<sup>75</sup> EBA, Opinion on virtual currencies (July 2014), p. 12.

<sup>76</sup> For instance, the risks related to virtual currencies led some organizations and economic actors to decide not to accept donations and payments in Bitcoins. ECB Report, Virtual currency Schemes (October 2012) p. 25.

<sup>77</sup> Recital 10 Directive 2018/843/EU emphasizes the importance of such distinction.

<sup>78</sup> EBA, Opinion on virtual currencies (July 2014), p. 11.

<sup>79</sup> ECB Report, Virtual currency Schemes (October 2012), p. 43.

<sup>80</sup> Article 2(2) Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC, OJ [2009] L 267/7. Hereinafter Directive 2009/110/EC on Electronic Money.

<sup>81</sup> Art. 11 Directive 2009/110/EC on Electronic Money.

<sup>82</sup> ECB Report, Virtual currency Schemes (October 2012), p. 43.

<sup>83</sup> In order to counter the volatility characterizing cryptocurrencies, stablecoins such as Tether or Libra ‘rely on a set of stabilisation tools which are supposed to minimise fluctuations of their price in such currency(ies)’. For a

regulators qualified as e-money,<sup>84</sup> as virtual currencies is not necessarily pegged to a fiat currency.<sup>85</sup> It does not involve a claim on the issuer and it constitutes itself the unit of currency.<sup>86</sup> Admittedly, some virtual currencies are convertible in real currency,<sup>87</sup> meaning that users can buy and sell virtual currencies for Euros or US Dollars.<sup>88</sup> However, such convertibility is not guaranteed by law nor by any central bank or public authority,<sup>89</sup> but depends on fluctuating exchange rates, moving with the daily supply and demand. Consequently, risks of devaluation have been commonly associated with the high volatility of virtual currencies.<sup>90</sup>

## B. Virtual currencies, digital tokens and virtual assets

The 5<sup>th</sup> AML Directive does not solve, however, the thorny question regarding the legal status of virtual currencies. Nor does it contradict sectorial legal qualifications – such as security, commodity, property, money – that State authorities extended or denied in their specific field of competences with the aim to clarify whether and to what extent this new technology falls within the scope of existing regulations.<sup>91</sup> Article 3 (18) Directive 2015/849/EU intends to provide a transversal legal definition, which is meant to be sufficiently broad to encompass the myriad of existing virtual currencies schemes.<sup>92</sup> The difficulty is even greater, as the appropriateness of the definition adopted is dependent on the rapid technological advances, which incessantly drive the emergence of new forms of digital assets.<sup>93</sup> Along this line, the positive definition provided by the 5<sup>th</sup> AML Directive reads ‘*virtual currencies*’ means a digital representation of value that [...] is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically’.<sup>94</sup>

---

definition and detailed analysis of stablecoins, see D Bullmann, J Klemm, A Pinna, In search for stability in crypto-assets: are stablecoins the solution?, ECB Occasional Paper Series No. 230 (August 2019) <<https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf>>.

<sup>84</sup> EBA, Report with Advice for the European Commission on Opinion on Crypto-assets (January 2019).

<sup>85</sup> Art. 3 (18) Directive (EU) 2015/849.

<sup>86</sup> R. Stokes, ‘Virtual money laundering: the case of Bitcoin and Linder dollar’, 21(3) Information & Communication Technology Law (October 2012), p. 227.

<sup>87</sup> FATF Report, Virtual currencies. Key Definitions and Potential AML/CFT Risks (June 2014), p. 5.

<sup>88</sup> As for the ‘interoperability’ of virtual currencies with the real world, ECB Report, Virtual currency Schemes (October 2012), p. 14.

<sup>89</sup> FATF Report, Virtual currencies. Key Definitions and Potential AML/CFT Risks (June 2014), p. 4.

<sup>90</sup> ECB Report, Virtual currency Schemes – a further analysis (February 2015), p. 23.

<sup>91</sup> At the national level in particular, States’ regulators and law enforcement agencies strived to define the legal status of cryptocurrencies (e.g. banking and financial regulations, tax and consumer law) Such a sectorial approach has resulted in a patchwork of warnings, guidelines and few regulatory measures that primarily focus on the disputed legal status of cryptocurrencies. Similar questions arose concerning the scope of application of EU legal instruments. For instance, the CJEU held that Bitcoin is ‘a direct means of payment’ and, therefore, conversion of such virtual currency into fiat currencies is a transaction exempted from VAT within the meaning of Directive 2006/112/EC. Case C-264/14, *Skatteverket v David Hedqvist*, EU:C:2015:718.

<sup>92</sup> It has been estimated that the sole Bitcoin has spawned around 500 to 600 similar virtual currencies. See European Parliament Think Thank, Virtual currencies: Challenges following their introduction (22 March 2016), PE 579.110.

<sup>93</sup> EBA. Opinion on virtual currencies (4 July 2014), p. 10. Similarly, the FATF stresses that the ‘vocabulary may change as virtual currencies evolves’. FATF Report, Virtual currencies. Key Definitions and Potential AML/CFT Risks (June 2014), p. 4.

<sup>94</sup> Art 3 (18) Directive 2015/849/EU.

The wording of Article 3 (18) Directive 2015/849/EU leads to two remarks. Firstly, the above-mentioned provision ‘is phrased technologically neutral’.<sup>95</sup> It does not refer to specific technical features that would characterize virtual currencies, such as cryptography or blockchain. However, references to cryptographic keys<sup>96</sup> and convertibility for fiat currencies<sup>97</sup> make clear the EU legislator intends to tackle above all criminal misuses of cryptocurrencies.<sup>98</sup>

Secondly, one may wonder whether the so-called ‘tokenisation’ process<sup>99</sup> makes already the 5<sup>th</sup> AML Directive outdated. Indeed, cryptocurrencies are chronologically speaking the first type of crypto-assets. Few years after the creation of Bitcoin, start-ups began to experiment a new form of fundraising based on the distributed ledger technology. The subsequent development of Initial Coin Offering (ICOs) led to the diversification of virtual assets that are not anymore and exclusively conceived as an alternative mean of payment, as cryptocurrencies initially were.<sup>100</sup> Some of them also provide specific rights ‘in the form of ownership rights or entitlements similar to dividends’, such as investment tokens.<sup>101</sup> Others ‘enable access to a specific product or service often provided using a DLT platform but are not accepted as a means of payment for other products or services’, like utility tokens.<sup>102</sup>

Do virtual currencies within the meaning of the 5<sup>th</sup> AML Directive also encompass these new categories of virtual assets? Interesting enough, the legal definition of virtual currency does not limit its function to a mean of payment, as the Commission proposal initially did.<sup>103</sup> It refers to digital representations of a value accepted as ‘means of exchange’.<sup>104</sup> The preamble of the 5<sup>th</sup> AML Directive suggests the adoption of a broad interpretation of the term that aims to ‘cover all the potential uses of virtual currencies’, including ‘investment, store-of-value products or use in online casinos’.<sup>105</sup> It is fairly evident that the EU decision-makers sought to ensure that cryptocurrencies fall under the scope of AML regulations even when used as speculative investment at the time of the rocketing Bitcoin prices.<sup>106</sup> One may wonder, however, whether the exchange function referred to under the Directive suffices to cover all sorts of tokens. In this regard, the wording of Article 3 (18) Directive 2015/849/EU is confusing since it evokes

---

<sup>95</sup> L Haffke, M Fromberger, P Zimmermann, ‘Virtual Currencies and Anti-Money Laundering – The Shortcomings of the 5th AML Directive (EU) and How to Address Them’, *Journal of Banking Regulation* (2019), forthcoming, pre-print version, p. 9.

<sup>96</sup> Art 1(2) g) Directive 2015/849/EU.

<sup>97</sup> Art 3 (19) Directive 2015/849/EU.

<sup>98</sup> N Vandezande, *Virtual Currencies: A Legal Framework* (Intersentia 2018), p. 292.

<sup>99</sup> The term ‘tokenisation’ is commonly used to describe ‘method that converts rights to an asset into a crypto token which becomes a representation of such right’. See V Burilov, ‘Regulation of Crypto Tokens and Initial Coin Offerings in the EU, de lege lata and de lege ferenda’, *6 European Journal of Comparative Law and Governance* (2019), p. 147.

<sup>100</sup> On the spectacular development of ICOs, see P Hacker, C Thomale, ‘Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law’, *15 European Company and Financial Law Review* (2018), p. 645.

<sup>101</sup> In a recent report, EBA outlines the following taxonomy of crypto-assets. EBA, Report with advice for the European Commission on crypto-assets (January 2019), p. 7.

<sup>102</sup> *Ibid.*

<sup>103</sup> Art. 1(2) c) Proposal for a Directive, COM(2016)450 final.

<sup>104</sup> Art 3 (18) Directive 2015/849/EU.

<sup>105</sup> Recital 10 Directive (EU) 2015/849.

<sup>106</sup> The different uses of cryptocurrencies where particularly highlighted by ECB, Opinion of 12 October 2016 on a proposal for a directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/E, JO [2016] C 459/3, p. 5.

the economic meaning of ‘means of exchange’ that is commonly used to describe the economic function of money. From this perspective, the above-mentioned provision would not broadly refer to the exchangeable character of an asset, but only to those intermediary objects that facilitate trading of goods and services.<sup>107</sup> Accordingly, some authors advocate for a narrow interpretation that would exclude from the scope of application investment and utility tokens that are not - at least not predominantly – ‘used as such an intermediary asset in trade’.<sup>108</sup>

Such a stringent interpretation heightens even more the legal uncertainty surrounding the material scope of the 5<sup>th</sup> AML Directive insofar as the inclusion of a specific digital token would ultimately rely on the functionalities and the purpose for which it was designed. Moreover, national transposal measures are likely to go beyond the minimum requirements set out by the Directive in order to comply with the much more ambitious FATF Recommendations. Indeed, the international standards on combating money laundering target any sort of ‘virtual asset’, which is understood as ‘*a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes*’.<sup>109</sup> The definition is so vague that it is difficult to circumscribe the notion, which clearly aspires to cover future forms of digital assets<sup>110</sup> that are not ‘already covered elsewhere in the FATF Recommendations’.<sup>111</sup> Admittedly, the fuzzy phrasing has also the merit of overcoming divergent understandings and classifications of digital assets that may vary ‘across jurisdictions or even among industry’.<sup>112</sup> Nonetheless, legal uncertainty as for the object of AML regulations inevitably affects the identification of its subjects, namely those virtual currencies and/or assets service providers that become obliged entities.

## **V. Identifying obliged entities: transposing or reshaping the AML enforcement architecture?**

### **A. Targeting the gatekeepers: exchanges and custodial wallet providers**

Due diligence, KYC procedures, duties to report and to cooperate are the pillars of AML/CTF legislation. Along this line, the EU Directives impose a set of obligations to credit institutions, professionals of the financial system, lawyers, notaries and other middlemen, who execute transactions that are likely to be part of a money laundering or terrorism financing scheme.<sup>113</sup> Hence, intermediaries of investment and other financial operations play a frontline role in detecting suspicious transactions, thus becoming key actors of the AML enforcement system. This approach can hardly be extended as such to cryptocurrencies schemes, precisely

---

<sup>107</sup> L Haffke, M Fromberger, P Zimmermann, *loc. cit.*, pp. 11 ff.

<sup>108</sup> *Ibid.*, 13.

<sup>109</sup> FATF Recommendations, p. 124.

<sup>110</sup> The FATF indeed stressed the technology-neutral and future-proofing character of the definition, which is ‘intended to have sufficient flexibility that countries and relevant entities can apply them to existing technologies as well as to evolving and emerging technologies without requiring additional revisions’. FATF, Guidance on Virtual Assets and Virtual Assets Service Providers, para. 19.

<sup>111</sup> FATF Recommendations, p. 124.

<sup>112</sup> FATF, Guidance on Virtual Assets and Virtual Assets Service Providers, para. 49.

<sup>113</sup> Art 2 Directive 2015/849/EU

because the underlying distributed ledger technology undertakes the disintermediation of payment systems.<sup>114</sup> The resulting peer-to-peer networks build on the lack of trust intermediaries and cut out – or at least seeks to remove as much as possible – middlemen.<sup>115</sup> Therefore, instead of identifying spots of control within the market, the 5<sup>th</sup> AML Directive defines as obliged entities the ‘gatekeepers’, in other words those services that work as access and exit points of the cryptocurrencies ecosystem.<sup>116</sup> By implementing this strategy, the EU legislature added two actors to the list of obliged entities provided in Article 2 Directive 2015/849/UE.

The first category consists in natural or legal persons acting in the exercise of their professional activities who provide exchange services between virtual currencies and fiat currencies.<sup>117</sup> Thus, the 5<sup>th</sup> AML Directive clearly targets exchange platforms that enable users to buy and sell cryptocurrencies against payment of a fee.<sup>118</sup> Whilst the Commission intended to specifically target such centralized exchange platforms, the final wording of the provision is broader and thus encompasses other entities. For instance, cryptocurrencies ATMs or ‘kiosks’, also enable users to convert back and forth virtual currencies into banknotes.<sup>119</sup>

Conversely, doubts may arise as for the very nature of peer-to-peer trading platforms and decentralized exchanges. The service provided by those entities does not consist properly speaking in the exchange or conversion of cryptocurrencies. Peer-to-peer exchanges simply provide users with a market place maintained and operated by a software that facilitates transactions among buyers and sellers by connecting them to one another.<sup>120</sup> Hence, if a trading platform works like a forum where users can post bids and offers but transactions take place outside that platform, it does not fall within the scope of the 5<sup>th</sup> AML Directive. However, one may argue, in line with the FATF Guidance on Virtual Assets, that peer-to-peer platforms facilitate the exchange and, therefore, provide an exchange service when acting as an intermediary in the transaction.<sup>121</sup> This would be the case, for instance, where the platform purchases virtual currencies from a seller and sells them to a buyer after that the former’s bid matched with the latter’s offer.<sup>122</sup> Assuming that certain peer-to-peer trading platforms engage in exchange services, the identification of the person that would consequently qualify as obliged entity still is problematic.<sup>123</sup> Given that trading platforms are not run by a central administrator, the FATF goes as far as to target the owner or operator of the software program in question.<sup>124</sup>

The major limitation in the scope of the 5<sup>th</sup> AML Directive lies in the conversion requirement between virtual and fiat currencies. As a result, the so-called crypto-to-crypto exchanges that enable a user to convert a specific virtual currency into another do not fall within

---

<sup>114</sup> In a similar way Stokes underlines that the decentralized structure of Bitcoin constitute a major challenge for the enforcement of AML/CTF measures. See R. Stokes, *loc. cit.*, p. 230.

<sup>115</sup> Disintermediation is among the characteristic features of blockchain. See P De Filippi, A Wright, *loc. cit.*, pp. 34 ff

<sup>116</sup> COM(2016) 450 final, 7.

<sup>117</sup> Art. 2 (3) lit g Directive 2015/849/EU.

<sup>118</sup> R. Houben, A. Snyers, *loc. cit.*, p. 26.

<sup>119</sup> T. Keatinge, D. Carlisle, F. Keen, ‘Virtual currencies and terrorist financing: assessing the risks and evaluating responses’, Study requested by the TERR Committee of the European Parliament (May 2018), PE. 604.970, p. 15.

<sup>120</sup> R. Houben, A. Snyers, *loc. cit.*, pp. 27 and 77.

<sup>121</sup> FATF, Guidance on Virtual Assets and Virtual Assets Service Providers, para. 39.

<sup>122</sup> *Ibid.*, 15

<sup>123</sup> R. Houben, A. Snyers, *loc. cit.*, p. 77.

<sup>124</sup> FATF, Guidance on Virtual Assets and Virtual Assets Service Providers, para. 40.

this first category of obliged entities.<sup>125</sup> Based on this limitation, one can also exclude the vast majority of companies running ICOs. Indeed, assuming that the tokens in question qualify as virtual assets within the meaning of the 5<sup>th</sup> AML Directive,<sup>126</sup> only if the issuer sells tokens for fiat currencies, that company is bound by AML compliance rules. Yet, most of the ICOs exchange tokens for Bitcoin or Ether, meaning that they consist in a crypto-to-crypto exchange service.<sup>127</sup> Again, the 5<sup>th</sup> AML proves to be outdated in the light of the FATF Recommendations that apply to both fiat-to-crypto and crypto-to-crypto exchange services.<sup>128</sup>

The second category of obliged entities introduced by the 5<sup>th</sup> AML Directive are custodian wallet providers.<sup>129</sup> According to Article 3 (19) Directive 2015/849, a custodial wallet is ‘an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies’. The definition is essential since it excludes other types of digital wallets from the scope of the AML/CTF legislation. If the service in question consists in hardware or software solutions that facilitate access to the network and transfer of funds by users, the providers of such services do not constitute obliged entities within the meaning of EU law.<sup>130</sup> Indeed, neither entities selling physical devices like USB sticks where the user can store his private key offline – i.e. hardware wallets –, nor companies developing downloadable applications that ‘can be maintained on a desktop or mobile device and allow storage of private keys securely on the device’ – i.e. software wallets – have access to the private key that is essential for both identifying the users and freeze or confiscate the funds.<sup>131</sup> Conversely, the Directive focuses on entities that host on their server the users’ private keys and thus keep control on the funds stored in the wallet. Thus defined, the scope of application of EU AML regulation targets those services that resemble bank or payment accounts subject to Regulation 2015/847/EU,<sup>132</sup> which primarily correspond to hot wallets accessible via an internet connection.<sup>133</sup>

Considering that most exchange platforms also provide custodian wallet services, one could infer that crypto-to-crypto exchanges fall under this second category of obliged entities.<sup>134</sup> Such a reading highlights a major shortcoming. On the one hand, the main argument for including custodian wallets into the list of obliged entities is to monitor transactions within the cryptocurrencies economy.<sup>135</sup> As emphasized by the Commission, this becomes crucial as the ‘growing network acceptance [reduces] the need to ‘cash-out’ of virtual currencies and exchange them for fiat currencies’.<sup>136</sup> On the other hand, the 5<sup>th</sup> AML Directive expressly limits its scope of application to crypto-to-fiat transactions only, casting doubts on the intention of the

---

<sup>125</sup> R. Houben, A. Snyers, *loc. cit.*, p. 77

<sup>126</sup> See above.

<sup>127</sup> D Zetzsche et al., *loc. cit.*

<sup>128</sup> The said activities are part of the definition of VASP under (i) and (ii). See FATF Recommendations, p. 125.

<sup>129</sup> Art. 2 (3) lit. h Directive 2015/849/EU.

<sup>130</sup> R. Houben, A. Snyers, *loc. cit.*, p. 78

<sup>131</sup> T. Keatinge, D. Carlisle, F. Keen, *loc. cit.*, p. 14.

<sup>132</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, OJ [2015] L 141/1. Hereinafter Fund Transfer Regulation.

<sup>133</sup> On the distinction between hot and cold wallets, EBA, Report with advice for the European Commission on crypto-assets (January 2019), p. 9.

<sup>134</sup> L Haffke, M Fromberger, P Zimmermann, *loc. cit.*, pp. 16.

<sup>135</sup> SWD (2016) 223 final, p. 51.

<sup>136</sup> *Ibid.*, p. 31.



drafters to regulate crypto-to-crypto exchanges. Yet, the latter present a high risk of money laundering in so far as they enable users to convert digital assets into more anonymous brands of virtual currencies.<sup>137</sup> Nevertheless, they are bound by due diligence and reporting duties under the 5<sup>th</sup> AML Directive solely when they provide ancillary services characterizing one of the other obliged entities listed under Article 2 Directive 2015/849/UE.

## **B. Users and minors, the excluded market players**

Limits in the scope of application of the 5<sup>th</sup> AML Directive are the result of a proportionate approach adopted by the Commission, which emphasized the need to protect not only privacy but also freedom to conduct business.<sup>138</sup> As highlighted above, the function of the service providers included in the list of obliged entities is to facilitate access to the cryptocurrencies schemes and simplify transactions orders. However, a user does not necessarily need a custodial wallet or exchange platform to transfer and convert virtual currencies. The European policy-makers are well aware of this, since they acknowledge in the preamble of the 5<sup>th</sup> AML Directive that ‘a large part of the virtual currency environment will remain anonymous because users can also transact without such providers’.<sup>139</sup> The resulting balanced approach automatically entails the exclusion of key market players.

There is indeed no benefit in including miners among the obliged entities, considering that they participate in the validation process of the transaction without however having specific interactions with the users.<sup>140</sup> Interesting enough, the Commission clearly acknowledged at the time of writing the proposal that the massive location of minors in China ‘would make any initiative largely impossible to enforce’.<sup>141</sup>

As regards the users, the 5<sup>th</sup> AML Directive invites the Commission to explore the possibility of setting-up a system of self-declaration,<sup>142</sup> which would enable users of virtual currencies to identify themselves to designated authorities on a voluntary basis.<sup>143</sup> The information thus collected could feed ‘a central database registering users’ identities and wallet addresses accessible to FIUs’.<sup>144</sup> One may doubt, however, the effectiveness of a voluntary self-identification system as a useful tool against money laundering and terrorism financing, the perpetrators of which are presumably willing to hide their identity.<sup>145</sup>

---

<sup>137</sup> An ‘increasing use of virtual-to-virtual layering schemes’ has been noticed in the FATF, Guidance on Virtual Assets and Virtual Assets Service Providers, para. 4.

<sup>138</sup> COM (2016) 450, p. 11.

<sup>139</sup> Recital 9 Directive 2018/843/EU.

<sup>140</sup> SWD (2016) 223 final, p. 15.

<sup>141</sup> *Ibid.*

<sup>142</sup> Art. 65 (1) Directive 2015/849/EU.

<sup>143</sup> Recital 9 Directive 2018/843/EU.

<sup>144</sup> Art. 65 (1) Directive 2015/849/EU.

<sup>145</sup> On the problematic aspects of the measure see R. Houben, A. Snyers, *loc. cit.*, p. 80; D. Connel, *loc. cit.*, p. 84; A.A. Gikay, ‘Regulating Decentralized Cryptocurrencies under Payment Service Law: Lessons from the European Union Law’, 9 *Journal of Law, Technology and the Internet* (2018), p. 28.

### C. Further inclusion of virtual assets service providers

Last but not least, we should not exclude that the EU will amend once again the AML Directives in the near future for the sake of implementing the last amendments to the FATF Recommendations. As of October 2018, Recommendation 15 requires the State Parties to ensure that virtual assets service providers (VASPs) ‘are regulated for AML/CTF purposes’.<sup>146</sup> The concept covers a broader array of market players that goes far beyond the scope *ratione personae* of the 5<sup>th</sup> AML Directive. Unlike the subject-based list of obliged entities provided under Article 2 Directive 2015/849/EU, the FATF adopted an activity-based definition of VASPs that, in order to overcome difficulties and divergences with the classification of relevant actors, focuses on the nature of the product and service provided.<sup>147</sup> Hence, where a natural or legal person conducts as a business one or more of the activities or operations characterizing VASPs for or on the behalf of his client, that person qualifies as obliged entity under the international standards.<sup>148</sup> Consequently, the same entity may fall into one or more of the activities listed in the VASPs definition.<sup>149</sup>

As for the substance, the FATF aims to target not only entities that play the role of ‘gatekeepers’ in its literal meaning or ‘gateways’ at the boundary between crypto markets and real economy. The Recommendations clearly seek to include market players that circumscribe their business in a ‘virtual-to-virtual’ dimension.<sup>150</sup> Indeed, besides (i) exchange between virtual assets and fiat currencies, the listed activities encompass (ii) exchange between one or more forms of virtual assets, (iii) transfer of virtual assets, (iv) safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets and participation in and (v) provision of financial services related to an issuer’s offer and/or sale of a virtual asset.<sup>151</sup> When read in conjunction with the broad definition of virtual assets,<sup>152</sup> the 2018 amendments to the FATF Recommendations leave no doubt as to the will to wipe as many as possible blind spots within the exploding crypto-assets economy. Indeed, the VASPs definition embraces a wide range of entities that are not, or at least not systematically, subject to the 5<sup>th</sup> AML Directive, such as among others crypto-to-crypto exchanges, ICOs, virtual assets escrow services and brokerage services, decentralized exchange platforms.<sup>153</sup>

In doing so, the FATF Recommendations make AML regulation far more future-proofing than the 5<sup>th</sup> AML Directive, since the wide-ranging activities defining VASPs tend to anticipate both the emergence of new business models as well as a widespread acceptance of virtual currencies and assets, which boosts the self-standing character of the crypto economy.<sup>154</sup> As technological innovations will solve volatility and scalability issues weighing on cryptocurrencies ecosystems, one can hardly assume that users and particularly those who perpetrate criminal activities systematically need, sooner or later, to convert virtual currencies

---

<sup>146</sup> FATF Recommendation 15, para. 2.

<sup>147</sup> FATF, Guidance on Virtual Assets and Virtual Assets Service Provider, para 49.

<sup>148</sup> FATF Recommendations, p. 125.

<sup>149</sup> FATF, Guidance on Virtual Assets and Virtual Assets Service Providers, para. 44.

<sup>150</sup> FATF, Guidance on Virtual Assets and Virtual Assets Service Providers, para. 52.

<sup>151</sup> FATF Recommendations, p. 125.

<sup>152</sup> See above.

<sup>153</sup> FATF, Guidance on Virtual Assets and Virtual Assets Service Providers, para. 35 ff.

<sup>154</sup> FATF, Guidance on Virtual Assets and Virtual Assets Service Providers, para 19.

or assets and integrate again the traditional regulated markets. Paradoxically, the in-depth implementation of AML regulations within the crypto markets may have the effect of intensifying interactions with the traditional banking and financial institutions that still look on the unregulated virtual assets service providers with distrust.<sup>155</sup> As a result, the extended scope of AML regulations preconized by the FATF will not only significantly increase the number of intra-market spots of control. In an indirect way, it is likely to foster the role of credit institutions and other obliged entities in detecting the illicit origin of funds or profits delivered from virtual currencies and/or assets trading. This holds true provided that the said obliged entities are able to implement in an effective way due diligence rules and monitoring requirements.

## **VI. Implementing customer due diligence: collection, decryption and analysis of transactions data**

### **A. From ‘pseudonymity’ to privacy coins**

The ultimate goal of due diligence rules imposed on exchange services and custodian wallet providers lies in the detection of suspicious transactions that are part of a laundering or terrorism financing scheme. The obligations imposed on obliged entities notably imply the duty to identify customers and the beneficial owner (so-called KYC requirements), to collect information on the business relationship including the source of the funds, to monitor and scrutinize certain transactions on the basis of a risk-assessment<sup>156</sup> and, when confronted with a suspicious transaction, to report and cooperate with the competent authorities.<sup>157</sup>

By extending these measures to virtual currencies service providers, the 5<sup>th</sup> AML Directive tackles what regulators, bodies and agencies around the world consistently acknowledged as being a major challenge for the law enforcement authorities: the anonymity of cryptocurrencies schemes.<sup>158</sup> Contrary to conventional wisdom, however, all cryptocurrencies are not equally anonymous. Instead, the level of anonymity actually depends on the technological features that characterize each specific currency.<sup>159</sup> Bitcoin for instance is far from being anonymous. It would be more accurate to describe it in terms of pseudonymity.<sup>160</sup> Indeed, the system relies on a public blockchain, namely an openly accessible and tamperproof ledger that allows every user to check the date, amount, origin and destination addresses of Bitcoin transfers.<sup>161</sup> Whilst transaction records are transparent, the real challenge

---

<sup>155</sup> Such mistrust has initially taken the form of refusing banking services to cryptocurrencies sellers and VASPs. D. Connel, *loc. cit.*, p.81.

<sup>156</sup> Customer due diligence duties are defined under Article 11 Directive 2015/948/EU.

<sup>157</sup> Art 33 Directive 2015/948/EU.

<sup>158</sup> See for instance, European Parliament, Committee on Economic and Monetary Affairs, Report on virtual currencies (May 2016), PE575.277v02-00, p. 7; ECB, Virtual currency schemes – a further analysis (February 2015), p. 22 ; EBA, Opinion on ‘virtual currencies’, EBA/Op/2014/08 (July 2014), p. 32 ; Joint Warning, ESMA, EBA and EIOPA warn consumers on the risks of Virtual Currencies (February 2018).

<sup>159</sup> T. Keatinge, D. Carlisle, F. Keen, *loc. cit.*, pp. 30 ff.

<sup>160</sup> On the concept of ‘pseudonymity’ as opposed to ‘anonymity’, C. Brenig, R. Accorsi, G. Müller, ‘Economic Analysis of Cryptocurrency Backed Money Laundering’, ECIS 2015 Completed Research Paper n° 20 (2015), pp. 8 – 9.

<sup>161</sup> P De Filippi, A Wright, *loc. cit.*, p. 37.

lies in the identification of the user who hides behind his public and private keys.<sup>162</sup> In the light of this, KYC checks that exchange platforms and custodian wallet providers are required to perform under the 5<sup>th</sup> AML Directive precisely aim at linking the virtual account or address to the real identity of his owner.<sup>163</sup>

From a law enforcement perspective, more problematic are the so-called ‘privacy altcoins’, such as Monero, Dash or Zcash.<sup>164</sup> These are currencies specifically designed to provide users with a high level of anonymity, to the extent that their developers readily compare them with digital cash.<sup>165</sup> Again, the degree of confidentiality relies on the specific technology on which each privacy coin is based. Monero, for instance, is a telling illustration of how a set of cryptographic protocols can significantly hamper not only the identification of users, but also the tracing of funds.<sup>166</sup> The user first hides his identity behind ‘ring signatures’: instead of validating the transfer of funds with his own key only, the system combines or mixes it with other signatures that are randomly selected on the blockchain.<sup>167</sup> As a result, it becomes extremely difficult to distinguish the real signer of the transaction among the ring members and, consequently, to identify the issuing account. In addition, the system generates ‘stealth addresses’ when executing the transaction. Thanks to this, ‘all payments sent to the recipient are routed through these addresses, ensuring there are no links on the blockchain between the sender’s and the recipient’s address’.<sup>168</sup> Hence, as other privacy coins, Monero holds the promise of untraceability and unlinkability, explaining an increasing trend in the use of anonymity-enhanced cryptocurrencies.<sup>169</sup>

Given their anonymous character, privacy coins represent a major challenge for both law enforcement authorities and obliged entities that will be subject to due diligence rules once the 5<sup>th</sup> AML Directive will be transposed into national law. In this regard, it is worth mentioning that EU law as well as the FATF Recommendations abides by the principle of technological neutrality:<sup>170</sup> they do not prohibit privacy coins as such, but simply apply customer due diligence duties irrespective of the technology involved.<sup>171</sup> Despite this, one may wonder whether the enforcement of AML rules is likely to make the provision of services related to privacy coins illegal in practice. Wouldn’t an exchange platform converting Euros for Monero systematically violate the AML regulations if not able to identify neither his client nor the

---

<sup>162</sup> D. Bryans, ‘Bitcoin and Money Laundering: Mining for an Effective Solution’, 89 *Indiana Law Journal* (2014), p. 447.

<sup>163</sup> Recital 9 Directive 2018/843/UE.

<sup>164</sup> Whilst listing privacy coins among the major challenges of AML regulations, the FATF uses the term ‘anonymity-enhanced cryptocurrencies’ (AECs). See FATF Guidance on Virtual Assets and Virtual Assets Service Providers, p. 4.

<sup>165</sup> ‘Monero is cash for a connected world’ is the first sentence introducing the cryptocurrencies to users that connect on the Monero project webpage. See <<https://www.getmonero.org>>

<sup>166</sup> Other privacy coins build on different technological application. Zcash, for instance, preserve anonymity thanks to a cryptographic protocol called ‘zero-knowledge proofs’, which allows the system to validate and certify an information without such information being disclosed to the parties involved in the transaction. T. Keatinge, D. Carlisle, F. Keen, *loc. cit.*, p. 32.

<sup>167</sup> R. Houben, A. Snyers, *loc. cit.*, p. 46.

<sup>168</sup> *Ibid.*

<sup>169</sup> Europol, IOCTA 2018, *loc. cit.*, p. 58.

<sup>170</sup> On the *rationale* and arguments for and against the principle of tech neutrality, see W. Hartzog, *Privacy's Blueprint : The Battle to Control the Design of New Technologies* (Harvard University Press, 2018), pp. 45 ff.

<sup>171</sup> FATF Guidance on Virtual Assets and Virtual Assets Service Providers, para. 19.

beneficial owner of the transaction?<sup>172</sup> Wouldn't a custodian wallet provider be exposed to sanctions where the technology inherent to a cryptocurrency prevent it from ascertaining the source and destination of the transferred funds and therefore from identifying unusual or suspicious transactions?<sup>173</sup> Those questions are not purely hypothetical. In May 2018, the exchange platform Coincheck renounced to trade four privacy coins, including Monero and ZCash, to conform with the guidelines of the Japanese Financial Services Agency, which strongly warned about the crime-related risks inherent to their anonymous character.<sup>174</sup> Later on, the exchange resumed part of the suspended activities by requiring the users to provide detailed information about destination addresses and reasons for the transactions.<sup>175</sup> A similar policy was adopted by Changelly, a Czech platform that, due to high risks of money laundering inherent to privacy coins, withheld hundreds of Monero belonging to customers who refused to undergo strict KYC checks.<sup>176</sup>

## B. Mixers, tumbler and other anonymity-enhancing tools

Whilst such measures triggered strong reactions from users claiming their right to opt for more privacy-protective altcoins, law enforcement agencies started to pool their efforts against other anonymizing tools that are specifically designed to obfuscate cryptocurrencies transactions. In May 2019, the Dutch authorities in cooperation with Europol and Luxembourg shut down 'Bestmixer.io', one of the three largest mixing services for cryptocurrencies with an estimated annual turnover exceeding 200 millions US dollars.<sup>177</sup> Such mixers or tumblers work like a blender that clusters cryptocurrencies belonging to many users, mixes inputs and outputs of transactions and finally redistribute coins among the users.<sup>178</sup> As a result, mixers enhance also anonymity of pseudonymous coins, 'scrambling the trail of transactions to make it more difficult to decipher the flow'.<sup>179</sup>

Some authors advocate for the inclusion of mixers and tumblers among the obliged entities targeted by the 5<sup>th</sup> AML Directive.<sup>180</sup> The very broad definition of VASPs under the FATF Recommendations seems to move in that direction: services consisting in the 'transfer of virtual assets', i.e. 'conduct a transaction on behalf of another natural or legal person that moves a virtual asset from one virtual asset address or account to another', shall be subject to

---

<sup>172</sup> Art 13 (1) Directive 2015/948/EU.

<sup>173</sup> Art. 15 (3) Directive 2015/948/EU.

<sup>174</sup> J. Adelstein, 'Japan's Financial Regulator Is Pushing Crypto Exchanges To Drop 'Altcoins' Favored By Criminals', *Forbes* (30 April 2018).

<sup>175</sup> K. Helms, *Coincheck Delists XMR, DASH, ZEC, REP – Prompted by Japanese Regulator* (19 May 2018), <<https://news.bitcoin.com/coincheck-delists-xmr-dash-zec-rep/>>.

<sup>176</sup> C. Masters, 'Changelly Service Under Fire for Holding Back Monero (XMR)' (5 September 2018), <<https://cryptovest.com/news/changelly-service-under-fire-for-holding-back-monero-xmr/>>.

<sup>177</sup> Europol Press Release, *Multi-million Euro Cryptocurrency Laundering Service Bestmixer.io taken down* (22 May 2019), <<https://www.europol.europa.eu/newsroom/news/multi-million-euro-cryptocurrency-laundering-service-bestmixer-io-taken-down>>.

<sup>178</sup> Users can access mixing services directly via the Internet or through the Tor network, they can either 'create an account or interact with the service via a web interface'. On the use of mixers for the purpose of money laundering, M.Möser, R. Böhme, D. Breuker, 'An inquiry into Money Laundering Tools in the Bitcoin Ecosystem', 2013 APWG eCrime Researchers Summit, p. 5.

<sup>179</sup> T. Keatinge, D. Carlisle, F. Keen, *loc. cit.*, p. 32.

<sup>180</sup> L Haffke, M Fromberger, P Zimmermann, , *loc. cit.*, p. 18.

due diligence, reporting and cooperation duties.<sup>181</sup> To clarify the scope of such definition, it is worth referring to the distinction made by the US Financial Crimes Enforcement Network (FinCEN) in a guidance published in May 2019.<sup>182</sup> On the one hand, an ‘anonymizing services provider’ plays the role of an intermediary ‘by accepting value from a customer and transmitting the same or another type of value to the recipient, in a way designed to mask the identity of the transmitter’.<sup>183</sup> Those entities qualify as ‘money transmitter’ under FinCEN regulations and therefore become obliged entities for the purpose of AML rules. Likewise, one may argue that anonymizing service providers fall under the FATF definition of VASPs. On the contrary, ‘anonymizing software providers’ simply offers a tool that a user can utilize on his behalf to anonymize its own transactions.<sup>184</sup> Accordingly, this second category of decentralized or peer-to-peer mixers does not engage in the ‘transfer of virtual assets’ within the meaning of the FATF Recommendations. Including mixers and tumblers among the list of obliged entities highlights, however, the paradoxical limits of tech neutrality: AML regulation does not forbid *a priori* anonymizing service providers, but obliges those entities whose core business consists in obfuscating data to precisely collect, monitor and report such information to State authorities.

Whereas the said anonymizing services are in direct contrast with AML regulations,<sup>185</sup> one should not underestimate the impact of technological advances that are not designed for privacy purposes, but are nonetheless likely to strengthen confidentiality. Examples of the second category can be found in technological applications primarily aimed at solving scalability issues or circumventing centralized service providers that raise cyber vulnerabilities. Whilst the ‘atomic swap’ makes possible for two users to exchange different types of cryptocurrencies without the need to resort on a platform,<sup>186</sup> other systems such as the Lightning Network<sup>187</sup> or ‘mimble wimble’ applications may significantly increase the level of anonymity by reducing the volume of data records for the blockchain to work securely and faster.<sup>188</sup>

### C. Expertise and analysis software

Whilst technological innovations may enhance on purpose or increase as a side effect the opacity of cryptocurrencies schemes, IT tools are also crucial for the effective implementation of AML regulations. From this perspective, the question arises of whether obliged entities as well as law enforcement authorities, in particular financial intelligence units (FIUs), have adequate means to record and analyze data related to transactions and beneficial ownerships.

---

<sup>181</sup> FARF Recommendations, p. 125.

<sup>182</sup> FinCEN Guidance, Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies (9 May 2019), FIN-2019-G001.

<sup>183</sup> *Ibid*, p. 19.

<sup>184</sup> *Ibid*, p. 20.

<sup>185</sup> The FATF clearly identifies mixers and tumblers among the high risk factors that facilitate money laundering. FATF, Guidance on Virtual Assets and Virtual Assets Service Providers, para. 151.

<sup>186</sup> R. Houben, A. Snyers, *loc. cit.*, p. 38.

<sup>187</sup> J. Poon, T. Dryja, ‘The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments’ (2016), <<https://nakamotoinstitute.org/static/docs/lightning-network.pdf>>.

<sup>188</sup> T. E. Jedusor, ‘MimbleWimble’ (19 July 2016), <<https://scalingbitcoin.org/papers/mimblewimble.txt>>.

As regards the new obliged entities subject to AML regulations, one of the most controversial aspects lies in the implementation of the so-called ‘travel rule’ enshrined in Recommendation 16 of the FATF.<sup>189</sup> The measure aims to facilitate investigations by the law enforcement authorities by creating an information trail accompanying wire transfers. To this end, when a bank transfers funds on behalf of his client, it shall on the one hand transmit to the receiving financial institution accurate information enabling the identification of the sender (the originator) and hold information about the recipient of the funds (beneficiary) shared by the receiving financial institution.<sup>190</sup> From a technical point of view, the implementation of the travel rule by VASPs raises operational hurdles, pushing them to look for specific technological solutions.<sup>191</sup> Worthy of mention is that the adoption of the 5<sup>th</sup> AML Directive did not automatically impose obligations stemming from the travel rule to virtual currencies exchanges and custodian wallet providers. Indeed, at the time of writing, the EU Fund transfer Regulation<sup>192</sup> implementing Recommendation 16 of the FATF does not cover virtual currencies.<sup>193</sup> The extension of its scope of application by the EU is only a matter of time and may represent additional costs that VASPs will have to bear in order to comply with the whole set of due diligence rules.

From the viewpoint of FIUs, police and prosecuting authorities, the enforcement of AML regulations in the field of virtual assets opens up several legal and operational questions. Assuming that an exchange platform diligently reports suspicious transfers, the competent FIU can hardly exploit the information without an appropriate software that enables its officers to analyse and track transactions.<sup>194</sup> Analytical tools are not *per se* sufficient if the competent authority lacks expertise and understanding of the complex technology underlying crypto-assets.<sup>195</sup> Finally yet importantly, detecting suspicious operations cannot effectively tackle money laundering if EU and national procedural rules do not provide law enforcement authorities with investigative tools for the monitoring, freezing and seizure of crypto-assets.<sup>196</sup>

---

<sup>189</sup> FATF, Interpretative Note to Recommendation 15, pt 7 (b).

<sup>190</sup> More details in FATF, Interpretative Note to Recommendation 16, in FATF Recommendations, pp. 70 ff.

<sup>191</sup> On the operational challenges and possible emerging solutions, A. Bryant, ‘Using Instant Messenger to Explain the FATF Travel Rule for VASPs’ (25 September 2019), <<https://medium.com/swlh/using-instant-messenger-to-explain-the-fatf-travel-rule-for-vasps-2bd786558fb6>>.

<sup>192</sup> Fund Transfer Regulation 2015/847/EU.

<sup>193</sup> Indeed, the European Supervisory Authorities held that virtual currencies do not fall under the definition of ‘funds’ provided by point (15) of Article 4 of Directive 2007/64/EC that determines the scope of application of the Fund Transfer Regulation. See Joint Committee of European Supervisory Authorities (EBA, EIOPA and ESMA - ESAs), Joint Guidelines under Article 25 of Regulation (EU) 2015/847 on the measures payment service providers should take to detect missing or incomplete information on the payer or the payee, and the procedures they should put in place to manage a transfer of funds lacking the required information (22 September 2017) JC/GL/2017/16, p. 33.

<sup>194</sup> Examples of the analytical softwares referred to are Chainanalysis, Elliptic and Neutrino. On the importance of strong cyber and blockchain analysis abilities of law enforcement agencies, M.J. Cronin, ‘Hunting in the Dark: A Prosecutor’s Guide to the Dark Net and Cryptocurrencies’, 66 United States Attorneys’ Bulletin (July 2018), p. 70.

<sup>195</sup> *Ibid.*

<sup>196</sup> In 2014, the United Nations already identified freezing, seizure and confiscation of virtual currencies among the key challenges of for the law enforcement authorities. See United Nations Office on Drugs and Crime, *Basic Manual on the Detection and Investigation of the Laundering of Crime Proceeds Using Virtual Currencies* (June 2014), <[https://www.imolin.org/pdf/imolin/FULL10-UNODCVirtualCurrencies\\_final.pdf](https://www.imolin.org/pdf/imolin/FULL10-UNODCVirtualCurrencies_final.pdf)>, pp. 137 ff.

## VII. Conclusive remarks

By extending the list of obliged entities to professionals providing exchange services between virtual and fiat currencies and custodial wallets, the 5<sup>th</sup> AML Directive represents a step forward in the fighting against criminal misuses of cryptocurrencies. Not only does it tackle terrorism financing and money laundering perpetrated by means of new technologies, but in an indirect way also a wide range of predicate offences perpetrated by means of virtual currencies. A detailed analysis showed, however, a chronic backwardness of the legislative response with regard to the technological breakthroughs and new business opportunities that make continuously and rapidly evolve the crypto economy.<sup>197</sup> As a result, even before the expiry of the transposition deadline, the 5<sup>th</sup> AML Directive looks like a new but in many aspects outdated legal framework for crypto assets. All the more so that the EU legislature will have to adopt in the near future further amendments to its AML regulation in order implement the recent FATF Recommendations, which build on the broader notion of virtual assets and longer list of VASPs.

The adoption and implementation of common international standards is all the more crucial having regards to the intrinsic globalized nature of cryptocurrencies transactions. The resulting convergence among national AML regulations is not sufficient however to solve a key question, which neither the 5<sup>th</sup> AML Directive nor the FATF Recommendation do entirely solve: the law of which country should apply to a virtual assets service provider? From this perspective, the more far-reaching national regulation, the greater the jurisdiction of supervisory authorities that are vested with the power to monitor and ensure compliance of the supervised entities with requirements to combat money laundering and terrorism financing.<sup>198</sup> Whereas regulation and supervision are core pillars of the anti-money laundering preventive policy,<sup>199</sup> cryptocurrencies and digital assets are still subject, however, to differing regulatory approaches around the world<sup>200</sup> and within the EU single market.<sup>201</sup>

In this regard, the 5<sup>th</sup> AML Directive simply requires Member States to ensure that ‘providers of exchange services between virtual currencies and fiat currencies, and custodian wallet providers, are registered’,<sup>202</sup> without explicitly preventing the national competent authorities to impose license requirements and carry out their supervisory mandate on licensed entities.<sup>203</sup> In a similar way, Recommendation 15 of the FATF provides that ‘virtual asset service providers are [...] licensed or registered and subject to effective systems for monitoring

---

<sup>197</sup> The same observation holds true as regards national legislation. See for instance, F. Boehm, P. Pesch, ‘Bitcoin: A first Legal Analysis with reference to German and US-American law’, in R. Böhme, M. Brenner, T. Moore and M. Smith, eds., *Financial Cryptography and Data Security* (Springer, 2014), pp. 43–54.

<sup>198</sup> FATF, Recommendation 27.

<sup>199</sup> As opposed to the anti-money laundering repressive policy that builds on criminal sanctions and criminal law enforcement. See M. van den Broek, *Preventing money laundering. A legal study on the effectiveness of supervision in the European Union* (Eleven International Publishing, 2015), p. 4.

<sup>200</sup> For an overview of the fragmented legal framework at a global level, Library of the US Congress, Report ‘Regulation of Cryptocurrency Around the World’ (June 2018), <<https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf>>.

<sup>201</sup> EBA, Report with advice for the European Commission on crypto-assets (January 2019), p. 17.

<sup>202</sup> Art 47 (1) Directive 2015/849/UE.

<sup>203</sup> The Commission proposal was more explicit on this aspect, since it require the Member States to ‘ensure that providers of exchanging services between virtual currencies and fiat currencies, custodian wallet providers [...] are licensed or registered’. Art 1 (16) Proposal for a Directive, COM (2016) 450 final. See also N. Vandezande, *Virtual Currencies: A Legal Framework*, *loc. cit.*, p. 351.



and ensuring compliance' with the AML international standards.<sup>204</sup> The Guidance on virtual assets sketches out some jurisdictional criteria for the implementation of such licensing and registration requirements. At a minimum, a country shall require a company that is incorporated in its own jurisdiction and engages in one or more activities qualifying VASPs to be registered.<sup>205</sup> Where the VASP is a natural person, he shall be subject to registration or license requirements in the country 'where its place of business is located', a criteria that may correspond to the primary location where the activity is performed, the business books are kept, the person resides or the server is located.<sup>206</sup> This does not prevent, however, a State from regulating foreign-located VASPs,<sup>207</sup> nor does it exclude overlapping regulations and conflicts of jurisdiction.<sup>208</sup>

The determination of the applicable law raises very practical implications in terms of cross-border cooperation. If the obliged entity is licensed and thus subject to the AML/CTF regulation of State A, it will be under the duty to report suspicious transactions to the competent authorities of that country, which will subsequently forward spontaneously or upon request the collected information to the FIU of State B. At stake is a direct access to data that enables law enforcement authorities to detect suspicious transaction and, thereby, crimes perpetrated by means of cryptocurrencies. From that perspective, the effectiveness of AML legislation within the virtual assets' economy will ultimately depend on whether that competent authority has sufficient expertise, performing analysis software, as well as adequate investigating and sanctions powers. Hence, a successful AML enforcement system ultimately rests on smooth coordination and cooperation between regulators, supervisors and law enforcement authorities throughout Europe and beyond. At a time when the EU institutions are reflecting on a common regulatory and oversight framework for crypto-assets,<sup>209</sup> a holistic approach is essential for building up a European integrated supervisory and enforcement system against criminal misuses of cryptocurrencies. Time will tell whether legislative efforts will overturn an old cyber-anarchist prophecy: is a regulatory specter haunting the crypto-world?<sup>210</sup>

---

<sup>204</sup> FATF, Recommendation 15, para 2.

<sup>205</sup> FATF, Guidance on Virtual Assets and Virtual Assets Service Providers, para. 78.

<sup>206</sup> *Ibid*, para. 79.

<sup>207</sup> For instance the US, see FinCEN Guidance, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies (9 May 2019), p. 12.

<sup>208</sup> This is of particular relevance having regards to far-reaching grounds for jurisdiction on the basis of which certain countries exert the power to investigate and prosecute offences involving cryptocurrencies. For instance, US authorities have jurisdiction over fraud perpetrated anywhere but upon the use of the US telecommunications network. This may explain the high number of criminal cases related to Bitcoin scams prosecuted in the US. See I. Plaum, E. Hateley, 'A Bit of a Problem: National and Extraterritorial Regulation of Virtual Currency in the Age of Financial Disintermediation', 45 *Georgetown Journal of International Law* (2014), p. 1203.

<sup>209</sup> See notably EBA, Report with advice for the European Commission on crypto-assets (January 2019), p. 29; ECB, 'Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures' (May 2019) pp. 28 ff.

<sup>210</sup> In the late 1980s, a member of the cyberpunk movement published the 'Crypto Anarchist Manifesto', which starts with the sentence 'A specter is haunting the modern world, the specter of crypto anarchy'. T.C. May, 'The Crypto Anarchist Manifesto' (published on 22 November 1992), < <https://www.activism.net/cypherpunk/crypto-anarchy.html>>.

# **Money Laundering using Cryptocurrency: The Case of Bitcoin!**

*By Gaspare Jucan Sicignano\**

*The bitcoin, one of the most discussed topics in recent years, is a virtual currency with enormous potential and can be used almost immediately with no intervention from financial institutions. It has spread rapidly over the last few years, and all financial and governmental institutions have warned of the risk of its use for money laundering. The paper focuses on this aspect in order to understand if any purchases of bitcoins, using illicit money, can come under the anti-money laundering criminal law.*

**Keywords:** *Bitcoin; Money laundering; Italian law; Cryptocurrency.*

## **Introduction**

The bitcoin<sup>1</sup> is a virtual, decentralised and partially anonymous currency based on cryptography and peer-to-peer technology<sup>2</sup>. With bitcoins it is possible to buy any type of good or service securely and rapidly. Transactions need not be authorised by a central entity; rather, they are validated by all users of the platform. The system is totally secure, since it is practically impossible to hack the protocol<sup>3</sup>.

Bitcoin has been much criticised over the last few years; it has quickly become public enemy number one for everything from financing terrorism to drug dealing to money laundering. It has also recently been said that bitcoin would pollute the planet due to the resources required for mining<sup>4</sup>.

This paper will attempt to analyse in depth the relationship between the bitcoin and money laundering in Italian law. It will analyse the warnings issued by authorities in various sectors, as well as the opinions expressed in Italian legal literature regarding the possibility of committing money laundering and self-laundering crimes in various operations carried out using virtual currency. Finally, it will compare the accusations levelled against Bitcoin today with those levelled against the Internet in the early 2000s.

---

\*PhD Researcher in Criminal Law, Faculty of Law, Suor Orsola Benincasa University, Naples (Italy). Email: [gasparesicignano@unisob.na.it](mailto:gasparesicignano@unisob.na.it).

\* Ph.D. Researcher in criminal law, Faculty of Law, Suor Orsola Benincasa University, Naples (Italy). Email: [gasparesicignano@unisob.na.it](mailto:gasparesicignano@unisob.na.it)

<sup>1</sup>By convention, the word "bitcoin", written in lower case, denotes the virtual currency, while the term "Bitcoin", with the initial capitalised, indicates the protocol, i.e. the technology and network used to generate and transfer money.

<sup>2</sup>Antonopoulos (2017) at 3; Wiseman (2016).

<sup>3</sup>Sicignano (2019).

<sup>4</sup>Mora, Rollins, Taladay, Kantar, Chock, Shimada & Franklin (2018) at 931-933.

## The Risk of Money Laundering

According to many commentators, the primary risk associated with the use of bitcoins is money laundering.

In the 2013 Report of the Financial Intelligence Unit of Italy (UIF), the Bank of Italy announced that investigations were ongoing regarding the potential risk of money laundering and financing terrorism via Bitcoin. In particular, the Director of the UIF stated that the urgency of further investigations was confirmed by several reports of suspicious anomalous international transactions.

The European Banking Authority (EBA), together with the European Central Bank (ECB) and the European Securities and Markets Authority (ESMA), also emphasised the risks of virtual currencies. According to the head of the Attorney General's office in Rome, Bitcoin does not offer clear traceability and can be a means of laundering money, financing terrorism and the mafias, and trafficking illegal goods<sup>5</sup>. In a bitcoin transaction there is in fact no guarantee of being able to verify the real identities of those involved.

Bitcoin may be used as a tool for criminals, terrorists, financiers, and tax evaders, according to the Financial Action Task Force (FATF), the independent inter-governmental agency that develops and promotes policies aimed at protecting the global financial system against money laundering, financing terrorists, and arms proliferation<sup>6</sup>.

The Italian agencies of the *Direzione Investigativa Antimafia* (Anti-Mafia Investigation Directorate) and the *Guardia di Finanza* (the Italian financial police) have also issued warnings on the risks connected with using bitcoins. According to a deputy national anti-mafia prosecutor, the bitcoin is an ingenious invention, “*it's just that it is a criminal invention!*”<sup>7</sup>. The commander of the Technology Fraud Unit of the *Guardia di Finanza* stated that “*money laundering lurks in that code*”<sup>8</sup>. According to the Director General of the Bank of Italy: “*Bitcoin and cryptocurrencies guarantee absolute anonymity and absolute impermeability, all of which is extraordinarily attractive for those who want to launder money*”<sup>9</sup>.

## The Crime of Money Laundering in Italian Law.

While financial authorities have warned of the risks of money laundering with bitcoin, opinions expressed in Italian legal scholarship have attempted to offer a solution to the problem by claiming that the various operations carried out using bitcoin can be included without difficulty under Italian law as part of the crimes of money laundering and self-laundering<sup>10</sup>.

---

<sup>5</sup>Quarantino (2014).

<sup>6</sup>Mincuzzi & Galullo (2017).

<sup>7</sup>Stefanini (2018).

<sup>8</sup>Bonini (2014).

<sup>9</sup>Galullo (2017).

<sup>10</sup>Bechini & Cignarella (2018); Bocchini (2017) at 46; Capaccioli (2015) at 251; Capogna, Peraino, Perugi, Cecili, Zborowski & Ruffo (2015) at 3; Danielli, Di Maio, Gendusa & Rinaldi (2018) at 13; Da Rold (2019) at 12; Di Fizio (2018) at 21; Gasparri (2015) at 3; Ingraio (2019) at 148; Majorana

In Italian law, the crime of money laundering is established by Article 648-*bis* of the Italian criminal code, which punishes the behaviour of those who, in actions distinct from participation in the predicated offence, “*substitute or transfer money, goods, or other property from an intentionally committed crime, or carry out other related operations in order to prevent identifying their criminal origin*”. Regarding the purchase of bitcoins with illicitly acquired money, such conduct would come under one of the three factual models of Article 648-*bis* of the Italian criminal code (i.e., substitution, transfer, or carrying out other activities). Under a provision making concealment behaviour regarding money, goods, or other property unlawful, Bitcoin may come under the first or the third of such typological models<sup>11</sup>.

Purchasing bitcoins using illicitly obtained money would also constitute another element of the crime referred to in Article 648-*bis* of the Italian criminal code, namely, the suitability of the behaviour to obstruct identifying the criminal origin of the goods.

From this perspective it has been stated that: “*the probability that Bitcoin will become a system for laundering international illicit proceeds will be directly proportional to its ability to hinder identification of their origin. While it is undeniable that the blockchain mechanism is a valid tool for tracking online transactions carried out using Bitcoin, it has nevertheless been shown that this chain ultimately corresponds to a purely mathematical algorithm that is not only complex to resolve but frequently difficult to trace back to a clearly identifiable physical or legal person*”<sup>12</sup>.

Thus, it would be “*misleading to argue that the a posteriori ability to reconstruct transactions and their digital agents is an absolute impediment to constituting it as a money laundering crime; in the case of virtual currencies, what is indeed not ensured is the link between the transaction addresses and the identity of those who actually control them, thus the possibility is highly developed that the transfer and the substitutions complicate identifying the criminal origins*”<sup>13</sup>.

In the case at hand, “*it is able to ‘obstruct’ the identification of the origins, be they objective or subjective, of currency and ‘assets’, without the need for absolute impossibility, or there being a definitory constraint with regard to the physical nature of the subject matter of the conduct itself, which extends far beyond the traditional sphere of ‘money’ or currencies as they are traditionally understood*”<sup>14</sup>.

It would thus be “*purely a diversionary tactic*” to object that, in reality, Bitcoin is not anonymous but pseudo-anonymous, because “*the ‘pseudonym’, or the Bitcoin account represented by a series of numbers and letters, once traced by law enforcement, does not allow any further tracing, and thus it continues to conceal the true physical identity of the identified account’s owner. Furthermore, as if that were not enough, a single physical person can actually own multiple*

---

(2018) at 630; Molinaro (2014); Naddeo (2019) at 2447; Passarelli (2016) at 12; Picotti (2018) at 599; Plantamura (2019) at 883; Pomes (2019) at 2; Razzante (2018) at 63; Sabella (2018) at 545; Simoncini (2015) at 897; Sturzo (2018) at 19; Teti (2013) at 46; Vardi (2015) at 3.

<sup>11</sup>Pomes (2019) at 160; Di Fizio (2018) at 57; Sturzo (2018) at 24; Naddeo (2019) at 106.

<sup>12</sup>Sturzo (2018) at 22.

<sup>13</sup>Di Fizio (2018) at 58.

<sup>14</sup>Picotti (2018) at 608.

*accounts and make multiple illicit transactions, each one traceable to a different account*<sup>15</sup>.

### **Our Opinion on the Risk of Money Laundering.**

There are various reasons why we are in disagreement with the considerations outlined above.

Above all, an attentive reading of the various warnings issued by the authorities in various sectors is sufficient to understand that, in many of them, either they are openly ignoring the historical and cultural context in which Bitcoin was created, or they are wildly confusing the actual characteristics of this new computer technology.

It is profoundly wrong to argue that the bitcoin was a criminal invention. Bitcoin was not created by criminals, traffickers, and/or drug dealers. It emerged from a community of computer activists called Cypherpunks who had been working on a digital money project since the 1990s. They were computer experts strongly committed to ensuring privacy; some had university experience while others were already very wealthy, thanks to the Internet. For them, anonymity was not a gimmick to escape control by police authorities but a way of countering the tyranny of surveillance.

At the same time, claiming that bitcoin does not offer clarity in tracking exchanges is to deny the way the entire system operates. All bitcoin transactions are public and are contained in a freely available distributed database. Anyone can check who sold a certain amount of bitcoins to someone else, and anyone can discover the history of every transaction. It is not particularly difficult to check which wallet contains a certain bitcoin or the route a given amount followed to arrive at a particular destination.

The same alleged anonymity that Bitcoin guarantees to its users, which so frightens the authorities in various sectors, is more legend than fact. Bitcoin is not anonymous; it is pseudo-anonymous. This means that each user is linked to a given nickname, or pseudonym, constituted by a long string of numbers that make up the address linked to a certain wallet. It follows that it is possible to identify the originator of a given operation once the pseudonym used is known.

Numerous studies have worked out various techniques to discover the users concealed behind bitcoin addresses. Suffice it to mention BitIodine, an application created by three Italian scholars, which is capable of identifying the “*addresses in clusters that could belong to the same user or group of users, classifying such users and their nicknames, and even displaying complex data extracted from the Bitcoin network*”<sup>16</sup>. Work presented by a team at the University of California produced similar results<sup>17</sup>.

Recently, a study by AgiproNews in collaboration with the Polytechnic University of Milan showed that using Bitcoin for illicit purposes is even riskier

---

<sup>15</sup>Sturzo (2018) at 31.

<sup>16</sup>Spagnuolo, Maggi & Zanero (2014) at 457.

<sup>17</sup>Meiklejohn, Pomarole, Jordan, Levchenko, McCoy, Voelker & Savage (2013).

than using electronic money or bank transfers. In particular, it emphasised that the bitcoin is one of the more traceable currencies, and that every transaction, whether licit or illicit, is always viewable at zero cost<sup>18</sup>.

The study cited a 2015 report published by HM Treasury and the UK Home Office, according to which the riskiness of cryptocurrencies for money laundering and financing terrorism was evaluated as “low.”

The same conclusion was reached in a report issued by Elliptic, a company that works with the risks of cryptocurrencies, and by the Centre on Sanctions and Illicit Financing, a programme by the Foundation for Defense of Democracies (FDD), a non-profit entity focused on foreign policies and national security. The study, which was an in-depth analysis of a narrow sample of transactions between 2013 and 2016, analysed the trends of illicit activities carried out using Bitcoin<sup>19</sup>. Yet, according to those same experts, the number of illicit operations committed using Bitcoin is quite low: around 1% of all transactions that enter the Bitcoin network.

The report takes advantage of several computer techniques that make it possible to identify suspicious bitcoin movements that involve Bitcoin forensics and Bitcoin intelligence. The former refers to “*the use of statistical tools for aggregating transactions and identifying the users*”<sup>20</sup>; the second refers to monitoring the blockchain in order to identify “*addresses at risk for money laundering*” and “*to provide a probabilistic estimate of the risk of each specific transaction*”<sup>21</sup>.

Recently, many companies have specialised in this area, including providing consulting services to law enforcement agencies. The best known among them is Neutrino s.r.l., an Italian company that evaluates the risk of money laundering of each specific bitcoin transaction. The Blockchain Intelligence Group in Vancouver is also well known, which does the same analyses as Neutrino S.r.l.<sup>22</sup>.

Thus, it does not seem like a gamble to argue that large criminal organisations still prefer dollars to Bitcoin. This is also because the bitcoin “*does not have market liquidity*” and thus could not be easily used for money laundering purposes<sup>23</sup>.

## Our Opinion on Money Laundering in Italian Law

The observations stated in Italian legal doctrine regarding the possibility of establishing the crime of money laundering do not seem convincing either.

While agreeing with the choice to classify the bitcoin as a form of “other asset”<sup>24</sup>, we do not agree with the stated reasoning with regard to the other

---

<sup>18</sup>Tripoldi (2017).

<sup>19</sup>Fanusie & Robinson (2018).

<sup>20</sup>Perugini (2018).

<sup>21</sup>Danielli, Di Maio, Gendusa & Rinaldi (2018) at 40.

<sup>22</sup>Dal Checco (2017).

<sup>23</sup>Frediani (2014).

<sup>24</sup>The term “*other asset*” seems to come closest to the concept of “*altra utilità*” used in Italian law, which uses *utilità* to refer to anything that can be used to replace what has been obtained through criminal activity.

behavioural requirement of Article 648-*bis* of the Italian Criminal Code, namely that behaviour must be carried out in such a way that it obstructs identifying the criminal origin of the laundered goods.

On this point, while noting that bitcoin transactions are perfectly traceable, it can be inferred that an obstacle exists from the fact that virtual money transactions would ensure the anonymity of the various users.

We do not agree with this point of view.

Even setting aside the fact that Bitcoin does not ensure any anonymity, as previously stated, we should recall that in the case of money laundering the obstacle should not generically be the concern of investigations, but rather identifying the criminal origin of the goods<sup>25</sup>. This means that not all obstructive activities are punishable, but only those that “*affect, either materially or legally, the “other asset” itself in some way*”<sup>26</sup>.

Legal scholars have argued that any operation that deceives or disguises reality, and which affects other aspects of the actual event, may be punished on other grounds, but such activity cannot constitute money laundering<sup>27</sup>. Someone who buys something of criminal origin, reports it to the authorities, and then assists with reconstructing its criminal origin while obstructing the search for the perpetrator, is not responsible for money laundering<sup>28</sup>.

Consequently, if concealing the origin of an asset is done by obstructing the identification of the perpetrator of a crime (the so-called “concealment of the perpetrator” of the predicated offence), this cannot be constituted as money laundering<sup>29</sup>.

Take the example of transferring a vehicle obtained fraudulently by several individuals who use a false document to take title of the vehicle, which they then sell. In this case the actions do not constitute money laundering because the actions taken to conceal reality do not regard the asset itself, but rather the perpetrators of the legal manoeuvres used to sell it<sup>30</sup>.

This principle is confirmed regarding payments using stolen bank cheques after replacing the beneficiary’s information. According to the *Corte Suprema di Cassazione* (the Supreme Court at the top tier of the Italian ordinary jurisdiction) “*when the accused only cashes cheques of illegal origin into their own bank account, after replacing the beneficiary’s information with their own and endorsing the cheque, without tampering with the information identifying the issuing bank or the serial number of the cheques, such behaviour shall not be qualified as money laundering*”<sup>31</sup>

And yet, if the problem with Bitcoin is that it ensures its users anonymity, in the light of Italian legal scholarship and the ruling just cited, it seems clear that the obstruction referred to in Article 648 of the Italian criminal code does not apply in such cases. With Bitcoin, only the concealment concerns the possible owner of the

---

<sup>25</sup>Maugeri (2016) at 140.

<sup>26</sup>Maugeri (2016) at 141.

<sup>27</sup>Razzante (2011) at 34; Faiella (2009) at 163; Magri (2007) at 442.

<sup>28</sup>Zanchetti, (1997) at 368.

<sup>29</sup>Faiella (2009) at 260.

<sup>30</sup>Razzante (2011) at 34; Magri (2007) at 455.

<sup>31</sup>Cass. Pen. sez. II, May 11, 2017, n. 30265 in *Italggiure*.

virtual money, which could be concealed by pseudo-anonymity. From a physical point of view, the asset undergoes no concealment, resulting in perfectly traceable and visible transactions.

That said, however, a clarification is required: acquiring virtual money through online transactions does not seem to constitute the crime of money laundering; however, it may do so in the case of purely cash payments.

Cyberlaundering is traditionally broken down into two types: “*instrumental cyberlaundering*” and “*online cyberlaundering*”. The former is when at least one of the three phases of laundering (placement, layering, and integration) is carried out digitally. A typical example of instrumental cyberlaundering carried out via Bitcoin is purchasing virtual money with the cash proceeds of a crime.

In online cyberlaundering, all phases in the process of laundering dirty money take place digitally. The money to be laundered is already available in digital form, and the laundering procedures tend to be quick and easy<sup>32</sup>. Online cyberlaundering takes place when purchasing virtual money with money that is already virtual.

And yet, as previously mentioned, acquiring bitcoins with money of illicit origin, according to the definition of online cyberlaundering, does not seem to obstruct identifying the criminal origin of the asset. In this particular example, the entire operation is tracked. When purchasing bitcoins, there is no obvious concealment. Normally, a purchase is paid for by wire transfer or credit card, and law enforcement agencies can very easily trace it back to the alleged crime<sup>33</sup>. If one chooses to use a virtual currency, one must provide the identity of the user, as required by recent anti-money laundering regulations (Decreto Legislativo n. 90 of 25 May 2017).

Bitcoins are registered on the blockchain, and all transactions regarding every single unit are always visible at zero cost. The system is so transparent that, once a given suspicious bitcoin has been identified, it is possible to find out who has used it: all the way back to the origin of the blockchain. A case in point is the Silk Road issue; after the arrest of the site operator, investigators followed the bitcoins to track down everyone who had any role in the online platform operating in the deep web<sup>34</sup>.

Instrumental cyberlaundering operations are a different matter. In such cases, users purchase virtual money using cash. This is not a widespread practice in the crypto-world, as cash exchanges presuppose physical encounters between the parties, and Bitcoin platform users typically interact virtually from their various corners of the world.

And yet, acquiring bitcoins using money of criminal origin from someone other than the perpetrator of the alleged crime does seem to constitute the specific case referred to in Article 648-bis of the Italian criminal code. In this case, with the transition from the physical to the virtual world, bitcoin is potentially capable of severing all links between the illicit proceeds and the alleged crime. This transition irremediably cuts off all ties between the substituted good and the predicated

---

<sup>32</sup>Simoncini (2015) at 897.

<sup>33</sup>Capaccioli (2015) at 254.

<sup>34</sup>Frediani (2018).



offence, constituting an example of actual concealment of the physical object of the crime.

In the case of a person who purchases a quantity of bitcoins using cash obtained as the result of a crime, if he or she makes the transaction by working with a private individual, without resorting to an official currency, it is not subject to any sort of control or reporting obligation.

The person could easily exchange money for bitcoins, with no tracking at all. Once the transaction has been completed, no one would be able to connect the bitcoins with the alleged crime. There would be no possible traceability of the bitcoin transactions, because the operation was anonymous at its source when the cash was converted into virtual currency.

Furthermore, since Bitcoin is based on a decentralised system incompatible with any intervention by any central authority, it ensures the impossibility of any physical goods being confiscated. Indeed, if the investigating agencies do not have individuals' passwords – or better yet, the encryption keys – of a given wallet, they cannot actually seize anything<sup>35</sup>.

Lastly, the decentralised structure of Bitcoin makes oversight extremely difficult. There is no authority to which the State can turn to order that all suspicious transactions be reported. The system is based on a peer-to-peer network automatically managed by an algorithm<sup>36</sup>.

## Conclusions

This paper has attempted to analyse the relationship between Bitcoin and money laundering in Italian law. We have sought to show that using virtual currency does not pose serious laundering risks. Indeed, in this case virtual money, rather than being a tool for criminals and launderers, would truly be a Trojan horse. If money launderers were to invest significant capital in Bitcoin, in a single blow they would risk attracting the attention of all law enforcement agencies.

This is similar to what happened with the Internet in the early 2000s. At that time many commentators decried the risk of money laundering that lurked behind using the web.

Indeed, in an interview on 11 December 2000, Edward P. Rindler, a special adviser to Bill Clinton, then President of the United States of America, argued that the Internet was the new frontier of globalised crime and explained that it was possible to launder dirty money via the web<sup>37</sup>. Alessandro Scartezzini, of the Transcrime research centre at the University of Trento, was of the same view<sup>38</sup>. According to Alessandro Pansa, the Director of the Central Operational Service of the Central Anti-Crime Directorate of the State Police, and Donato Masciandaro, a

---

<sup>35</sup>Morone (2018); Frediani (2018).

<sup>36</sup>Tamburini (2014).

<sup>37</sup>Calabrò (2000) at 17.

<sup>38</sup>Montefiori (1998) at 23.

professor at the Bocconi University of Milan, the Internet would be favourable to an increase in laundering dirty money<sup>39</sup>.

Today, however, there is unanimous belief that only the transition from cash to digital money is capable of defeating money laundering; thus the Internet has gone from being a dangerous tool to a valuable ally in the fight against money laundering. Who knows? Might something similar happen with Bitcoin?

## References

- Antonopoulos, A.M. (2017). *Mastering bitcoin: Programming the Open Blockchain*. 2<sup>nd</sup> ed. California, Sebastopol: O'Reilly Media, Inc.
- Bagnoli R. (2000). 'Il paradiso fiscale giusto? Si trova in rete'. *Corriere della Sera*, August 9, 23.
- Bechini, U. & M.C. Cignarella (2018). 'Antiriciclaggio – compravendita di immobile – pagamento del prezzo in bitcoin'. Quesito antiriciclaggio n. 3/2018 in *Consiglio Nazionale del Notariato*, March 20.
- Bocchini, R. (2017). 'Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche' in *Diritto dell'informazione e dell'informatica* 1:46.
- Bonin, C. (2000). 'L'allarme del superpoliziotto: così i boss fanno affari con Internet e l'euro'. *Corriere della Sera*, June 16, 7.
- Bonin, C. (2014). Bitcoin, l'investigatore della Finanza: "In quei codici si annida il riciclaggio". *La Repubblica*, July 10.
- Calabrò, M.A. (2000). «Un'intesa per vigilare in rete». Il consigliere di Clinton: così su Internet il riciclaggio è diventato globale'. *Corriere della Sera*, December 11, 17.
- Capaccioli, S. (2015). *Criptovalute e bitcoin: un'analisi giuridica*. Milano: Giuffrè.
- Capogna, A., Peraino, L., Perugi, S., Cecili, M., Zborowski, G. & A. Ruffo (2015). 'Bitcoin: profili giuridici e comparatistici. Analisi e sviluppi futuri di un fenomeno in evoluzione' in *Diritto Mercato Tecnologia* 3:32-74.
- Dal Checco, P. (2017). 'Nasce il Blockchain Intelligence Group Japan' in [www.Bitcoinforensics.it](http://www.Bitcoinforensics.it), 27 aprile 2017.
- Danielli, A., Di Maio, D., Gendusa, M. & G. Rinaldi (2018). *Bitcoin e Criptovalute. Funzionalità e rischi delle monete virtuali*. Montecatini Terme: Altalex.
- Da Rold, M. (2019). 'Innovazione tecnologica ed implicazioni penalistiche. Le monete virtuali' in *Giurisprudenza penale web* 2:12.
- Di Fizio, F. (2018). 'Le cinte diziarie del diritto penale alla prova delle valute virtuali degli internauti' in *Diritto penale contemporaneo, rivista trimestrale* 10:21-81.
- Faiella, S. (2009). *Riciclaggio e crimine organizzato transnazionale*. Milano: Giuffrè.
- Robinson & Fanusie (2018). "Bitcoin Laundering: an analysis of illicit flows into digital currency service". *Defenddemocracy.org.*, January 12.
- Frediani, C. (2014). 'Bitcoin non è il paradiso dei terroristi e della criminalità organizzata'. *Wired.it*, July 11.
- Galullo, R. (2017). 'Padoan: "Le mafie sguazzano nella finanza opaca'. *Il sole 24 ore.it*, November 24.
- Gasparri, G. (2015). 'Timidi tentativi giuridici di messa a fuoco del Bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?' in *Diritto dell'informazione e dell'informatica (II)* 3:415-442

<sup>39</sup>Bonin (2000) at 7; Bagnoli (2000) at 23.

- Ingrao, C. (2019). 'Gli strumenti di prevenzione nazionali ed europei in materia di valute virtuali e riciclaggio' in *Diritto penale contemporaneo, rivista trimestrale* 2:148-158.
- Magri, P. (2007). *I delitti contro il patrimonio mediante frode*. Padua: Cedam.
- Majorana, D. (2018). "Disciplina giuridica e fiscale delle criptovalute: sfida al legislatore dal web" in *Corriere tributario* 8:630-636.
- Maugeri, A.M. (2016). 'L'autoriciclaggio dei proventi dei delitti tributari: ulteriore espressione di voracità statale o utile strumento di politica criminale?' in E. Mezzetti & D. Piva (eds.) *Punire l'Autoriciclaggio. Come, quando e perché*. 100-140. Torino: Gappicelli.
- Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M. & S. Savage (2013). 'A Fistful of Bitcoins: Characterizing Payments Among Men with No Names' in *Proceedings of the 2013 Conference on Internet Measurement, ACM*. <https://doi.org/10.1145/2504730.2504747> (pp. 127-139).
- Mincuzzi, A. & R. Galullo (2017). 'Bitcoin, il riciclaggio invisibile di mafie e terrorismo internazionale'. *Il sole 24 ore.it*, February 7.
- Molinaro, G. (2014). 'Sono tassabili le manifestazioni di capacità economica emergenti nelle operazioni relative a bitcoin?' in *Il Fisco* 25:2447.
- Montefiori, S. (1998). 'Casinò nuova mania su Internet'. *Corriere della Sera*, December 7, 23;
- Mora C., Rollins R.L., Taladay K., Kantar M.B., Chock M.K., Shimada, M. & E.C. Franklin (2018). 'Bitcoin emissions alone could push global warming above 2°C' in *Nature Climate Change* 8:931-933.
- Morone, R.M. (2018). 'Bitcoin e successione ereditaria: profili civili e fiscali' in *Giustizia civile.com*, 2/2018:1-12, February 23.
- Naddeo, M. (2019). 'Nuove frontiere del risparmio, Bit Coin Exchange e rischio penale' in *Diritto penale e processo* 1:101.
- Passarelli, N. (2016). 'Bitcoin e antiriciclaggio' in *Sicurezza.gov.it*, November 15.
- Perugini, M.L. (2018). *Distributed Ledger Technologies e sistemi di Blockchain: Digital Currency, Smart Contract e altre applicazioni*. Vicalvi: Key.
- Picotti, L. (2018). 'Profili penali del cyberlaundering: le nuove tecniche di riciclaggio' in *Rivista trimestrale di diritto penale dell'economia* 3-4:590-619.
- Plantamura, V. (2019). 'Il Cybericiclaggio' in A. Cadoppi., S. Canestrari, A. Manna & M. Papa (eds.) *Trattato di Diritto penale, Cybercrime*, 850-890. Torino: Utet.
- Pomes, F. (2019). 'Le valute virtuali e gli ontologici rischi di riciclaggio: tecniche di repressione' in *Diritto penale contemporaneo, rivista trimestrale* 2:159-176
- Quarantino, E. (2014). 'Allarme del Pg di Roma, da bitcoin rischi riciclaggio e terrorismo' in *Ansa.it*, July 9.
- Razzante, R. (2011). *Il riciclaggio nella giurisprudenza. Normativa e prassi applicative*. Milano: Giuffrè.
- Razzante, R. (2018). 'L'utilizzo illecito delle monete virtuali' in R. Razzante *Bitcoin e criptovalute-Profilo fiscali, giuridici e finanziari*. Rimini: Maggioli.
- Sabella, P.M. (2018). 'Vendita di società "ready made" ed obblighi di verifica della clientela nella disciplina sulla prevenzione di riciclaggio e finanziamento del terrorismo: contrasto all'anonimato e valute virtuali. Nota a C.G.U.E Grande sezione 17 gennaio 2018 (causa C-676/16)' in *DPCE online*, 2: 545.
- Sicignano, G.J. (2019). *Bitcoin e riciclaggio*. Torino: Giappicelli/.
- Simoncini, E. (2015). 'Il cybelaundering: la nuova frontiera del riciclo' in *Rivista trimestrale di diritto penale dell'economia* 4:897-915.
- Spagnuolo, M., Maggi, F. & S. Zanero (2014). 'Extracting Intelligence from the Bitcoin Network' in *Financial Cryptography and Data Security: 18th International Conference, FC*: 457-468. Heidelberg: Springer.

- Stefanini, M. (2018). 'Il bitcoin? Un'invenzione criminale'. *Il foglio.it*, April 10.
- Sturzo, L. (2018). 'Bitcoin e riciclaggio 2.0' in *Diritto penale contemporaneo* 5: 19-34.
- Tamburini, F. (2014). 'Bitcoin, oltre 2 milioni e mezzo di persone nel mondo usano la moneta virtuale'. *Il fatto quotidiano.it*, April 26.
- Teti, A. (2013). 'Bitcoin: la criptomoneta del cyberspazio che sfida banche e governi' in *Mondo Digitale* 46:1-16.
- Tripodi, A. (2017). Gaming, la "nuova era" del Bitcoin. Gli esperti: rischio riciclaggio resta basso'. *Il sole 24 ore.it*, October 5.
- Vardi, N. (2015). ' "Criptovalute" e dintorni: alcune considerazioni sulla natura giuridica dei bitcoin' in *Diritto dell'informazione e dell'informatica* 3:443-456
- Wiseman, S. (2016). 'Property or Currency? The Tax Dilemma Behind Bitcoin' in *Utah Law Review* 2016(2):416-440
- Zanchetti, M. (1997). *Il riciclaggio di denaro proveniente da reato*. Milano: Giuffrè.





# BITCOIN: THE DECENTRALISED VIRTUAL CURRENCY AS A CRIMINAL TOOL



**Dániel Eszteri,**  
Dr, Criminal Case Administrator, Budapest Police Headquarters' Cybercrime Unit

## INTRODUCTION

In January 2009, the Japanese software designer Satoshi Nakamoto invented a virtual currency named Bitcoin and released software for managing transactions in the new money <sup>(1)</sup>.

It consists solely of bits and bytes, but we cannot see it as a coin or banknote on the market. There is no cover in terms of gold or stocks, in fact, nothing but the source code of the software which consists of 31 000 lines of code <sup>(2)</sup>. The payment system is completely decentralised and so contains no central organisation which monitors transactions. Many people use this new currency to pay for services or products on the Internet, since it is not less safe than traditional payment systems.

The anonym currency can be a perfect tool in the hands of criminals to reach their goals. Law enforcement authorities like the FBI have dealt with the question in a long report that recently leaked to the Internet <sup>(3)</sup>. It can be interesting to examine the 'Bitcoin problem' from this point of view too, because the anonymous money transferring possibility seems to be the root of money laundering at first sight.

## THE ESSENTIAL CHARACTERISTICS OF BITCOIN

Bitcoin is not a concrete, physically existing currency, but virtual money: an amount associated with a so-called virtual wallet. First, we have to download software from the Internet, which is also called Bitcoin. We can find this on the official homepage of the virtual currency <sup>(4)</sup>.

This software functions as a digital wallet on our computer after installation and stores our virtual money. Our wallet is nothing but a file on our hard drive named 'wallet.dat' <sup>(5)</sup>. Bitcoin software is open-source, available for almost every operating system, updated regularly and contains every necessary function for sending and receiving Bitcoin.

## ADVANTAGES AND DANGERS OF THE LACK OF CENTRAL CONTROL

Due to the Bitcoin network feature that users give no personal information about themselves and that there is no central control authority behind the system, the identification of

<sup>(1)</sup> Nakamoto, S., 'Bitcoin: A Peer-to-Peer Electronic Cash System', <http://bitcoin.org/bitcoin.pdf> (1.6.2013).

<sup>(2)</sup> Davis, J., 'The Crypto-Currency', [http://www.newyorker.com/reporting/2011/10/10/111010fa\\_fact\\_davis](http://www.newyorker.com/reporting/2011/10/10/111010fa_fact_davis) (2.6.2013).

<sup>(3)</sup> Federal Bureau of Investigation (2012), 'Intelligence assessment: Bitcoin virtual currency: Unique features present distinct challenges for deterring illicit activity', <http://cryptome.org/2012/05/fbi-bitcoin.pdf> (31.5.2013).

<sup>(4)</sup> Bitcoin webpage, <http://bitcoin.org/> (4.6.2013).

<sup>(5)</sup> Bitcoin on Wikipedia, <https://en.bitcoin.it/wiki/Wallet> (4.6.2013).



suspicious transactions and users or obtaining transaction logs seems impossible at first sight. Nevertheless, the network has features which can help us track transactions and link them to someone. First, every transfer is public and can be seen on <http://www.blockexplorer.com> or <http://blockchain.info> websites<sup>(6)</sup>. We do not have to request transaction records from authorities or financial institutions, since they can be browsed freely on the Internet. Every single transfer made by a suspected Bitcoin address can be followed along the chain.

However, it is not guaranteed that the person behind a transfer can be identified since the information includes no personal data — especially not the sender's or receiver's IP address — but merely the amount transferred between two public keys.

We have to keep in mind that most people use Bitcoin as a simple, anonymous, online payment tool and not as a currency to replace real world money. Most users buy Bitcoin for a certain purpose (for example to buy something in a web shop), but sooner or later they change back to real world currencies.

Official currencies can be changed to Bitcoin and back on some special exchange websites, such as the Japan-based MtGox (<http://mtgox.com>). To use services offered by the website, users have to register an account and give it an account name, password and e-mail address. This information can be a good starting point for further identification. The operators of the website could confirm whether or not someone is the user of a certain Bitcoin address registered on their website. If the answer is yes, they could provide further information, such as the registered account name, e-mail address, or IP-addresses used during logins<sup>(7)</sup>. There are also exchange sites which ask for the bank account numbers of users, and so the service providers can transfer the amount changed in real world money. A bank account's transactions and documents concerning the owner of the account mostly provide enough information to identify a person.

According to the FBI, it is good to keep in mind that some users publish their Bitcoin addresses on online forums in their comments.

## MONEY LAUNDERING WITH VIRTUAL CURRENCIES

It seems that Bitcoin could be an ideal tool to hide money made by committing a crime — money laundering — because of the anonymous paying opportunity and the absence of transaction costs. It is possible since such attempts happened recently with other virtual currencies, like a currency of an online game that is used to buy virtual items on the game's marketplace.

One good example is when an online, organised crime group changed their crime-related money to an online game's virtual currency on a special exchange website. Later they bought several virtual items (like virtual swords or armours) using the virtual world's in-game market and sold them to other players for real-world 'clean money'. Popular in-game currencies can be changed to real world money on several websites. There are also online games where the developers have made it possible to exchange virtual money for real currencies via the game clients themselves (for example 'Linden Dollars' in life-simulator 'Second Life' or 'gold' in the fantasy role-playing game 'Diablo III').

Coming back to our original topic, it is possible (criminally) to commit money laundering when someone uses Bitcoin exchange as a *modus operandi*. Someone changes criminally acquired money to Bitcoin and then forwards this to various addresses. However, it is possible to track the transactions because they are public and can be accessed by everyone on the Internet. Information could also be available in the log files of exchange websites where people can change their Bitcoin to real-world currencies.

## BITCOIN THEFT

Bitcoin represents a certain value on the Internet, and we should thus keep in mind that it could be a possible target for thieves, as real-world money is.

The most important factor in these abuses is the virtual wallet file (wallet.dat) which contains the

<sup>(6)</sup> Nakamoto, S., *supra nota* 1, p. 6.

<sup>(7)</sup> Federal Bureau of Investigation, Intelligence Assessment, *supra nota* 3, p. 10.



actual amount of a user's Bitcoin. If someone deletes this file — and no backup has been made — the user could lose access to the Bitcoin forever. Bitcoin will not be deleted from the system, but the user loses the public and private key pairs which are crucial for access and transactions.

A more sophisticated criminal behaviour is when somebody steals virtual money, not directly, but by trying to impact other computers to mine Bitcoin, creating a Bitcoin-miner zombie network without the permission and knowledge of the owners of participating computers. Computer networks created with such illegal intent are called botnets. At first the cybercriminal needs to install a virus on the target computer that uses its video card's or CPU's computing power to mine Bitcoin. This can be achieved most easily by spams (unsolicited bulk messages) or phishing websites.

An example of this phenomenon was the malware named *ZeUs*, which used the computer's resources to illegally mine Bitcoin. This harmful software spread through deceptive advertisements posted to various websites in the first half of 2011 <sup>(8)</sup>.

Other sources mention that larger computer networks would be ideal for cybercriminals for joint Bitcoin-mining (e.g. a company's or a university's local network). This technique is more expedient, because effective mining typically requires excessively high calculating power <sup>(9)</sup>.

## BUYING ILLEGAL GOODS WITH BITCOIN

There are several pages on the Internet where Bitcoin can be used as a paying option. We can browse clothes, books, trinkets, or computer parts <sup>(10)</sup>.

According to an article published on *gawker.com* on 1 June 2011, there is a webpage where we can buy any drug imaginable. The page is called *SilkRoad* and can be visited only through a special anonymous browser called *Tor (The Onion Router)*. After some search and registration effort we can look at the world's largest drug market, where we can order anything from marijuana to heroin or cocaine! However, drugs are not the only things that can be purchased: we also find tools for growing or producing drugs; we can even order ammunition, registration codes for websites, licences, etc., all of which can only be purchased with one type of currency: Bitcoin <sup>(11)</sup>.

Sadly, virtual money can be an excellent tool for criminal activities, because it is nearly impossible to trace who sent what amount to whom.

## CONCLUSION

The technology behind the virtual currency is a novelty which means a paradigm shift without parallel among financial systems, and it is still unclear what may become of it, since the tools necessary for its greater evolution are still under development.

It is presently very difficult to form an opinion of this virtual phenomenon's future since it is too new to interpret it clearly. We have to pay close attention not just to the decentralised virtual currency, Bitcoin, and its role in future crimes, but to other (centralised) types of virtual money-like currencies of online games to handle possible dangers suitably. We have to keep in mind that virtual currencies and items represent a real product in the online world and have value in physical world's money too. My essay was written to serve this goal.

<sup>(8)</sup> Segura, J., 'Zeus, Bitcoin and the Ub3erhackers', <http://blog.sparktrust.com/?p=572> (11.6.2013).

<sup>(9)</sup> Bitcoin forum, <https://bitcointalk.org/index.php?topic=11506.0> (11.6.2013).

<sup>(10)</sup> Bitcoin wiki, <https://en.bitcoin.it/wiki/Trade> (13.6.2013).

<sup>(11)</sup> Fischermann, T., 'Anarcho-Geld', <http://www.zeit.de/2011/27/Internet-Bitcoins> (10.6.2013).







UNIVERSITÉ PARIS 1  
**PANTHÉON SORBONNE**

---

**LA LUTTE CONTRE LE BLANCHIMENT DE CAPITAUX  
A L'ÉPREUVE DES CRYPTO-ACTIFS**

Master 2 de Droit Pénal International et des Affaires  
Année universitaire 2019 - 2020

Alexandra PUERTAS

Sous la direction de Monsieur le Professeur Pascal BEAUVAIS,  
Agrégé de droit privé et sciences criminelles,

et de Monsieur Jacques MARTINON, Chef de la mission de lutte  
contre la cybercriminalité à la Direction des Affaires Criminelles et des  
Grâces



*L'Université Paris 1 n'entend donner aucune approbation aux opinions émises dans ce mémoire. Ces opinions doivent être considérées comme propres à leur auteur.*

Les données chiffrées présentes dans ce mémoire sont le fruit du croisement de diverses études portant sur le sujet et dont les références figurent en bibliographie. Elles ont pour objet de donner au lecteur un ordre d'idée des phénomènes étudiés dans la présente contribution.

La nature décentralisée des crypto-actifs combinée à l'évolution rapide et permanente de leurs usages appellent le lecteur à prendre ces chiffres avec prudence.



## REMERCIEMENTS

J'adresse mes remerciements à **Monsieur Pascal Beauvais** pour sa bienveillance, ses conseils avisés et la confiance qu'il m'a accordé dans le choix de ce sujet.

Mes remerciements vont également à **Monsieur Jacques Martinon** pour le partage de son expérience judiciaire qui a contribué à enrichir mes réflexions.

Je tiens par ailleurs à remercier **Monsieur Jérémy Azencoth**, **Monsieur Kévin Dubois**, **Monsieur Jean-Luc Houel**, **Monsieur William O'rorke**, **Monsieur Thierry Pezenec**, **Monsieur Frédéric Pierson**, **Monsieur Hervé Putigny**, **Monsieur Alexandre Stachtchenko**, et **Monsieur Éric Vernier** pour les entretiens qu'ils m'ont accordés.

Enfin, j'ai une pensée toute particulière pour **mes proches**, notamment **mes parents** sans qui je n'en serai pas là aujourd'hui.



## ABRÉVIATIONS UTILISÉES

<b>ACPR</b>	Autorité de Contrôle Prudentiel et de Résolution
<b>AGRASC</b>	Agence de Gestion et de Recouvrement des Avoirs Saisies et Confisqués
<b>AMF</b>	Autorité des Marchés Financiers
<b>ANSSI</b>	Agence Nationale de la Sécurité des Systèmes d'Information
<b>CEDH</b>	Cour Européenne des Droits de l'Homme
<b>CJUE</b>	Cour de Justice de l'Union Européenne
<b>C. mon. fin</b>	Code monétaire et financier
<b>C. pén.</b>	Code pénal
<b>C. proc. pén.</b>	Code de procédure pénale
<b>CSPN</b>	Certification de Sécurité de Premier Niveau
<b>FICOBA</b>	Fichier National des Comptes Bancaires et Assimilés
<b>GAFI</b>	Groupe d'Action Financière
<b>IP</b>	Protocole Internet ( <i>Internet Protocol</i> )
<b>ICO</b>	Offre au public de jetons ( <i>Initial Coin Offering</i> )
<b>IPO</b>	Introduction en bourse ( <i>Initial Public Offering</i> )
<b>LCB</b>	Lutte Contre le Blanchiment
<b>OCDE</b>	Organisation de Coopération et de Développement Économiques
<b>STO</b>	Offre de Jeton de Sécurité ( <i>Security Token Offering</i> )
<b>TOR</b>	Routeur en Oignons ( <i>The Onion Routers</i> )
<b>UE</b>	Union Européenne

**VPN**

Réseau Privé Virtuel (*Virtual Private Network*)





# SOMMAIRE

<b>Remerciements</b>	<b>5</b>
<b>Abréviations utilisées</b>	<b>7</b>
<b>Introduction</b>	<b>12</b>
<b>I. La prévention du blanchiment au moyen de crypto-actifs</b>	<b>28</b>
A. L'assujettissement des prestataires de services sur actifs numériques aux obligations de lutte contre le blanchiment	36
B. L'assujettissement des offres au public de jetons aux obligations de lutte contre le blanchiment	41
<b>II. L'incrimination du blanchiment au moyen de crypto-actifs</b>	<b>48</b>
A. Les éléments constitutifs	48
B. Les processus infractionnels	55
<b>III. La répression du blanchiment au moyen de crypto-actifs</b>	<b>72</b>
A. Le régime juridique	72
B. Les saisies pénales et la peine de confiscation	75
<b>Conclusion</b>	<b>83</b>
<b>Bibliographie</b>	<b>84</b>
<b>Liste des personnes interrogées</b>	<b>91</b>



## Introduction

**1. – Définition fonctionnelle de la monnaie** – Théorisée par Aristote au IV<sup>ème</sup> siècle avant notre ère<sup>1</sup>, la monnaie remplit trois fonctions fondamentales complémentaires. Elle est : une unité de compte (1), à l'aune de laquelle il est possible de mesurer des biens hétérogènes au moyen d'un unique étalon ; un moyen d'échange (2), en ce qu'elle est universellement acceptée comme instrument de paiement ; une réserve de valeur (3) permettant à ses utilisateurs de reporter leur pouvoir d'achat dans le temps, « *une sorte de gage, donnant l'assurance que l'échange sera possible si jamais le besoin s'en fait sentir*<sup>2</sup> ». Pour remplir ces fonctions, la monnaie doit reposer sur un consensus social : la croyance dans son pouvoir libérateur.

**2. – De la valeur à la confiance** – La forme de la monnaie a évolué au cours des siècles, passant de l'utilisation de coquillages, les cauris - première monnaie ayant circulé au-delà des frontières<sup>3</sup> - aux pièces et billets. Sa fonction est pourtant restée la même. Aujourd'hui, comme hier, elle est une contrepartie acceptée par tous. Cependant, la fin de la convertibilité des monnaies en or<sup>4</sup> nous invite à nous interroger. Nos économies modernes sont fondées sur une monnaie fiduciaire et scripturale n'ayant aucune valeur intrinsèque. Dès lors, quelle est la raison d'être de notre croyance en sa valeur ? La réponse n'est autre que la confiance universelle et tacite que nous lui accordons.

**3. – Origine des crypto-actifs** – Cette confiance commune n'est cependant pas aveugle. Elle fût fortement entachée à la suite de la crise des *subprimes*. C'est dans ce contexte que le premier crypto-actif mondial a vu le jour. Le 1<sup>er</sup> novembre 2008, un dénommé Satoshi Nakamoto, annonça la publication d'un livre blanc décrivant « un nouveau système de paiement électronique entièrement de pair à pair, sans tiers de confiance<sup>5</sup> ».

---

<sup>1</sup> ARISTOTE, *Ethique à Nicomaque*, Jules Tricot (trad.), Paris, Vrin, 1990, p. 240-244.

<sup>2</sup> ARISTOTE, *La Politique*, Jules Tricot (trad.), Paris, Vrin, 1962, p. 57-58.

<sup>3</sup> Les traces les plus anciennes de l'utilisation des cauris comme moyen de paiement, représentées sur des objets en bronze découverts en Chine, remontent au 13<sup>e</sup> siècle avant notre ère. Ces coquillages provenant essentiellement des eaux chaudes de l'Océan Indien et Pacifique ont circulé en Aise, en Afrique, en Océanie, allant jusqu'à atteindre l'Europe. VAN DAMME Ingrid, « Une monnaie singulière, le cauri », sur *Musée de la Banque nationale de Belgique* [en ligne], publié le 11 janvier 2007, [consulté le 11 mars 2020], <https://www.nbbmuseum.be/fr/2007/01/cowry-shells.htm>.

<sup>4</sup> La fin de la convertibilité du franc français en or date de 1936, suivi par le dollar américain le 15 août 1971.

<sup>5</sup> NAKAMOTO Satoshi, *Bitcoin P2P e-cash paper* [courriel], 1<sup>er</sup> novembre 2008 sur The Cryptography Mailing List.

**4. – Le technologie blockchain** – La majorité des crypto-actifs fonctionnent grâce à un protocole sous-jacent appelé *blockchain* ou chaîne de blocs. La *blockchain* est une technologie de stockage et de diffusion d'informations de pair à pair, c'est-à-dire sans entité centrale<sup>6</sup>. Elle permet à ses utilisateurs, les *nœuds*, de se transférer directement des données et ce, de manière irrémédiable. Les transactions effectuées sont alors regroupées en blocs horodatés<sup>7</sup>, classés les uns après les autres ce qui forme la *blockchain*<sup>8</sup>.

#### Représentation d'une blockchain



**Source :** BLOCKCHAIN FRANCE, « Qu'est-ce que la blockchain ? », sur *Blockchain France* [en ligne], <https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/>.

**5. – Fonctionnement de la blockchain** – Concrètement, la *blockchain* est une sorte de registre qui retrace toutes les transactions effectuées entre ses utilisateurs depuis sa création. Pour qu'une transaction soit effective, elle doit être contenue dans un bloc ajouté à la chaîne<sup>9</sup>. Cette opération dénommée *minage*, en référence aux mines d'or, est réalisée par certains utilisateurs du réseaux, les *mineurs*<sup>10</sup>. Ces derniers emploient la puissance de calcul de leurs ordinateurs pour trouver un identifiant unique qui permettra de connecter le bloc à la chaîne en contrepartie de l'attribution de nouvelles unités

<sup>6</sup> BLOCKCHAIN FRANCE, « Qu'est-ce que la blockchain ? », sur *Blockchain France* [en ligne], [consulté le 13 mars 2020], <https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/>.

<sup>7</sup> La blockchain horodatée fût théorisée pour la première fois par Stuart Haber et W. Scott Stornetta en 1991. HABER Stuart et STORNETTA W. Scott, « How to time-stamp a digital document », *Journal of Cryptology*, janvier 1991, n°3, p. 99-111.

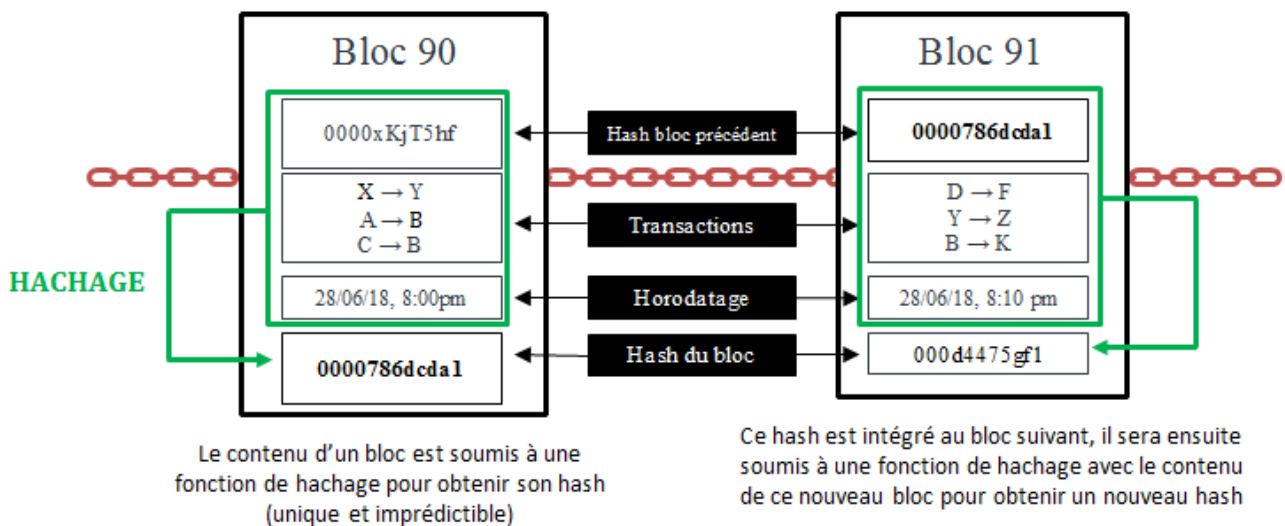
<sup>9</sup> BLOCKCHAIN FRANCE, « Qu'est-ce que la blockchain ? », sur *Blockchain France* [en ligne], [consulté le 13 mars 2020], <https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/>.

<sup>10</sup> FAURE-MUNTIAN Valéria, GANAY Claude, LE GLEUT Ronan, *Les enjeux technologiques des blockchain*, Rapport au nom de l'office parlementaire d'évaluation des choix scientifiques et technologiques, Assemblée nationale, 20 juin 2018, p. 36-37.

de crypto-actifs. Cet identifiant dénommé *hash* n'est rien d'autre que la compression de l'ensemble des données numériques qu'il contient<sup>11</sup>.

Les transactions émises sur la blockchain sont stockées suivant une structure appelée *arbre de hachage*<sup>12</sup> qui a pour principal intérêt de les lier entre elles. En effet, le *hash* d'un bloc est déterminé en fonction du *hash* du bloc précédent. Puisque chaque bloc renferme le résumé de l'ensemble des transactions contenues dans les blocs qui le précède, la blockchain est en principe infalsifiable.

### La structure d'une blockchain et le rôle des hashes



**Source :** FAURE-MUNTIAN Valéria, GANAY Claude, LE GLEUT Ronan, *Les enjeux technologiques des blockchain*, Rapport au nom de l'office parlementaire d'évaluation des choix scientifiques et technologiques, Assemblée nationale, 20 juin 2018, p. 31.

En outre, la fonction de *hachage* permet aux *mineurs* de remonter rapidement l'historique des transactions afin de s'assurer qu'un utilisateur ne procède pas deux fois à une même transaction. Ce mécanisme de vérification appelé *Unspent Transaction Output (UTXO)* résout le problème des doubles dépenses. Une fois *miné* selon une méthode cryptographique propre au type de blockchain<sup>13</sup>, le bloc

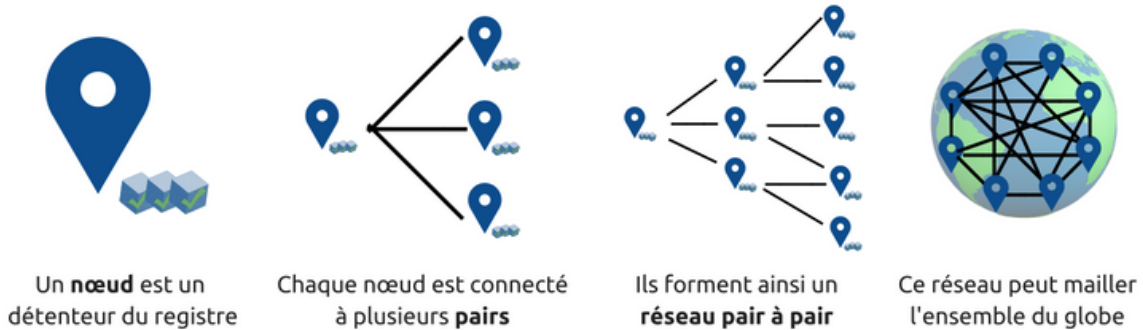
<sup>11</sup> *Ibid.*, p. 26-32.

<sup>12</sup> Les arbres de Merkle ou arbres de hachage ont été inventés par Ralph Merkle en 1979.

<sup>13</sup> Il existe deux méthodes pour créer de nouveaux blocs dans une chaîne, la plus répandue est connue sous le nom de *Proof-of-Work*, tandis que l'autre est dénommée *Proof-of-stack*.

est transmis par le *mineur* à ses *nœuds pairs*, c'est-à-dire aux détenteurs du registre avec lesquels il est connecté.

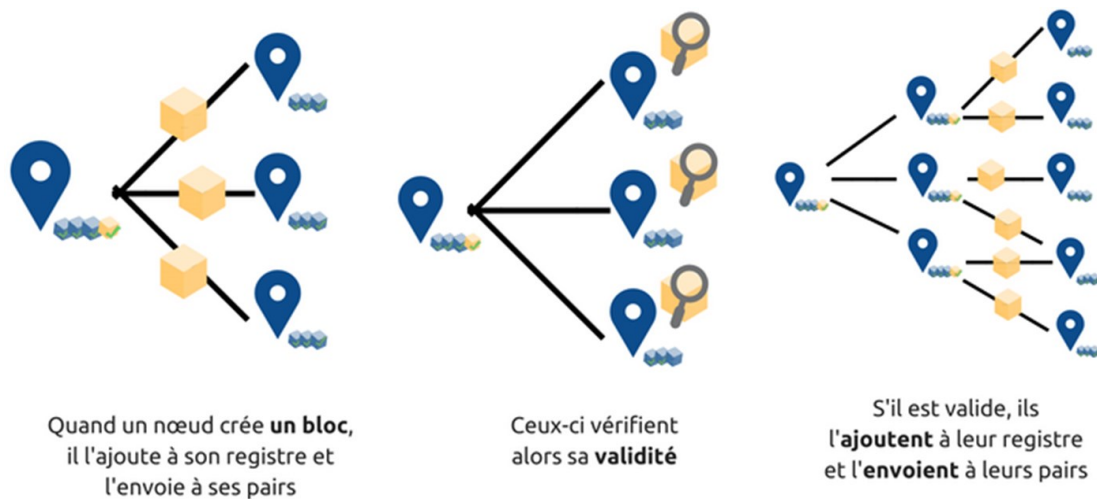
### Représentation d'un réseau de pair à pair



**Source :** *Les enjeux technologiques des blockchain*, Rapport au nom de l'office parlementaire d'évaluation des choix scientifiques et technologiques, Assemblée nationale, 20 juin 2018, p. 33.

Chaque *nœud* vérifie alors la validité du bloc, l'intègre à sa copie du registre et le transmet à son tour à ses *pairs*.

### La diffusion d'un bloc dans un réseau de pair à pair



**Source :** *Les enjeux technologiques des blockchain*, Rapport au nom de l'office parlementaire d'évaluation des choix scientifiques et technologiques, Assemblée nationale, 20 juin 2018, p. 34.

Une fois le consensus distribué entre les nœuds du réseau, le bloc est horodaté et ajouté à la chaîne de blocs à laquelle tous les utilisateurs ont accès. La blockchain est donc une grande base de données transparente, sécurisée et décentralisée où sont enregistrées toutes les opérations réalisées depuis son lancement.

**6. – Ampleur et avantages des crypto-actifs** – L’innovation technologique nous invite à repenser notre système financier. Elle offre la perspective d’une nouvelle relation de confiance fondée sur la preuve cryptographique communément admise par ses utilisateurs. Aujourd’hui, il existe plus de 5 563 crypto-actifs pour une capitalisation totale de près de 277 milliards de dollars<sup>14</sup>. Si cette dernière demeure négligeable comparativement à la masse monétaire mondiale (environ 13 000 milliards d’euros, rien que dans la zone euro, selon l’agrégat M3), certains acteurs y voient une technologie à même de soutenir l’innovation et l’inclusion financière. La démocratisation de l’usage des crypto-actifs porte en effet la promesse d’un accès simple et à moindre coût aux services financiers, par internet et mobile, sans compte bancaire traditionnel. En outre, le caractère décentralisé de la technologie blockchain permet des transactions plus rapides et moins coûteuses. Selon diverses études reprises par l’Autorité Bancaire Européenne (ABE), les frais de transaction moyens sur le protocole Bitcoin<sup>15</sup> avoisinent les 1% du montant des transactions<sup>16</sup>, là où ce taux s’élève à 6,87 % pour les transactions bancaires et 7,04 % pour les transferts d’argent liquide<sup>17</sup>. De plus, les transactions transfrontalières en crypto-actifs ne sont pas soumises aux frais de change. Enfin, la technologie blockchain élargit le champ des possibles en matière d’accès au financement en permettant des levées de fonds internationales et sans intermédiaire, dites Initial Coin Offering<sup>18</sup> (ICO).

---

<sup>14</sup> COINMARKETCAP, All cryptocurrencies, sur *Coinmarketcap* [en ligne], [consulté le 10 juin 2020], <https://coinmarketcap.com/all/views/all/>.

<sup>15</sup> Bitcoin avec une majuscule désigne le réseau Bitcoin, tandis que bitcoin sans majuscule est utilisé pour désigner les bitcoins en tant que cryptos-actifs.

<sup>16</sup> AUTORITE BANCAIRE EUROPEENNE, *Opinion on ‘virtual currencies’*, 4 juillet 2014, p. 16.

<sup>17</sup> BANQUE MONDIALE, *Remittance Prices Worldwide*, mars 2020, p. 12.

<sup>18</sup> Une offre au public de jetons est une opération de levée de fonds, effectuée sur une blockchain, par laquelle un porteur de projet ayant besoin de financement émet des jetons appelés *tokens* auxquels des investisseurs souscrivent généralement en crypto-actifs. Ces jetons peuvent accorder à leur détenteur un droit d’user des produits ou services du porteur de projet (*utility token*) ou lui offrir des droits financiers et/ou politiques tels que des droits de vote (*security token*). Ces jetons peuvent ensuite être revendus sur un marché secondaire à des fins spéculatives.



**7. – Définition** – Un crypto-actif est avant tout un actif virtuel, c'est-à-dire « *une représentation numérique de valeur qui peut être négociée numériquement*<sup>19</sup> ». Il se distingue de la « *représentation numérique de la monnaie fiduciaire*<sup>20</sup> » utilisée pour transférer électroniquement une somme d'argent ayant cours légal, dit e-argent, en ce qu'il n'a pas de valeur légale dans toute juridiction. En outre, les crypto-actifs ont deux caractéristiques qui leur sont propres. D'une part, ils sont convertibles, ce qui signifie qu'ils peuvent être échangés dans les deux sens contre une monnaie ayant cours légal<sup>21</sup>. D'autre part, ils fonctionnent de manière décentralisée<sup>22</sup>, placés sous la protection de la cryptographie.

En droit interne, les crypto-actifs ont été définis pour la première fois dans le cadre du dispositif de lutte contre le blanchiment et le financement du terrorisme. L'article L. 561-2 du Code monétaire et financier fût réécrit par l'ordonnance du 1<sup>er</sup> décembre 2016 afin d'élargir le domaine des assujettis aux obligations de lutte contre le blanchiment. Les actifs numériques étaient alors définis comme : « *tout instrument contenant sous forme numérique des unités de valeur non monétaires pouvant être conservées ou être transférées dans le but d'acquérir un bien ou un service, mais ne représentant pas de créance sur l'émetteur* ».

La création, par la loi de finances pour 2019, d'un régime d'imposition des plus-values résultant de la cession de crypto-actifs par des particuliers fit évoluer cette définition. L'article 150 VH bis du Code général des impôts s'efforça de distinguer deux nouveaux actifs numériques : les jetons et les coins. Ces derniers furent définis comme : « *toute représentation numérique d'une valeur qui n'est pas émise ou garantie par une banque centrale ou par une autorité publique, qui n'est pas nécessairement attachée à une monnaie ayant cours légal et qui ne possède pas le statut juridique d'une monnaie, mais qui est acceptée par des personnes physiques ou morales comme un moyen d'échange et qui peut être*

---

<sup>19</sup> GAFI, *Virtual currencies: Key definitions and potential AML/CFT Risks*, juin 2014, p. 4.

<sup>20</sup> *Ibid.*

<sup>21</sup> La notion de monnaie convertible ne signifie pas que la convertibilité est garantie par la loi. En effet, sa convertibilité est conditionnée à l'existence d'une offre et d'une demande sur un marché.

<sup>22</sup> Les crypto-actifs se distinguent donc des actifs virtuels centralisés, c'est-à-dire émis et contrôlés par un administrateur, tels que ceux utilisés dans des jeux en ligne massivement multijoueur (Linden Dollar pour le jeu Second Life) ou sur des plateformes de e-commerce (Amazon Coins). L'utilisation de ces actifs à des fins de blanchiment ne sera pas traitée dans la présente contribution mais reste avérée. CHAMBRE DE COMMERCE INTERNATIONALE, « Virtual money laundering threat identified », sur *Service de la criminalité commerciale de la Chambre de commerce internationale* [en ligne], 12 novembre 2017, [consulté le 17 mars 2020], [https://icc-ccs.org/icc\\_2527/index.php/388-virtual-money-laundering-threat-identified](https://icc-ccs.org/icc_2527/index.php/388-virtual-money-laundering-threat-identified).

*transférée, stockée ou échangée électroniquement* ». Le nouvel article L.54-10-1 du Code monétaire et financier, créé par la loi PACTE du 22 mai 2019, en reprend la définition.

**8. – Distinction** – La définition retenue en droit interne met l'accent sur le fait que ces actifs numériques ne peuvent pas juridiquement être considérés comme des monnaies. La dénomination crypto-actif était déjà préférée à celle de crypto-monnaie par la Banque Centrale Européenne en 2015<sup>23</sup>, suivie par la Banque de France en 2017<sup>24</sup>. Les banques centrales lui reprochent de ne remplir qu'imparfaitement la triple fonction économique dévolue à la monnaie. Elles font valoir que la reconnaissance limitée de leur pouvoir libératoire empêche de les considérer comme de véritables instruments d'échange. Qui plus est, il est possible de les refuser sans contrevenir aux dispositions de l'article R. 642-3 du Code pénal. Néanmoins, ces arguments tendent à être remis en cause au regard de l'augmentation du nombre de professionnels acceptant les crypto-actifs comme moyen de paiement. Leur utilisation s'est popularisée et touche aujourd'hui tous les secteurs : du restaurateur à l'avocat, en passant par les dons aux associations et fondations<sup>25</sup>. Enfin, en raison de leur forte volatilité, les crypto-actifs peuvent difficilement servir d'unité de compte ou constituer une réserve de valeur. En effet, s'il a fallu huit ans au bitcoin pour atteindre 1 000 dollars et deux mois pour passer de 6 000 dollars à 19 000 dollars, il a aussi chuté en seulement quelques jours de 20 000 dollars à 6 000 dollars<sup>26</sup>.

**9. – Enjeux de souveraineté** – Toutefois, la monnaie ne peut se résumer à ces fonctions économiques. En tant que partie intégrante du système de paiement, institution fondamentale de la société, elle est aussi un instrument de cohésion sociale et de souveraineté. L'annonce par Facebook, au mois de juin 2019, du lancement de sa propre crypto-monnaie, le Libra, a cristallisé les inquiétudes. Les États y voient une potentielle atteinte à leur prérogative régaliennne de battre monnaie. En effet, les ministres des Finances et les gouverneurs de Banques centrales du G7, réunis à Chantilly le 18 juillet 2019, ont fait unanimement part de leurs préoccupations en la matière. Le 12 septembre 2019, lors du forum

---

<sup>23</sup> BANQUE CENTRALE EUROPEENNE, *Virtual Currency schemes - a further analysis*, février 2015, p. 4.

<sup>24</sup> « Mais au-delà, il ne doit pas y avoir d'ambiguïté : le bitcoin n'est en rien une monnaie, ou même une crypto-monnaie. » VILLEROY DE GALHAU François, Gouverneur de la Banque de France, *Bitcoin* [déclaration], Pékin, 1<sup>er</sup> décembre 2017.

<sup>25</sup> Depuis 2019, la Fondation de France et l'Unicef acceptent les dons en crypto-monnaies. La liste des établissements français qui acceptent les paiements en bitcoins est disponible sur le site <http://bitcoin.fr>.

<sup>26</sup> WOERTH Eric, PERSON Pierre, BARROT Jean-Noël, BRICOUT Jean-Louis, COQUEREL Eric, DUFREGNE Jean-Paul, VIGIER Philippe, *Monnaies virtuelles*, Rapport au nom de la commission des finances, de l'économie générale et du contrôle budgétaire, janvier 2019, p. 88.

mondial de l'OCDE sur les politiques en matière de blockchain, Bruno Lemaire déclarait à ce sujet : « Avec le projet Libra, la souveraineté monétaire des états est en jeu ». A ce titre, il avançait des risques de substitution de devises dans les pays au système financier instable ou ayant perdu la confiance de la population. En outre, la forte volatilité des cours des crypto-actifs laisse craindre des risques pour la stabilité financière mondiale. A ce jour, les banques centrales et les institutions financières estiment que ce risque n'est pas avéré eu égard à leur faible capitalisation et à leur acceptabilité limitée<sup>27</sup>. Toutefois, fort de ses 2,6 milliards d'utilisateurs, Facebook pourrait rapidement changer la donne. Face à cet enjeu, le gouverneur de la Banque de France voit dans la mise en place d'une monnaie digitale de banque centrale : « un puissant levier d'affirmation de notre souveraineté<sup>28</sup> ». Le 8 janvier 2020, Christine Lagarde affirmait son souhait de faire de l'Eurosystème et de la Banque Centrale Européenne des « acteurs sur ces questions<sup>29</sup> ». Une étude sur la création d'un e-euro devrait bientôt voir le jour.

**10. – Enjeux environnementaux** – Le coût écologique des crypto-actifs est souvent pointé du doigt dans le débat public. En effet, le système de validation des transactions (minage) de certaines *blockchain*, notamment Bitcoin, nécessite une importante puissance de calcul et induit de ce fait une forte consommation d'électricité. Les données en la matière sont très approximatives, la consommation annuelle mondiale des mineurs oscillerait entre 21 et 52 kilowattheures par an<sup>30</sup>. Certains acteurs appellent cependant à ne pas confondre consommation énergétique et empreinte écologie. En effet, l'empreinte écologique d'une consommation d'électricité donnée dépend très largement du moyen de production utilisée<sup>31</sup>. Ainsi, l'utilisation massive d'énergies renouvelables par les mineurs pourrait permettre de limiter l'impact écologique des crypto-actifs.

---

<sup>27</sup> FOND MONETAIRE INTERNATIONAL, *Global Financial Stability Report*, avril 2018, p. 24

BANQUE CENTRALE EUROPEENNE, *Crypto-Assets : Implications for financial stability, monetary policy, and payments and market infrastructures*, mai 2019, p. 3.

CONSEIL DE STABILITE FINANCIERE, *Crypto-assets*, mai 2019, p. 9.

<sup>28</sup> VILLEROY DE GALHAU François, *Monnaies digitale de banque centrale et paiements innovants* [discours], Paris, 4 décembre 2019.

<sup>29</sup> DE MENTHON Pierre-Henri et SYFUSS-ARNAUD Sabine, « Brexit, inflation, dettes... Les premières vérités de Christine Lagarde » [Interview], *Challenges*, 8 janvier 2020, [https://www.challenges.fr/economie/brexit-inflation-dettes-les-premieres-verites-de-christine-lagarde\\_692623](https://www.challenges.fr/economie/brexit-inflation-dettes-les-premieres-verites-de-christine-lagarde_692623).

<sup>30</sup> WOERTH Eric, PERSON Pierre, BARROT Jean-Noël, BRICOUT Jean-Louis, COQUEREL Eric, DUFREGNE Jean-Paul, VIGIER Philippe, *op. cit.*

<sup>31</sup> JEANNEAU Clément, *Impact écologique des blockchains et cryptomonnaies : idées reçues et réalités*, Blockchain Partner.

**11. – Enjeux juridiques** – Au-delà de ces considérations, les crypto-actifs posent de véritables défis en matière juridique. La diversité de leurs caractéristiques et usages ne permet pas de les rattacher à une catégorie juridique existante, la doctrine allant jusqu'à les qualifier d'« *objet juridique non identifié*<sup>32</sup> ». Cette incertitude de qualification entraîne des incertitudes quant aux régimes juridiques à leur appliquer et conduit nécessairement à un manque de cohérence et de clarté du sujet dans son ensemble. En outre, dans un contexte de compétition internationale, les régulateurs tentent de trouver un juste équilibre entre l'édiction d'un cadre réglementaire attractif, propice à l'innovation et à la croissance, et la réduction des risques liés à leur usage. Enfin, l'utilisation des crypto-actifs à des fins illicites conduit à une mutation de la délinquance économique et financière et remet en cause les méthodes traditionnelles de poursuites et de sanctions.

**12. – Utilisations illicites** – Sur le terrain pénal, la flambée des cours combinée à la nature décentralisée et semi-anonyme des crypto-actifs a suscité l'émergence de nouvelles formes de délinquance. La criminalité cryptographique, notion appréhendant les crypto-actifs à la fois en tant qu'objets et instruments d'infractions, s'inscrit dans le phénomène plus large de la cybercriminalité.

Animés par des motivations financières et techniques, les cybercriminels semblent aujourd'hui se rapprocher de ce que l'on appelait, dès 1937, la criminalité en "col blanc". En effet, le crime cryptographique profite à un segment petit mais puissant de criminels qui partagent la maîtrise et les codes du monde virtuel<sup>33</sup>.

Bien que l'utilisation de crypto-actifs à des fins illicites a plus que doublé entre 2018 et 2019, elle demeure minime en ce qu'elle ne représenterait qu'1,1% du volume total des transactions en crypto-actifs. Les sommes en question sont toutefois considérables et avoisineraient les 12 milliards de dollars rien que pour l'année 2019<sup>34</sup>.

---

<sup>32</sup> ROUSSILLE Myriam, « Le bitcoin : objet juridique non identifié », *Banque et Droit*, janvier 2015, n°159, p. 27 s.

<sup>33</sup> CABON Sarah-Marie, « L'influence du cyber espace sur la criminalité économique et financière », *Droit pénal*, mars 2018, n°3.

<sup>34</sup> CHAINANALYSIS, *The 2020 state of crypto crime*, janvier 2020, p. 5.

A ce stade, il convient de distinguer deux tendances, l'essor d'une cyber-délinquance nouvelle visant à l'appropriation de crypto-actifs de l'adaptation d'une délinquance plus traditionnelle à cette technologie.

– **Essor d'une cyberdélinquance nouvelle** – Les cyber-attaques visant les plateformes d'échange relèvent de la première catégorie. La plus emblématique reste le piratage de la plateforme japonaise Mt Gox considérée à l'époque comme la première plateforme mondiale d'échange et de stockage de bitcoins. Fondée par Jed McCaleb pour servir de plateforme d'échanges de cartes du jeu "Magic : The Gathering", Mt Gox fut converti en 2010 en plateforme d'échange de bitcoins. Un an plus tard, la plateforme fut rachetée par Mark Karpelès, un jeune informaticien français présenté comme un autodidacte surdoué. Au printemps 2013, Mt Gox connaît son apogée. Mark Karpelès, que l'on nomme désormais le « *Baron du Bitcoin* », enchaîne les interviews et affirme contrôler 80% des échanges mondiales de Bitcoin, représentant entre 5 et 20 millions de dollars de transactions par jour<sup>35</sup>. Le 7 février 2014, la plateforme suspend toutes ses transactions, 850 000 bitcoins ont été subtilisés pour une valeur à l'époque estimée à près de 473 millions de dollars. Cette attaque, en plus de provoquer la faillite de la plateforme et la ruine de milliers de clients, a ébranlé la confiance des investisseurs, faisant perdre au bitcoin la moitié de sa valeur en quelques jours.

Le nombre de cyberattaques a doublé en 2019 avec pas moins de 11 attaques de plateformes d'échanges, contre 6 en 2018 et 4 en 2017<sup>36</sup>. Bien que ce nombre ait augmenté de manière significative, le montant total de crypto-actifs dérobés a chuté par rapport à l'année passée, passant de 875 millions de dollars à 283 millions de dollars<sup>37</sup>. Ces chiffres s'expliquent par la survenance en janvier 2018 du plus important piratage lié aux crypto-actifs, la plateforme japonaise Coincheck s'étant vu dérober 534 millions de dollars.

Si les plateformes d'échange restent la cible privilégiée des cyberdélinquants, les particuliers ne sont pas épargnés par ce phénomène. Afin de subtiliser les crypto-actifs d'un usager, le cyberdélinquant

---

<sup>35</sup> LA TRIBUNE AVEC AFP, « Karpelès, le baron français du bitcoin, condamné au Japon », *La Tribune* [en ligne], 15 mars 2019, <https://www.latribune.fr/economie/international/karpeles-le-baron-francais-du-bitcoin-condamne-au-japon-810794.html>.

<sup>36</sup> CHAINANALYSIS, *The 2020 state of crypto crime*, janvier 2020, p. 41.

<sup>37</sup> *Ibid*

doit nécessairement obtenir la clé privée<sup>38</sup> de sa victime. Cette clé, assimilable à un code PIN de carte bancaire, est généralement stockée au sein d'un *wallet* ou portefeuille numérique qui peut être : un service en ligne dit *wallet online*, un programme informatique dit *software wallet*, ou un appareil dédié de type clé USB appelé *hardware wallet*. La méthode employée dépendra donc de la manière dont la clé privée est stockée. Dans le premier cas, dit *hot storage* (en ligne), l'appropriation consistera à accéder frauduleusement au support connecté à internet sur lequel est stocké la clé. Dans le second cas, dit *cold storage* (hors ligne), l'appropriation passera par la subtilisation du support physique sur lequel est consigné la clé privée de la victime. En outre, une technique populaire consiste en l'exfiltration des données dites copiées-collées. Les clés privées se présentant sous la forme d'une longue suite de chiffres et de lettres<sup>39</sup>, leurs propriétaires ont tendance à les "copier" pour ensuite les "coller" dans leurs presse-papiers. Ces derniers sont en général peu sécurisés et peuvent donc servir de vecteur d'attaque très efficace<sup>40</sup>.

Enfin, relève également de cette catégorie, le *cryptojacking* qui consiste à utiliser clandestinement la puissance de calcul d'un ordinateur afin de miner des crypto-actifs au bénéfice exclusif de l'attaquant. Le minage étant énergivore, la victime subit alors une augmentation de sa facture d'électricité et la détérioration de son matériel informatique.

– **Adaptation d'une délinquance traditionnelle** – Parmi cette deuxième catégorie, les escroqueries sont particulièrement préoccupantes. La forte volatilité des crypto-actifs a contribué, dans l'inconscience collective, à les assimiler à des placements financiers lucratifs<sup>41</sup>. Deux mille dix-neuf a été l'année de tous les records en matière d'escroquerie avec un butin estimé à près de 4,30 milliards de dollars<sup>42</sup>. Une part importante provient d'escroqueries à l'investissement de type Ponzi parmi lesquelles il convient de citer PlusToken, l'un des plus grands systèmes de Ponzi, qui aurait attiré à lui-

---

<sup>38</sup> La sécurité des transactions émises sur la blockchain est assurée par le recours à la cryptographie asymétrique qui repose sur une paire de clé publique et privée. Une comparaison peut être faite avec le monde bancaire opérant sur le modèle RIB/PIN. Le RIB, correspondant à la clé publique, peut-être communiqué au public et sert exclusivement à recevoir des fonds. Le code PIN, correspondant à la clé privée, doit être gardée confidentielle et permet de retirer les fonds.

<sup>39</sup> Exemple de clé : 1PhKuLP7AJRAXfSh1UGNetZjrPRkkVxwJB

<sup>40</sup> MARTINON Jacques, « Crypto-actifs : la justice pénale à l'épreuve des cryptomonnaies », *Dalloz IP/IT*, octobre 2019, p. 531.

<sup>41</sup> Le caractère hautement spéculatif du bitcoin résulte de la limitation du nombre maximal d'unités pouvant être créées (21 millions de bitcoins) et de la régulation du rythme de création (rythme divisé par deux tous les 210 000 blocs minés, soit tous les 4 ans environ). Ainsi, 50 bitcoins pouvaient être créés en 10 minutes en 2009, contre 12,5 depuis 2017.

<sup>42</sup> CHAINALYSIS, *The 2020 state of crypto crime*, janvier 2020, p. 17 s.

seul près de 3 milliards de dollars<sup>43</sup>. Par ailleurs, les Initial Coin Offerings<sup>44</sup> (ICO) sont une source non-négligeable d'escroqueries. Selon les chiffres du site Deadcoins, repris dans un rapport de l'Autorité des Marchés Financiers (AMF), on dénombrait fin 2018 environ 183 ICOs frauduleuses, pour des préjudices financiers élevés mais difficiles à estimer<sup>45</sup>.

En outre, les extorsions par le biais d'attaques de *ransomwares* (rançongiciels) sont l'une des menaces actuelles les plus importantes en terme de cybercriminalité. Europol les considère comme la « la forme de cyberattaque la plus répandue et la plus dommageable financièrement<sup>46</sup> ». Les *ransomwares* sont des logiciels malveillants qui chiffrent les données enregistrées sur un disque dur ou verrouille l'accès à un ordinateur. La victime se voit alors contrainte de payer une rançon, souvent en crypto-actifs, afin de reprendre le contrôle de ses fichiers ou de son appareil. Le 13 décembre 2019, le gouvernement de la Nouvelle-Orléans a été contraint de déclarer l'état d'urgence après que le réseau informatique de son administration ait été infecté. Le temps d'arrêt causé par l'attaque aurait coûté à la ville près de 7,2 millions de dollars<sup>47</sup>. La France n'est pas épargnée par ces attaques, récemment c'est l'agglomération de Grand Cognac<sup>48</sup> ainsi que le CHU de Rouen<sup>49</sup> qui en ont fait les frais.

---

<sup>43</sup> MC GARRY Dan, NANUA Richard et MALAPA Terence, « Six chinese face deportation », *Vanuatu Daily Post* [en ligne], juin 2019, [https://dailypost.vu/news/six-chinese-face-deportation/article\\_fef7f311-679d-5d1b-9ec5-4f44e73118bb.html](https://dailypost.vu/news/six-chinese-face-deportation/article_fef7f311-679d-5d1b-9ec5-4f44e73118bb.html).

<sup>44</sup> Une offre au public de jetons est une opération de levée de fonds, effectuée sur une blockchain, par laquelle un porteur de projet ayant besoin de financement émet des jetons appelés *tokens* auxquels des investisseurs souscrivent généralement en crypto-monnaies. Ces jetons peuvent accorder à leur détenteur un droit d'user des produits ou services de la société (*utility token*) ou lui offrir des droits politiques ou financiers tels que des droits de vote (*security token*). Ces jetons peuvent ensuite être revendus sur un marché secondaire à des fins spéculatives.

<sup>45</sup> LE MOIGN Caroline, *Ico françaises : un nouveau mode de financement ?*, AMF, novembre 2018. Le rapport cite le cas des sociétés américaine PlexCorps (15 millions de dollars), vietnamienne Modern Tech (660 millions de dollars via deux ICO) et anglaise BitConnect (700 000 dollars).

<sup>46</sup> EUROPOL, *Internet organised crime threat assessment 2019*, 9 octobre 2019, 4 p.

<sup>47</sup> WILLIAMS Jessica, « Cyberattack has cost New Orleans \$7.2 million; city email still not fully restored; tax payment deadline delayed », *The Times-Picayune*, 15 janvier 2020, [https://www.nola.com/news/politics/article\\_8dbed526-37d0-11ea-9998-bbe9bfc93b5b.html](https://www.nola.com/news/politics/article_8dbed526-37d0-11ea-9998-bbe9bfc93b5b.html).

<sup>48</sup> PASQUIER Julie, « Virus à l'agglomération de grand cognac : une attaque sans précédent », *Charente Libre*, 22 octobre 2019, <https://www.charentelibre.fr/2019/10/22/virus-a-l-agglomeration-de-grand-cognac-une-attaque-sans-precedent.3505276.php>.

<sup>49</sup> TRIOLLIER Gilles, « Frappé par une cyberattaque massive, le CHU de Rouen forcé de tourner sans ordinateurs », *Le Monde*, le 18 novembre 2019, [https://www.lemonde.fr/pixels/article/2019/11/18/frappe-par-une-cyberattaque-massive-le-chu-de-rouen-force-de-tourner-sans-ordinateurs\\_6019650\\_4408996.html](https://www.lemonde.fr/pixels/article/2019/11/18/frappe-par-une-cyberattaque-massive-le-chu-de-rouen-force-de-tourner-sans-ordinateurs_6019650_4408996.html).

Enfin, les crypto-actifs peuvent être utilisés à des fins de financement du terrorisme<sup>50</sup>. L'institut de recherche des médias du Moyen-Orient a publié le 21 août 2019 une étude sur le sujet<sup>51</sup>. Elle montre qu'au cours des cinq dernières années l'utilisation des crypto-actifs par les organisations terroristes s'est développée à partir de campagnes de levées de fonds. Bien qu'elles paraissent marginales et que leurs rendements semblent modestes (dans les dizaines de milliers de dollars), la menace est bien présente, les attaques terroristes ne nécessitant souvent que peu de moyens<sup>52</sup>.

**13. – Le blanchiment de capitaux** – Le blanchiment de capitaux est le dénominateur commun entre toutes ses infractions puisque chaque cybercriminel qui tire de son infraction un produit en crypto-actifs doit en obscurcir l'origine dans le but de les convertir en espèces. La conversion inverse (fiat-crypto) présente également des atouts, notamment en termes de traçabilité des fonds.

Le blanchiment de capitaux peut être défini comme l'opération ayant pour finalité de faire disparaître l'origine des fonds provenant d'un crime ou d'un délit afin de les réintégrer dans le circuit financier légal (C. pén. art. 324-1 du Code pénal). Parce que le produit de l'infraction est illicite, l'acte qui vise à lui donner une apparence légale, donc « *propre* » est dénommé blanchiment en droit français, blanchissage en droit suisse, *money laundering* en droit anglo-saxon ou encore recyclage en droit italien<sup>53</sup>. Cette terminologie serait liée à l'histoire d'Al Capone qui aurait, à la fin des années 20, investi une part significative des profits tirés de ses activités mafieuses dans une chaîne de blanchisseries<sup>54</sup>.

La métaphore prend tout son sens lorsque l'on constate que l'argent sale subit différents traitements comparables au programme d'une machine à laver : le prélavage qui correspond à la réintroduction des fonds illicites dans le système financier ; le lavage qui consiste à multiplier les opérations bancaires et financières dans le but de casser tout lien entre les fonds et l'infraction dont ils proviennent ; enfin

---

<sup>50</sup> DUBOIS Kévin, Analyste criminel à l'Office Central de Lutte contre la Cybercriminalité (OCLCTIC), Expert en crypto-actifs, entretien téléphonique mené par Alexandra Puertas, le 27 juin 2020

<sup>51</sup> STALINSKY Steven, *The coming storm : terrorists using cryptocurrency*, MEMRI, 21 août 2019.

<sup>52</sup> POPPER Nathaniel, « Terrorists Turn to Bitcoin for Funding and They're Learning Fast », *The New York Times*, 18 août 2019, <https://www.nytimes.com/2019/08/18/technology/terrorists-bitcoin.html>.

<sup>53</sup> MATSOPOULOU Haritini (dir.), MASCALA Corinne (dir.), *Le Lamy droit pénal des affaires*, Wolters Kluwer, 2020, 1739°.

<sup>54</sup> DAURY-FAUVEAU Morgane, *Fascicule 20 : blanchiment - conditions et constitution*, JurisClasseur Pénal des Affaires, Lexis Nexis, 2 mai 2020, 1°.



l'essorage qui est réalisé par l'investissement des fonds d'origine frauduleuse dans les circuits légaux de l'économie.

La lutte contre le blanchiment de capitaux poursuit donc un double objectif, d'une part, prévenir les activités criminelles en faisant en sorte que le crime ne paie pas, d'autre part, assurer l'intégrité et la stabilité du système économique et financier.

**14 – Utilisation des crypto-actifs à des fins de blanchiment** – Les risques de blanchiment liés à l'usage des crypto-actifs tiennent au fait qu'ils permettent des transferts d'actifs pseudonymes (Bitcoin) voir anonymes (Monero) en marge de toute entité centrale de contrôle. Leur utilisation est de ce fait beaucoup moins réglementée que le système bancaire traditionnel.

Ces risques sont cependant à relativiser au regard du fait que l'utilisation des mules d'argent reste le moyen de blanchiment privilégié des criminels pour transférer rapidement des fonds vers des territoires au système financier moins réglementé<sup>55</sup>. Néanmoins, la pandémie actuelle rend l'utilisation des mules d'argent difficile au regard de l'intensification des contrôles aux frontières voire leurs fermetures. Les blanchisseurs pourraient intégrer ces risques dans leur modèle criminel et trouver dans les crypto-actifs des aspects séduisants<sup>56</sup>.

En outre, certains font valoir que les crypto-actifs ne présentent pas de risque en matière de blanchiment puisque leur utilisation requiert des compétences techniques et que leurs cours exposent les blanchisseurs à des pertes financières. Toutefois, les risques liés à la volatilité des crypto-actifs tendent à être neutralisés par l'utilisation de stablecoins. Les stablecoins sont des crypto-actifs dont le cours est stabilisé par une réserve de monnaie ayant cours légal voir à un panier de devises tel que l'envisage le projet Libra.

Parmi les stablecoins, le crypto-actif Tether domine le marché avec une capitalisation boursière estimée à près de 9 milliards de dollars américains, le classant à la 3ème place des crypto-actifs en terme de

---

<sup>55</sup> COMMISSION EUROPENNE, Rapport de la Commission au Parlement européen et au Conseil sur l'évaluation des risques de blanchiment de capitaux et de financement du terrorisme pensant sur le marché intérieur et liés aux activités transfrontières, 3 p. ; EUROPOL, *Internet organised crime threat assessment 2019*, 9 octobre 2019, 52 p.

<sup>56</sup> PIERSON Frédérique, Capitaine de Police, Responsable du Bureau des avoirs criminels d'Europol, entretien téléphonique mené par Alexandra Puertas, le 10 juin 2020.

capitalisation boursière derrière Bitcoin et Ethereum<sup>57</sup>. Tether fonctionne sur le principe d'un ratio 1:1 de réserve ce qui signifie que chaque unité tether créée correspond à un dollar américain (pour le USD₯), un euro (pour le EUR₯) ou encore un yuan chinois offshore (pour le CNH₯) détenu sur les comptes bancaires de la société Tether Limited<sup>58</sup>. En un peu plus d'un an, la quantité de tether en circulation a quintuplé passant de 2 millions au 1<sup>er</sup> avril 2019 à 9,7 millions au 10 juin 2020<sup>59</sup>.

Enfin, l'utilisation des crypto-actifs à des fins de blanchiment présentent au moins quatre avantages :

- Un intérêt en matière logistique : la dissimulation d'une clé cryptographique étant bien plus aisée que la dissimulation de liquidités ;
- Des avantages en terme de mobilité : les crypto-actifs sont un moyen rapide et sécurisé pour faire transiter de la valeur au-delà des frontières ;
- Des intérêts en matière d'investissement : les crypto-actifs constituent un bon outil d'investissement criminel ;
- Des intérêts en matière de traçabilité : les portefeuilles cryptographiques ne figurent pas parmi le fichier national des comptes bancaires et assimilés (FICOBA) qui permet, depuis sa création en 1971, de recenser les comptes existants - qu'ils soient bancaires, postaux ou encore d'épargne - et de fournir des informations aux personnes habilitées<sup>60</sup>.

---

<sup>57</sup> COINMARKETCAP, All cryptocurrencies, sur *Coinmarketcap* [en ligne], [consulté le 10 juin 2020], <https://coinmarketcap.com/all/views/all/>.

<sup>58</sup> TETHER, « Tether : Fiat currencies on the Bitcoin blockchain », sur *Tether* [en ligne], [consulté le 10 juin 2020], <https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf>.

<sup>59</sup> THE STABLECOIN INDEX, « Market cap » [en ligne], sur *The stablecoin index* [consulté le 10 juin 2020], <https://stablecoinindex.com/marketcap>.

<sup>60</sup> HOUEL Jean-Luc, Ancien enquêteur financier à la section de recherches de Dijon, Ancien chef de la cellule régionale des avoirs criminels, entretien téléphonique mené par Alexandra Puertas, le 11 juin 2020.

Dès 2011, TRACFIN alertait sur les risques d'utilisation des crypto-actifs à des fins de blanchiment<sup>61</sup>. Il semblerait que ces risques tendent à s'intensifier depuis un an environ<sup>62</sup>. L'ampleur du blanchiment de capitaux au moyen de crypto-actifs est difficile à évoluer mais est considérée comme importante<sup>63</sup>.

Face à ce phénomène, le Groupe d'action financière (GAFI) a appelé en février 2018 ses trente-neuf états à membres, à adopter de nouvelles dispositions préventives et répressives pour renforcer la lutte contre le blanchiment de capitaux liée à l'usage des crypto-actifs<sup>64</sup>. Cette action fût appuyé par le G20 à l'occasion du sommet des 19 et 20 mars 2018<sup>65</sup>. Une question est donc à ce stade légitime :

La politique française de lutte contre le blanchiment est-elle adaptée aux nouveaux risques que constituent les crypto-actifs ?

Pour répondre à cette question, il convient de s'intéresser à l'assujettissement, en France, des acteurs de l'écosystème crypto (I), avant de vérifier que l'incrimination de blanchiment prévue par le Code pénal est applicable à celui commis au moyen de crypto-actifs (II), puis enfin s'assurer de l'effectivité du système répressif (III).

---

<sup>61</sup> TRACFIN, *Rapport d'activité 2011*, 11 p.

<sup>62</sup> PIERSON Frédérique, Capitaine de Police, Responsable du Bureau des avoirs criminels d'Europol, entretien téléphonique mené par Alexandra Puertas, le 10 juin 2020.

<sup>63</sup> CHAINALYSIS, *The 2020 state of crypto crime*, janvier 2020, 8 p.

<sup>64</sup> LANDAU Jean-Pierre avec la collaboration de GENAIS Alban, *Les crypto-monnaies*, Rapport au Ministre de l'Économie et des Finances, 4 juillet 2018, 54 p.

<sup>65</sup> BANQUE DE FRANCE, *G20 Osaka Leader's declaration*, 28 et 29 juin 2019.

## **I. La prévention du blanchiment de capitaux au moyen de crypto-actifs**

**15. – De la nature au régime** – L’approche préventive de la lutte contre le blanchiment de capitaux au moyen de crypto-actifs se matérialise par un ensemble de règles de droit destinées à réglementer leur usage. En droit, la détermination du régime juridique d’une chose passe traditionnellement par une opération intellectuelle dénommée qualification juridique. Qualifier juridiquement une chose consiste à rattacher une situation factuelle à « *une catégorie juridique existante parce qu’elle en a la nature et en emprunte donc le régime*<sup>66</sup> ». S’interroger sur la nature juridique des crypto-actifs revient donc à s’intéresser au régime juridique qu’elle induit.

Les crypto-actifs sont généralement définis au terme d’une classification tripartite en fonction de leurs usages<sup>67</sup>. Il convient dès lors de différencier les *currency tokens*, des *utility tokens* et des *security tokens*.

– **Nature juridique des *currency tokens*** – Les *currency tokens*, ou jetons de monnaie, sont définis à l’article L. 54-10-1, 2°, du Code monétaire et financier comme : « *Toute représentation numérique d’une valeur qui n’est pas émise ou garantie par une banque centrale ou par une autorité publique, qui n’est pas nécessairement attachée à une monnaie ayant cours légal et qui ne possède pas le statut juridique d’une monnaie, mais qui est acceptée par des personnes physiques ou morales comme un moyen d’échange et qui peut être transférée, stockée ou échangée électroniquement* ». En d’autres termes, ils désignent les crypto-actifs utilisés comme moyen d’échange ou détenus à des fins spéculatives tels que bitcoin ou ripple. Les *currency tokens* représentent la majorité des crypto-actifs émis sur le marché primaire et échangés sur le marché secondaire<sup>68</sup>. S’agissant de leur nature juridique, il semble davantage aisé de qualifier les *currency tokens* par voie d’exclusion.

---

<sup>66</sup> BERGEL Jean-Louis, *Théorie générale du droit*, 5<sup>ème</sup> édition, Dalloz, 2012, 239 p.

<sup>67</sup> WOERTH Eric, PERSON Pierre, BARROT Jean-Noël, BRICOUT Jean-Louis, COQUEREL Eric, DUFREGNE Jean-Paul, VIGIER Philippe, *Monnaies virtuelles*, Rapport au nom de la commission des finances, de l’économie générale et du contrôle budgétaire, Assemblée nationale, janvier 2019, 61 p.

AUTORITE BANCAIRE EUROPEENNE, *Report with advice for the European Commission on crypto-assets*, 9 janvier 2019, 7 p.

<sup>68</sup> WOERTH Eric, PERSON Pierre, BARROT Jean-Noël, BRICOUT Jean-Louis, COQUEREL Eric, DUFREGNE Jean-Paul, VIGIER Philippe, *op. cit.*

En effet, les *currency tokens* ne peuvent pas, d'une part, prétendre à la qualification juridique de monnaie, le cours légal étant réservé en France à l'Euro<sup>69</sup> (C. mon. fin. art. L. 111-1). Cette affirmation est confortée par la définition retenue en droit interne à l'article L. 51-10-1 du Code monétaire et financier qui dispose que les actifs numériques utilisés comme moyen d'échange « *ne possède pas le statut juridique d'une monnaie* ». D'autre part, les *currency tokens* ne peuvent être rattachés ni aux instruments financiers, faute d'entrer dans l'une des catégories visées par l'article L. 211-1 du Code monétaire et financier, ni aux créances, faute d'émetteur<sup>70</sup>. Cependant, certains crypto-actifs dits centralisés<sup>71</sup>, sont contrôlés et émis par une autorité centrale. Dans ce cas, la qualification de créance semble opportune.

Du point de vue de l'Union européenne, les *currency tokens* peuvent être qualifiés de monnaie électronique au sens de l'article 2 de la directive 2009/110/CE, tel que transposée à l'article L. 315-1 du Code monétaire et financier, sous réserves de remplir diverses conditions<sup>72</sup>. Ils doivent être stockés électroniquement, avoir une valeur monétaire, représenter une créance sur l'émetteur, être délivrés à la réception de fonds, émis dans le but d'effectuer des transactions de paiement et acceptés par des personnes autres que l'émetteur. Dans ce cas, ils relèvent également de la qualification de « *fonds* » au sens de l'article 4 de la directive 2015/2366 dite directive sur les services de paiement 2. Toutefois, à défaut de remplir un business model bien particulier, la majorité des activités impliquant des *currency tokens* n'entrent pas dans le champs d'application de la législation de l'UE sur les services de paiement qui comprend notamment des exigences de KYC. Il apparaît alors étonnant de constater que la Cour de Justice de l'Union Européenne n'hésite pas à qualifier « *la devise virtuelle bitcoin* » de moyen de paiement, lorsqu'il s'agit de soustraire l'activité de change de bitcoins à la TVA<sup>73</sup>, ou encore la Banque de France qui, tout en refusant de qualifier les *currency tokens* de moyen de paiement, considère que l'activité qui consiste à les convertir en monnaie ayant cours légal entre dans le champs de la

---

<sup>69</sup> CORBION-CONDE Lycette, « De la défiance à l'égard des monnaies nationales au miroir du bitcoin », *Revue de Droit bancaire et financier*, mars 2014, dossier 13, n°2.

<sup>70</sup> ALMASEANU Stephen, « Le traitement pénal du Bitcoin et des autres monnaies virtuelles », *Gazette du Palais*, 30 août 2014, n°242, 11 p.

<sup>71</sup> GAFI, *Virtual currencies: Key definitions and potential AML/CFT Risks*, juin 2014, 7 p.

<sup>72</sup> AUTORITE BANCAIRE EUROPEENNE, *Report with advice for the European Commission on crypto-assets*, 9 janvier 2019, 13 p.

<sup>73</sup> CJUE, 5<sup>e</sup> ch., 22 octobre 2015, aff. C-264/14, Hedqvist.

règlementation des services de paiement<sup>74</sup>. Ces qualifications opportunes contribuent à obscurcir la nature juridique des *currency tokens*<sup>75</sup>.

En tout état de cause, il apparaît que les *currency tokens* peuvent être qualifiés de biens meubles (C. civ. art. 527) en ce qu'ils sont susceptibles d'appropriation et cessibles<sup>76</sup>. En effet, le titulaire d'une clé privée peut user librement des *currency tokens* envoyés sur sa clé publique (*usus*). Il peut en outre jouir de l'accroissement de leur valeur économique (*fructus*) et en disposer librement (*abusus*). Il exerce ces droits de manière exclusive puisqu'il est le seul à pouvoir accéder aux *currency tokens* associés à sa clé publique, au moyen de sa clé privée. Dans un arrêt récent en date du 26 février 2020 (n°2018F00466), le tribunal de commerce de Nanterre a confirmé cette thèse en qualifiant le bitcoin de bien incorporel fongible et consommable dans le cadre d'un litige portant sur un contrat de prêt de bitcoins qui opposaient deux sociétés<sup>77</sup>. Enfin, à la lumière de la loi PACTE du 22 mai 2019, les *currency tokens* doivent être considérés comme une nouvelle catégorie de biens meubles incorporels dénommée actif numérique.

– **Nature juridique des utility tokens** – Les *utility tokens*, ou jetons de service, sont une forme de crypto-actifs émis dans le cadre d'une *Initial Coin Offering* (ICO) qui n'est autre que le pendant, sur une blockchain, d'une *Initial Public Offering* (IPO) par laquelle une société ouvre son capital à des investisseurs sur un marché boursier<sup>78</sup>. En d'autres termes, les *utility tokens* sont un type de jetons numériques, émis dans le cadre d'une levée de fonds effectuée sur une blockchain, et auxquels les investisseurs souscrivent en échange, généralement, de la remise de crypto-actifs. Ces derniers peuvent ensuite être revendus sur un marché secondaire à des fins spéculatives.

---

<sup>74</sup> BANQUE DE FRANCE, *Les dangers liés au développement des monnaies virtuelles : l'exemple du bitcoin*, 5 décembre 2013.

<sup>75</sup> BALI Mehdi, « Les crypto-monnaies, une application des block chain technologies à la monnaie », *Revue de Droit bancaire et financier*, n°2, janvier 2015, étude 8.

<sup>76</sup> TERRE François, SIMLER Philippe, *Droit civil - Les biens*, 10<sup>ème</sup> édition, Dalloz, 2018, 60 p. ; COURBE Patrick, LATINA Mathias, *Droit civil - Les biens*, 8<sup>ème</sup> édition, Dalloz, 2016, 5 p.

<sup>77</sup> MOREIL Sophie, « Le tribunal de commerce de Nanterre prend position sur la nature du prêt de bitcoins », *Gazette du Palais*, 9 juin 2020, n°21, 61 p.

<sup>78</sup> NJABOUM Jessica Joyce, « Régime juridique des ICOs et nature juridique des tokens », *Revue internationale des services financiers*, 2020, n°1, 58 p.

L'article L. 552-2 du Code monétaire et financier, créé par loi PACTE du 22 mai 2019, les définit sous le terme de jetons comme : « *tout bien incorporel représentant, sous forme numérique, un ou plusieurs droits pouvant être émis, inscrits, conservés ou transférés au moyen d'un dispositif d'enregistrement électronique partagé permettant d'identifier, directement ou indirectement, le propriétaire dudit bien* ». Cette définition large met en lumière le caractère protéiforme des jetons. En effet, un jeton est avant tout ce que son créateur souhaite qu'il soit puisqu'il peut représenter tout droit réel ou personnel<sup>79</sup>.

Les *utility tokens* se distinguent d'autres jetons dénommés *security tokens* en ce qu'ils octroient à leur détenteur un droit d'usage des biens et/ou des services du porteur de projet qui les a émis<sup>80</sup>. Leur émission s'inscrit dans des méthodes dites de « marketing captif » en permettant de cibler, à la fois des investisseurs et, des clients intéressés par les services que le porteur de projet souhaite développer<sup>81</sup>. A titre illustratif, un *utility token* pourrait servir de moyen de paiement afin d'acquérir les biens et services proposés par le porteur de projet qui les a émis, à l'image des miles d'AirFrance ou des cagnottes fidélités dans la grande distribution. Il pourrait également octroyer à leur détenteur des réductions sur les biens et services proposés.

La nature protéiforme des *utility tokens* complexifie leur analyse juridique. De nouveau, il convient de les définir par voie d'exclusion. D'une part, les *utility tokens* ne sont pas des instruments financiers au sens de l'article L. 211-1 du Code monétaire et financier, à défaut d'entrer dans l'une des catégories visées par ledit article. D'autre part, le doute persiste entre retenir la qualification de créance ou de bien. Certains auteurs font valoir que les *currency tokens* sont des créances non monétaires en ce qu'ils accordent à leurs détenteurs un droit personnel en vertu duquel ils peuvent exiger de l'émetteur un droit d'usage sur des biens et services déterminables<sup>82</sup>. Toutefois, les *currency tokens* n'étant pas nécessairement émis par une personne morale<sup>83</sup>, il devient alors difficile d'y voir un droit personnel en

---

<sup>79</sup> LEGEAIS Dominique, *Fascicule 535 : actifs numériques et prestataires sur actifs numériques*. JurisClasseur Commercial, Lexis Nexis, 14 octobre 2019.

<sup>80</sup> AMF, *Synthèse des réponses à la consultation publique portant sur les Initial Coin Offerings (ICO) et point d'étape sur le programme « UNICORN »*, février 2018, 3 p.

<sup>81</sup> *Ibid.*

<sup>82</sup> DE VAUPLANE Hubert, « La qualification juridique de certains tokens en titre de créance », *Revue trimestrielle de droit financier*, n°4, 2017 ; NJABOUM Jessica Joyce, *op. cit.*

<sup>83</sup> L'émetteur de jetons qui souhaite que son ICO porte le visa de l'AMF doit nécessairement être constitué sous la forme d'une personne morale établie ou immatriculée en France (C. mon. fin. art. L. 552-5). Pour le reste, les ICOs peuvent être générés par un algorithme ou être émis par une communauté ou une organisation n'ayant pas la personnalité morale.

l'absence de droit contre une personne<sup>84</sup>. D'autres auteurs considèrent que les *currency tokens* sont des biens meubles incorporels dès lors qu'ils sont appropriable et immatériel<sup>85</sup>. Cette qualification converge avec celle retenue par l'AMF qui considèrent que les tokens sont appropriables « *dans la mesure où ils peuvent être appréhendés par leurs souscripteurs*<sup>86</sup> ».

– **Nature juridique des security tokens** – Les *security tokens* sont également des crypto-actifs pouvant être émis dans le cadre d'une *Initial Coin Offering* (ICO). A la différence des *utility tokens*, les *security tokens* confèrent à leurs détenteurs des droits politiques et/ou financiers analogues à ceux octroyés par des titres financiers (droit de vote et droit aux dividendes notamment)<sup>87</sup>. En ce sens, une partie de la doctrine considère que les *security tokens* peuvent s'analyser « *comme des créances représentatives de somme d'argent* »<sup>88</sup>. Toutefois, d'autres auteurs considèrent que faute de conférer un droit de créance contre un émetteur personne morale, les *security tokens* ne peuvent pas être rattachés aux titres de créances (C. mon. fin. art. L. 213-1 A) et plus généralement aux titres financiers<sup>89</sup>. En effet, les *security tokens* n'étant pas nécessairement émis par un émetteur personne morale, leur rattachement systématique est donc exclu.

Il n'en reste pas moins que l'Autorité des Marchés Financiers (AMF), au terme « *d'une analyse privilégiant la substance du titre sur sa forme*<sup>90</sup> », n'exclut pas qu'un *security token* puisse être qualifié de titre financier « *dès lors qu'il incorpore des droits analogues à ceux qui sont classiquement compris dans un titre de capital ou un titre de créance*<sup>91</sup> ». Toutefois, une telle qualification emporterait

---

<sup>84</sup> NJABOUM Jessica Joyce, *op. cit.* ; SOLERANSKI Louis, « Réflexions sur la nature juridique des tokens », *Bulletin Joly Bourse*, 1<sup>er</sup> mai 2018, n°3, 191 p.

<sup>85</sup> *Ibid.*

<sup>86</sup> AMF, *Synthèse des réponses à la consultation publique portant sur les Initial Coin Offerings (ICO) et point d'étape sur le programme « UNICORN »*, février 2018, 9 p.

<sup>87</sup> WOERTH Eric, PERSON Pierre, BARROT Jean-Noël, BRICOUT Jean-Louis, COQUEREL Eric, DUFREGNE Jean-Paul, VIGIER Philippe, *Monnaies virtuelles*, Rapport au nom de la commission des finances, de l'économie générale et du contrôle budgétaire, Assemblée nationale, janvier 2019, 62 p.

<sup>88</sup> SOLERANSKI Louis, *op. cit.*

<sup>89</sup> BONNEAU Thierry, « Tokens, titres financiers ou biens divers ? » *Revue de Droit bancaire et financier*, janvier 2018 ; LACROIX Frédéric, « Les places financières alternatives : propos relatifs aux approches réglementaires concernant les plateformes de crowdfunding et d'échanges de bitcoin », in FRISON ROCHE Marie-Anne (dir.), *Internet, espace d'interrégulation*, Dalloz, 2016.

<sup>90</sup> AMF, *op. cit.*, 6 p.

<sup>91</sup> AMF, *op. cit.*



l'application de l'ensemble des règles applicables aux offres au public de valeurs mobilières au sens de la directive MiDIF 2 (2014/65/EU), dont les transpositions divergentes par les états membres<sup>92</sup> laissent craindre un risque de *regulatory shopping*.

**16. – De l'activité au dispositif LCB** – En définitive, le caractère multiforme des crypto-actifs, combiné à l'évolution rapide et permanente de leurs usages, ne permettent pas de les rattacher à une catégorie juridique existante puisqu'aucune n'est pleinement satisfaisante. Gény et Duguit dénonçaient déjà les risques liés à la classification qui, par des conceptions purement intellectuelles, conduit à donner au droit « *une raideur incompatible avec la complexité du réel et la souplesse de la vie* ».

L'analyse de la nature juridique des crypto-actifs met en évidence le fait que le législateur se préoccupe davantage de les réglementer, que de les qualifier en tant que tels. Cela conduit parfois à leur appliquer des régimes relatifs à des opérations portant sur certains biens, tout en leur déniaient la nature de ces derniers. Cette réglementation « *au compte-goutte* » conduit nécessairement à un manque de cohérence et de clarté du sujet dans son ensemble.

En matière de lutte contre le blanchiment, le législateur, après avoir défini largement ce qu'il faut entendre par crypto-actifs<sup>93</sup>, a consacré une nouvelle catégorie d'acteurs financiers, celle des prestataires de services numériques<sup>94</sup>. La loi PACTE du 22 mai 2019 vise à lutter contre l'utilisation des crypto-actifs à des fins de blanchiment en assujettissant lesdits prestataires aux obligations de lutte contre le blanchiment prévues aux articles L. 561-2 et suivants du Code monétaire et financier, dès lors qu'ils exercent une des activités listées à l'article L. 54-10-2 dudit code.

---

<sup>92</sup> AUTORITE EUROPENNE DES MARCHES FINANCIERS, *Initial coin offerings and crypto-assets*, 9 janvier 2019, p. 18 et suiv.

<sup>93</sup> Le terme actif numérique a été privilégié à celui de crypto-actif par le législateur (C. mon. fin. art. L. 552-2).

<sup>94</sup> LEGEAIS Dominique, *Fascicule 535 : actifs numériques et prestataires sur actifs numériques*. JurisClasseur Commercial, Lexis Nexis, 14 octobre 2019, 85°.

Ces activités sont les suivantes :

- Le service de conservation, pour le compte de tiers, d'actifs numériques ou d'accès à des actifs numériques, le cas échéant sous la forme de clés cryptographiques privées, en vue de détenir, stocker et transférer des actifs numériques ;
- Le service d'achat ou de vente d'actifs numériques en monnaie ayant cours légal ;
- Le service d'échange d'actifs numériques contre d'autres actifs numériques ;
- L'exploitation d'une plateforme de négociation d'actifs numériques.

Il s'agit enfin des services suivants :

- La réception et la transmission d'ordres sur actifs numériques pour le compte de tiers ;
- La gestion de portefeuille d'actifs numériques pour le compte de tiers ;
- Le conseil aux souscripteurs d'actifs numériques ;
- La prise ferme d'actifs numériques ;
- Le placement garanti d'actifs numériques ;
- Le placement non garanti d'actifs numériques.

Il semblerait que le législateur ait opté pour une approche fondée sur les risques, telle que recommandée par le Groupe d'Action Financière (GAFI)<sup>95</sup>, afin de fixer le curseur réglementaire au regard des risques de blanchiment de capitaux associés à chaque activité.

En ce sens, dès 2014, l'Autorité Bancaire Européenne (ABE) recommandait d'inclure, dans le champ d'application des assujettis aux obligations de lutte contre le blanchiment de capitaux (LCB), les plateformes d'échange de crypto-actifs contre monnaie ayant cours légal ainsi que les fournisseurs de services de portefeuille<sup>96</sup>.

Ces recommandations furent suivies par le Parlement européen et le Conseil qui ajoutèrent les fournisseurs de service de wallet, ainsi que les plateformes d'échange crypto-actifs contre monnaie

---

<sup>95</sup> GAFI, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, juin 2019.

<sup>96</sup> AUTORITE BANCAIRE EUROPEENNE, *Opinion on 'virtual currencies'*, 4 juillet 2014.

ayant cours légal (dite monnaie fiat), aux assujettis à la réglementation LCB, dans le cadre de l'adoption de la cinquième directive anti-blanchiment (2018/843), transposée en droit interne par l'ordonnance (2020-115) et les décrets (2020-118 / 2020-119) du 12 février 2020. Cependant, la loi PACTE du 22 mai 2019 est allée plus loin en prévoyant un double volet sur les crypto-actifs, le premier concerne les prestataires de services sur actifs numériques (A), et le second, l'encadrement des Initial Coin Offerings (B).

## **A. L'assujettissement des prestataires de services sur actifs numériques aux obligations de lutte contre le blanchiment**

**17. – Délimitation du sujet** – L'assujettissement des prestataires de services sur actifs numériques aux obligations LCB sera étudié, dans la présente partie, sous le seul prisme des activités de conservation pour le compte de tiers d'actifs numériques (C. mon. fin. art. L. 54-10-2, 1°), ainsi que les activités d'échange d'actifs numériques contre monnaie ayant cours légal et intra-actifs numériques (C. mon. fin. art. L. 54-10-2, 2° et 3°).

**18. – Définition** – Le décret d'application de la loi Pacte du 21 novembre 2019 (n°2019-1213) est venu apporter des précisions quant à la notion de service de conservation d'actifs, qui est proposé par ce qu'il est courant d'appeler les fournisseurs de portefeuille ou *wallet providers*. En effet, l'article D. 54-10-1, 1°, du Code monétaire et financier dispose que : « *Constitue le service de conservation d'actifs numériques pour le compte de tiers le fait de maîtriser, pour le compte d'un tiers, les moyens d'accès aux actifs numériques inscrits dans le dispositif d'enregistrement électronique partagé et de tenir un registre de positions, ouvert au nom du tiers, correspondants à ses droits sur lesdits actifs numériques* ». En d'autres termes, les *wallets providers* sont des prestataires de services sur actifs numériques qui proposent à leurs clients de conserver, pour leur compte, les moyens d'accès à leurs crypto-actifs, à savoir leurs clés cryptographiques privées. Parmi les leaders du marché, il est possible de citer des compagnies comme Binance (maltaise), Blockchain.com (anglaise), Coinbase (américaine), Coinhouse (française), GreenAddress (maltaise), Xapo (suisse), etc. Cependant, il convient de préciser que sont exclus de cette définition les fournisseurs de portefeuilles dits fournisseurs de solutions de *self-custody*, tels que Ledger (française) ou Trézor (tchèque), qui vendent à leurs clients des supports de stockage amovibles (semblables à des clés USB) pour stocker leurs clés privées hors ligne. En effet, ces sociétés ne maîtrisent pas, au sens de l'article D. 54-10-1, 1°, du Code monétaire et financier, les moyens d'accès aux actifs numériques de leurs clients puisqu'ils ne détiennent ni ne contrôlent, directement ou indirectement, les clés cryptographiques de ces derniers.

Enfin, le décret d'application du 21 novembre 2019 a clarifié ce qu'il faut entendre par service d'achat ou de vente d'actifs numériques en monnaie ayant cours légal et service d'échange intra-actifs numériques. Le premier est défini à l'article D. 54-10-1, 2°, du Code monétaire et financier comme : « *le fait de conclure des contrats d'achat ou de vente pour le compte d'un tiers portant sur des actifs numériques en monnaie ayant cours légal, avec, le cas échéant, interposition du compte propre du prestataire de service* ». Le second renvoie quant à lui au : « *fait de conclure des contrats prévoyant*

*l'échange pour le compte d'un tiers d'actifs numériques contre d'autres actifs numériques, avec, le cas échéant, interposition du compte propre du prestataire de service » (C. mon. fin. art. D. 54-10-1, 3°)*

**19. – Enregistrement obligatoire** – L'article L. 54-10-3 du Code monétaire et financier soumet les fournisseurs de service de portefeuille ainsi que les plateformes d'échanges d'actifs numériques contre monnaie ayant cours légal, dite monnaie fiat, à une obligation d'enregistrement préalable auprès de l'AMF. Cet enregistrement permet de s'assurer que ces derniers remplissent effectivement les obligations LCB auxquels ils sont soumis en vertu de l'article L. 561-2 du Code monétaire et financier. En effet, l'enregistrement est précédé d'un double contrôle de l'ACPR, puis de l'AMF, portant notamment sur la mise en place d'une « *organisation, de procédures et d'un dispositif de contrôle interne* » propres à assurer le respect des obligations relatives à la lutte contre le blanchiment de capitaux (C. mon. fin. art. L. 54-10-3).

Il convient de souligner que les plateformes d'échange intra-cryptos ne sont pas visées par la cinquième directive anti-blanchiment (2018/843) et ne figurent pas parmi les assujettis aux obligations LCB listées à l'article L. 561-2 du Code monétaire et financier. L'AMF contrôlera le dispositif LCB de ces plateformes à la condition qu'elles sollicitent l'agrément optionnel prévu à l'article L. 54-10-5 du Code monétaire et financier. Cependant, il convient de préciser que cette réglementation est amenée à évoluer au regard de l'obligation faite au Gouvernement (après avis de la Banque de France, de l'ACPR et de l'AMF) de remettre au Parlement, avant le 23 novembre 2020, un rapport destiné à étudier l'opportunité de rendre obligatoire cet agrément au vu de l'avancement des débats européens, des recommandations du GAFI et du développement international du marché des actifs numériques<sup>97</sup>.

En tout état de cause, lorsque le contrôle de l'AMF a lieu, son effectivité est assurée d'une part, par les nombreux éléments, destinés à prouver la réalité et l'étendue du dispositif anti-blanchiment, que doit contenir le dossier d'enregistrement ou d'agrément<sup>98</sup>, d'autre part, par l'octroi à l'AMF d'un droit de communication de tout document ou toutes informations utiles à l'exercice de sa mission (C. mon. fin. art. L. 54-10-3).

---

<sup>97</sup> Art. 86 de la loi PACTE ; MARRAUD DES GROTTES Gaëlle, « Loi PACTE : point sur l'encadre des prestataires de services sur actifs numériques », *Wolters Kluwer France - Actualités du droit*, 23 mai 2019.

<sup>98</sup> Les éléments relatifs au dispositif anti-blanchiment devant être contenus dans le dossier d'enregistrement ou d'agrément sont listés dans l'instruction 2019-23 de l'AMF.

Aujourd'hui, tous les *wallets providers* et les plateformes d'échanges fiat-crypto ayant commencé leur activité à compter du 24 mai 2019 doivent obligatoirement, au préalable, s'enregistrer auprès de l'AMF ; les autres ont jusqu'au 18 décembre 2020 pour se mettre en conformité<sup>99</sup>. Concrètement, la procédure d'enregistrement se matérialise par l'envoi d'un dossier, contenant un certain nombre d'informations, à l'AMF, qui procède ensuite à son instruction. L'AMF transmet ensuite le dossier, dans un délai de cinq jours ouvrés, à l'Autorité de Contrôle Prudentiel et de Résolution (ACPR) pour avis. L'ACPR dispose alors d'un délai de trois mois à compter de la réception du dossier complet pour transmettre son avis à l'AMF qui, dans un délai de six mois, prendra la décision, ou non, d'enregistrer le requérant (C. mon. fin. art. D. 54-10-3). L'obligation d'enregistrement s'avère persuasive puisque les prestataires qui exerceraient sans avoir été, au préalable, enregistrés par l'AMF encourent une peine de deux ans d'emprisonnement et 30 000 € d'amende (C. mon. fin. art. L. 572-23). De plus, le fait de communiquer à l'AMF des renseignements inexacts est passible d'une peine d'un an d'emprisonnement et 15 000 € d'amende (C. mon. fin. art. L. 572-24).

Enfin, l'AMF peut d'office ou à l'initiative de l'ACPR radier tout prestataire qui ne respecterait plus ses obligations en matière de lutte contre le blanchiment (C. mon. fin. art. L. 54-10-1). Cette faculté lui est également reconnue s'agissant du retrait, à titre temporaire ou définitif, de l'agrément d'un prestataire (C. mon. fin. art. L. 54-10-5).

**20. – Étendu des obligations LCB** – Conformément à l'article L. 561-2 du Code monétaire et financier, les fournisseurs de service de wallet ainsi que les plateformes d'échanges fiat-crypto sont soumis au dispositif anti-blanchiment prévu aux articles L. 561-1 à L. 561-36-4 du Code monétaire et financier.

L'effectivité de ce dispositif est contrôlée par l'AMF lors de l'instruction des demandes d'enregistrement et de visas des prestataires de services sur actifs numériques.

Ce dispositif distingue trois types d'obligations auxquels sont soumis les assujettis : l'obligation de mettre en place des systèmes d'évaluation et de gestion des risques de blanchiment, des obligations de vigilance à l'égard de la clientèle et des obligations de déclaration.

---

<sup>99</sup> Loi PACTE, art. 86, X ; AMF, « Obtenir un enregistrement / un agrément PSAN », sur *AMF* [en ligne], publié le 2 juin 2020, [https://www.amf-france.org/fr/espace-professionnels/fintech/mes-relations-avec-lamf/obtenir-un-enregistrement-un-agrement-psan-0#Liste\\_des\\_PSAN\\_enregistrés\\_auprès\\_de\\_l'AMF](https://www.amf-france.org/fr/espace-professionnels/fintech/mes-relations-avec-lamf/obtenir-un-enregistrement-un-agrement-psan-0#Liste_des_PSAN_enregistrés_auprès_de_l'AMF).

– **L’obligation de mettre en place des systèmes d’évaluation des risques** – L’approche par les risques est le concept central du dispositif préventif de lutte contre le blanchiment de capitaux. Figurant à la première place des recommandations du GAFI, elle consiste, en partant d’un socle d’obligations de vigilance, à les adapter (à la hausse ou à la baisse) au regard des risques de blanchiment induits par chaque opération<sup>100</sup>.

Pour mettre en œuvre cette approche, les prestataires de services sur actifs numériques ont l’obligation de mettre en place un dispositif d’évaluation et de gestion des risques de blanchiment en tenant notamment compte : « *des risques associés à la clientèle, à la nature des produits et des services fournis, aux canaux de distribution envisagés et aux zones géographiques d’activité*<sup>101</sup> ». Enfin, ils ont l’obligation de désigner une personne responsable de la mise en œuvre de ce dispositif (C. mon. fin. art. L. 561-32).

– **Les obligations de vigilance à l’égard de la clientèle** – Les obligations de vigilance à l’égard de la clientèle (C. mon. fin. art. L. 561-4-1 à L. 561-14-2) ont pour finalité de permettre aux assujettis de détecter des anomalies dans les relations d’affaire avec leurs clients au regard des risques visés dans leur procédure d’évaluation interne. Ces anomalies devront faire l’objet d’investigations de la part des assujettis, et déboucher le cas échéant sur une déclaration de soupçon à TRACFIN. L’AMF contrôle également le sérieux de ces diligences clients en imposant aux requérants de les décrire dans leurs dossiers d’enregistrement ou d’agrément<sup>102</sup>.

Le dossier doit notamment comporter :

- La description des modalités d’identification et de vérification de l’identité des clients et, le cas échéant, des bénéficiaires effectifs, avant l’entrée et durant toute la durée de la relation d’affaire (C. mon. fin. art. L. 561-5, art. R. 561-5 et suiv.) ;

---

<sup>100</sup> CUTAJAR Chantal, *Fascicule 10 : blanchiment - prévention du blanchiment*, JurisClasseur Pénal des Affaires, Lexis Nexis, 24 juillet 2020, mis à jour le 31 janvier 2017.

<sup>101</sup> AMF, *Instruction AMF - DOC-2019-23 - Régime applicable aux prestataires de services sur actifs numériques*, 3 juin 2019, 5 p.

<sup>102</sup> *Ibid.*

- La description des mesures de vigilances complémentaires lorsque le client est à distance ou est une personne politiquement exposée (C. min. fin. art. L. 561-10 tenant notamment aux mesures renforcées de certification et de vérification de l'identité du client) ;
- La description des procédures permettant de distinguer les relations d'affaires et les clients occasionnels, notamment pour les activités de change ;
- La description des procédures permettant d'identifier les clients réalisant des opérations d'échange entre actifs numériques dont la plus élevée des contre-valeurs en monnaie ayant cours légal excède 1000 euros ;
- La description des éléments d'information recueillis et vérifiés au titre de la connaissance du client (identité adresse du domicile, activités professionnelles, revenus<sup>103</sup>, etc.) ou de la relation d'affaires (provenance et destination des fonds, justification économique<sup>104</sup>, etc.)

– **L'obligation de déclaration à Tracfin** – Enfin, les prestataires de service sur actifs numériques doivent porter une attention particulière à toute opération paraissant être liée au blanchiment, et notamment celle particulièrement complexe ou d'un montant inhabituellement élevé ou ne paraissant pas avoir de justification économique ou d'objet licite (C. mon. fin. art. L. 561-10-2). En présence d'opération portant sur des sommes dont ils savent, soupçonnent ou ont de bonnes raisons de soupçonner qu'elle provienne notamment d'une infraction de blanchiment de capitaux, les prestataires ont l'obligation de la déclarer, dès sa détection, à la cellule de renseignement financier nationale (C. mon. fin. art. L. 561-15). Là encore, l'AMF exige des prestataires de services sur actifs numériques de détailler leurs dispositifs relatifs aux opérations suspectes afin d'en contrôler la pertinence<sup>105</sup>.

En définitive, les prestataires de service sur actifs numériques, à l'exception des plateformes d'échange intra-cryptos, sont soumis aux mêmes obligations de vigilance que les établissements financiers dont l'effectivité est contrôlée par l'AMF et l'ACPR, voir uniquement par l'AFM pour les prestataires sollicitant le visa optionnel.

---

<sup>103</sup> Art. 1<sup>er</sup> de l'arrêté du 2 septembre 2009 pris en application de l'art. R. 561-12 du Code monétaire et financier

<sup>104</sup> *Ibid.*

<sup>105</sup> AMF, *Instruction AMF - DOC-2019-23 - Régime applicable aux prestataires de services sur actifs numériques*, 3 juin 2019,



## **B. L'assujettissement des offres au public de jetons aux obligations de lutte contre le blanchiment**

**21. – Contexte** – La loi n°2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises, dite loi PACTE, affichait l'ambition de transformer le « *modèle économique français pour l'adapter aux réalités du 21<sup>ème</sup> siècle*<sup>106</sup> ». Pour cela, la loi envisageait de « *mobiliser tous les leviers disponibles*<sup>107</sup> » afin de « *faciliter l'accès aux marchés du financement à toutes les entreprises*<sup>108</sup> ».

Dans ce contexte, l'article 26 du projet de loi PACTE avait pour objet d'établir un cadre juridique clair pour les offres au public de jetons (ICO). Pour rappel, l'ICO est une opération de levée de fonds, réalisée au moyen de la technologie blockchain, destinée à financer le projet porté par l'émetteur et donnant lieu à une émission de jetons numériques (appelés *tokens*) auxquelles les investisseurs souscrivent généralement en crypto-actifs<sup>109</sup>. Les jetons numériques se distinguent en fonction des droits qu'ils accordent à leur détenteur ; les *utility tokens* ayant vocation à octroyer un droit d'usage sur les biens et/ou services de l'émetteur, et les *security tokens* conférant des droits politiques et financiers. Ces derniers, présentant les caractéristiques d'un titre financier (sans pour autant répondre aux éléments de définition des titres financiers), ont dès lors été exclus de cette réglementation, leur privilégiant la soumission au régime de l'offre au public de titres financiers (introduction en bourse), et notamment la réglementation « prospectus »<sup>110</sup>.

Il convient donc de distinguer les *utility tokens*, qui entrent dans le champ d'application de la loi PACTE, des *security tokens*, qui sont soumis à la réglementation relative aux titres financiers traditionnels.

---

<sup>106</sup> Exposé des motifs de la loi PACTE.

<sup>107</sup> *Ibid.*

<sup>108</sup> *Ibid.*

<sup>109</sup> BROSSET Jérôme, LORENTZ Philippe, BARBET-MASSIN Alice, « Les activités sur actifs numériques issues de la loi PACTE », *Revue Lamy droit des affaires*, n°151, 1<sup>er</sup> septembre 2019.

<sup>110</sup> MARRAUD DES GROTTES Gaëlle, « Anne Maréchal, directrice des affaires juridiques de l'AMF : Avec ce visa optionnel, nous espérons créer un écosystème attractif qui permette d'attirer en France les beaux projets d'ICO », *Wolters Kluwer France - Actualités du droit*, 22 mai 2019 ;

AMF, « La réglementation applicable aux prospectus », sur *AMF* [en ligne], publié le 21 février 2020, [https://www.amf-france.org/fr/actualites-publications/dossiers-thematiques/prospectus#:~:text=L'article%2046\(3\),21%20juillet%202019%2C%20la%20date](https://www.amf-france.org/fr/actualites-publications/dossiers-thematiques/prospectus#:~:text=L'article%2046(3),21%20juillet%202019%2C%20la%20date).

**22. – Visa optionnel institué par la loi PACTE** – L'article 26 du projet de loi PACTE avait pour objectif « *de fournir aux souscripteurs de jetons les moyens suffisants pour distinguer les acteurs qui mettent en œuvre des diligences en matière d'information, d'identification et de connaissance du client et ceux qui ne respectent aucune règle*<sup>111</sup> ». Pour se faire, les porteurs de projets qui le souhaitent peuvent solliciter auprès de l'AMF un visa optionnel, gage de leur sérieux. Selon Madame Anne Maréchal, directrice des affaires juridique de l'AMF, les acteurs percevraient ce visa comme : « *une possibilité de se différencier des émetteurs moins scrupuleux* » et leur feraient bénéficier d'un « *avantage compétitif important*<sup>112</sup> ».

Il convient cependant de préciser que cette possibilité est offerte aux seules offres de jetons ouvertes à la souscription par plus de 150 personnes agissant pour compte propre (C. mon. fin. art. L552-3 ; RG de l'AMF, art. 711-2).

Pour obtenir ce visa, les porteurs de projet doivent remplir diverses conditions tenant notamment, à la mise en place d'un dispositif de lutte anti-blanchiment conformément aux exigences légales et, à l'existence d'un lien de rattachement à la France. Cette dernière condition complète le dispositif anti-blanchiment dès lors que l'obligation, pour le porteur de projets, de se constituer sous la forme d'une personne morale établie ou immatriculée en France (C. mon. fin. art. L. 552-5) facilitera les échanges d'informations avec les autorités compétentes dans le cadre d'une enquête ou d'une instruction portant sur des faits de blanchiment.

Concrètement, l'instruction du dossier par l'AMF consistera à vérifier le respect de quatre exigences légales. La première exigence, telle que développé plus haut, tient à la forme juridique de l'émetteur et à son lien de rattachement à la France (C. mon. fin. art. L. 552-5). La seconde réside dans la mise en place d'un dispositif permettant d'assurer la fiabilité, l'opérabilité et l'efficacité de la sauvegarde des actifs recueillis dans le cadre de l'offre de jetons<sup>113</sup> (RG AMF, art. 712-7). La troisième consiste en l'établissement d'un document d'information, dit *whitepaper*, « *destiné à informer et protéger les*

---

<sup>111</sup> Exposé des motifs de la loi PACTE.

<sup>112</sup> MARRAUD DES GROTTES Gaëlle, *op. cit.*

<sup>113</sup> BROSSET Jérôme, LORENTZ Philippe, BARBET-MASSIN Alice, « Les activités sur actifs numériques issues de la loi PACTE », *Revue Lamy droit des affaires*, n°151, 1<sup>er</sup> septembre 2019.

*investisseurs en leur apportant tous éléments utiles* » (C. mon.fin. art. L. 552-4; RG AMF art. 712-1 *suiv.*). Enfin, la dernière exigence repose sur la mise en place du dispositif de lutte anti-blanchiment.

En ce sens, l'AMF contrôle, dans le cadre de l'instruction des demandes de visa, les mesures anti-blanchiment mis en place par les émetteurs de jetons. En pratique, elle porte une attention particulière aux éléments suivants<sup>114</sup> :

- La mise en place d'un dispositif d'évaluation et de gestion des risques permettant de déterminer le profil de risque de chaque souscripteur et le niveau des mesures de vigilance à respecter ;
- La mise en œuvre de mesures de vigilance permettant l'identification et la vérification de l'identité des souscripteurs pour toute souscription d'un montant supérieur à 1 000 euros ou pour toute souscription, y compris sous le seuil de 1 000 euros, dont l'émetteur pourrait soupçonner qu'elle participe au blanchiment des capitaux ou au financement du terrorisme ;
- La mise en œuvre de mesures de vigilance permettant l'identification de l'origine des fonds en cas de souscription d'un montant inhabituellement élevé ou ne paraissant pas avoir de justification économique ou d'objet licite ;
- La nomination d'un déclarant Tracfin.

Enfin, si l'émetteur a recours à des prestataires externes pour la réalisation de ces diligences, l'AMF procède au contrôle du caractère sérieux des exigences posées dans le contrat de prestations<sup>115</sup>.

A l'issue de l'examen du dossier, l'AMF peut décider d'apposer son visa sur le document d'information de l'offre au public de jetons ou de le refuser (RG AMF, art. L. 712-9). Étant précisé que l'accord de l'AMF emporte publication de l'offre parmi la liste blanche figurant sur son site internet, et que son refus doit être accompagné des éléments ayant motivé sa décision<sup>116</sup>.

---

<sup>114</sup> AMF, *Réglementation LCB-FT : précisions de l'AMF sur les principales mesures devant être mises en œuvre par les émetteurs de jetons sollicitant un visa optionnel*.

<sup>115</sup> MARRAUD DES GROTTES Gaëlle, *op. cit.*

<sup>116</sup> AMF, *Instruction - DOC-2019-06, 3.7. Délivrance du visa*, juin 2019, 7 p. ; BROSSET Jérôme, LORENTZ Philippe, BARBET-MASSIN Alice, *op. cit.*

Il convient ici d'apporter deux précisions, d'une part le visa est délivré pour la seule et unique offre instruite par l'AMF (il ne porte donc pas sur l'émetteur mais sur l'opération) et n'est valable que pour une durée ne pouvant excéder 6 mois (RG AMF, art. 712-10), d'autre part, les opérations n'ayant pas obtenu le visa optionnel demeurent légales<sup>117</sup>.

Enfin, l'AMF peut décider de retirer son visa si l'offre ne présente plus les garanties prévues en matière de lutte contre le blanchiment (C. mon. fin. art. L. 552-6). L'émetteur dispose alors d'un délai de trois jours ouvrés pour faire connaître par écrit ses observations.

Pour finir, la commission des sanctions de l'AMF peut sanctionner toute personne se prévalant du visa sans le posséder (C. mon. fin. art. L. 621-15-II, e).

---

<sup>117</sup> AMF, « Obtenir un visa pour une offre au public de jetons (ICO) », sur *AMF* [en ligne], publié le 16 janvier 2020, <https://www.amf-france.org/fr/espace-professionnels/fintech/mes-relations-avec-lamf/obtenir-un-visa-pour-une-ico/preparer-une-ico>.

Pour conclure, la France a fait le choix d'assujettir les prestataires de services sur actifs numériques aux mêmes obligations LCB que les acteurs financiers traditionnels. Ces obligations « *pas entièrement inadaptées* » mériteraient pour certains auteurs d'être modulées « *au regard des spécificités de ces actifs*<sup>118</sup> ».

En ce qui concerne les services sur actifs numériques, l'Union Européenne a opté pour un régime différencié (enregistrement obligatoire ou visa optionnel), comprenant un assujettissement obligatoire au dispositif de LCB, contrairement à la ville de New-York ou encore le Japon qui fonctionnent sur la base d'un agrément unique<sup>119</sup>. Cette différenciation de régimes est présentée, par le rapport Landau, comme un frein à l'attractivité de la place financière européenne. La solution résiderait dans la création d'un agrément unique européen qui emporterait l'obligation de respecter un socle minimal d'exigences en matière de LCB, modulé en fonction des activités exercées. Cette « Euro BitLicense », à même de concurrencer les Bitlicences new-yorkaise et japonaise, permettait de « *rétablir les conditions d'une concurrence entre les États membres et avec les autres grandes places financières*<sup>120</sup> ».

Plus précisément, le régime des offres au public de jetons est scindé entre les émissions de jetons de sécurité et les émissions de jetons d'utilité. Les premières sont soumises au régime des offres au public de titres financiers, et à ce titre, à la directive « prospectus » (2003/71/CE) qui apparaît à la fois inadaptée et trop lourde aux spécificités de ce type d'opération. Anne Maréchal, directrice des affaires juridiques de l'AMF, déclarait à l'occasion d'une interview de mai 2019, n'avoir : « *reçu aucun porteur de projet de STO (security token offering) ayant déposé un projet de prospectus* » en raison, à son sens, de « *difficultés juridiques et techniques sérieuses* » liées à une réglementation n'ayant pas été pensée pour la blockchain<sup>121</sup>. Les émetteurs de jetons d'utilité ont, pour leur part, la possibilité d'obtenir un agrément optionnel qui emportera l'obligation de se soumettre aux exigences légales de lutte anti-blanchiment.

---

<sup>118</sup> POLROT Simon, « La régulation LCB-FT face à l'émergence des cryptomonnaies », *Revue internationale de la compliance et de l'éthique des affaires*, février 2020, n°1, étude 38.

<sup>119</sup> LANDAU Jean-Pierre avec la collaboration de GENAIS Alban, *Les crypto-monnaies*, Rapport au Ministre de l'Économie et des Finances, 4 juillet 2018, p. 60.

<sup>120</sup> *Ibid.*

<sup>121</sup> MARRAUD DES GROTTES Gaëlle, « Anne Maréchal, directrice des affaires juridiques de l'AMF : Avec ce visa optionnel, nous espérons créer un écosystème attractif qui permette d'attirer en France les beaux projets d'ICO », *Wolters Kluwer France - Actualités du droit*, 22 mai 2019

Ces régimes optionnels encourent toutefois le risque, d'une part, que la lourdeur des obligations LCB qui leurs sont associées dissuade les prestataires de tout demande d'agrément optionnel<sup>122</sup>, et, d'autre part, que l'exclusion des plateformes d'échange intra-cryptos du champ des assujettis au dispositif LCB constitue un obstacle à la traçabilité des fonds<sup>123</sup>. Il est toutefois possible d'avancer trois arguments qui tempèrent ces critiques. D'une part, les prestataires de services sur actifs numériques enregistrés ou agréés, qui feraient face à un refus d'ouverture de compte bancaire, bénéficient d'une voie de recours auprès de l'ACPR qui peut, en outre, proposer au demandeur de saisir en son nom et pour son compte la Banque de France d'une demande de désignation d'un établissement de crédit (C. mon. fin. art. D. 312-23). Ce « droit au compte » permet de rendre attractif les demandes optionnelles d'assujettissement des acteurs à l'AMF tant il peut être difficile pour les porteurs de projets *blockchain* d'ouvrir un compte bancaire<sup>124</sup>. De plus, seuls les prestataires agréés peuvent se livrer « *aux activités de quasi-démarchage via des formulaires de contact en ligne et des opérations de sponsoring ou de mécénat*<sup>125</sup> ». D'autre part, les risques de blanchiment étant focalisés sur les services servant de passerelles entre l'économie légale et l'économie souterraine puisqu'on : « *peine à distinguer l'intérêt de blanchir un actif numérique dans un autre actif numérique à partir du moment où le passage en monnaie ayant cours légal est soumis à un dispositif LCB/FT*<sup>126</sup> » ; le contrôle des portes d'entrées et de sortie entre le monde des crypto-actifs et le système monétaire et financier<sup>127</sup> semble pour certains aboutir à un compromis suffisant et proportionné aux risques<sup>128</sup>. Enfin, et plus généralement, la labélisation des acteurs de l'industrie « crypto » permet aux autorités compétentes de mieux cibler le suivi et la détection d'opérations frauduleuses en distinguant les services agréés de ceux qui ne le sont pas.

---

<sup>122</sup> O'RORKE William, « La mise en œuvre des obligations LCB-F par l'industrie crypto », *Revue internationale de la compliance et de l'éthique des affaires*, février 2020, n°1, étude 38.

<sup>123</sup> Cf. *Infra*, n°35 : plateformes de conversion intra-crypto.

<sup>124</sup> MARRAUD DES GROTTES Gaëlle, « Prestataires de services sur actifs numériques : le décret est paru ! », *Wolters Kluwer France - Actualités du droit*, 22 mai 2019.

<sup>125</sup> BROSSET Jérôme, LORENTZ Philippe, BARBET-MASSIN Alice, « Les activités sur actifs numériques issues de la loi PACTE », *Revue Lamy droit des affaires*, n°151, 1<sup>er</sup> septembre 2019 ; C. conso. art. L. 222-16-1, a. ; C. conso. art. L. 222-16-2.

<sup>126</sup> O'RORKE William, *op. cit.*

<sup>127</sup> Encore faut-il pouvoir identifier les portes d'entrées et de sorties ce qui est rendu difficile par l'utilisation de certaines plateformes d'échange intra-cryptos ; Cf. *Infra*, n°35 : plateformes de conversion intra-crypto.

<sup>128</sup> O'RORKE William, Avocat fondateur du Cabinet ORWL Avocats, entretien téléphonique mené par Alexandra Puertas, le 28 mai 2020 ; STACHTCHENKO Alexandre, Co-fondateur et Directeur général de Blockchain Partner, entretien téléphonique mené par Alexandra Puertas, le 27 mai 2020.

En outre, la réglementation des prestataires de services sur actifs numériques appelle un double défi : accompagner la technologie pour permettre l'émergence de champions français et attirer les acteurs étrangers, tout en protégeant la société contre les risques de son utilisation à des fins de blanchiment. Le législateur doit donc au préalable identifier les risques de blanchiment afin de moduler la réglementation LCB conformément au principe de proportionnalité et ne pas appliquer aveuglement « *un principe de précaution généralisé*<sup>129</sup> ». En effet, il n'est pas s'en rappeler que l'assujettissement des prestataires au dispositif LCB induit des compétences et des coûts financiers pouvant être un frein à l'apparition de nouveaux acteurs sur le marché, et de ce fait, propice à une concentration du secteur<sup>130</sup>.

Pour finir, la portée mondiale des crypto-actifs combinée à des processus infractionnels de plus en plus complexes, impliquant plusieurs entités souvent réparties sur différents états, appellent à une harmonisation au niveau européen et international des obligations LCB. En ce sens, le Groupe d'Action Financière (GAFI) a émis le 21 juin 2019, à destination de ses 39 états membres, des recommandations sur les actifs numériques<sup>131</sup>. Cependant, il convient une fois de plus de se demander si les activités liées aux crypto-actifs font peser un risque de blanchiment tel qu'il justifierait un assujettissement obligatoire de tous les acteurs et la mise en place d'une « *Travel Rule*<sup>132</sup> » comme le préconise le GAFI.

---

<sup>129</sup> POLROT Simon, « La régulation LCB-FT face à l'émergence des cryptomonnaies », *Revue internationale de la compliance et de l'éthique des affaires*, février 2020, n°1, étude 38.

<sup>130</sup> R. Remy, « AMLD5 aux Pays-Bas : un désastre pour les petites crypto-entreprises », *Journal du coin* [en ligne], 29 avril 2020, <https://journalducoin.com/regulation/loi-amld5-pays-bas-desastre-pour-les-petites-crypto-entreprises>.

<sup>131</sup> GROUPE D'ACTION FINANCIERE, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, juin 2019.

<sup>132</sup> La « Travel Rule » (recommandation n°16 du GAFI) oblige tout prestataire qui effectue un virement à communiquer automatiquement au prestataire destinataire les informations sur l'identité du client qui en est à l'origine.

## II. L'incrimination du blanchiment de capitaux au moyen de crypto-actifs

Étudier l'incrimination du blanchiment de capitaux au moyen de crypto-actifs revient à étudier les éléments constitutifs de l'infraction (A) avant de s'intéresser aux processus infractionnels (B).

### A. Les éléments constitutifs

**23. – Existence préalable d'une infraction principale** – Le blanchiment de capitaux peut être défini comme l'opération ayant pour finalité de faire disparaître l'origine des fonds provenant d'un crime ou d'un délit afin de les réintégrer dans le circuit financier légal (C. pén. art. 324-1 du Code pénal). Le blanchiment est donc une infraction de conséquence dont la constitution nécessite la préexistence d'une infraction principale dite aussi originaire, primaire ou encore infraction source<sup>133</sup>. L'article 324-1 du Code pénal précise que cette infraction doit être un délit ou un crime.

La généralité des termes employés permet d'étendre le champ d'application de l'infraction générale de blanchiment à toute infraction principale, qu'elle soit définie par le code pénal, par d'autres codes ou par des lois demeurées hors codification<sup>134</sup>, pourvue qu'elle soit punie d'une peine d'emprisonnement et qu'elle ait procuré à son auteur un profit ou qu'elle ait généré un produit susceptible d'être blanchi<sup>135</sup>. Le législateur de l'époque avait alors en tête d'éviter tout obstacle à la répression que peut constituer la difficulté de rapporter la preuve de cette infraction d'origine. Toutes les propositions tendant à limiter le champ des infractions sources ont par conséquent été rejetées lors des débats parlementaires précédant l'adoption de la loi n°96-392 du 13 mai 1996<sup>136</sup>.

– **Preuve de l'infraction principale** – La circulaire d'application de la loi, datée du 10 juin 1996 (n°96/11 G), encore en vigueur aujourd'hui, demandait au parquet d'établir : « *que les fonds blanchis provenaient d'un crime ou d'un délit, quel qu'il soit* ». Les autorités de poursuites avaient interprété la circulaire comme nécessitant de rapporter la preuve de l'infraction source en tous ses éléments

---

<sup>133</sup> DAURY-FAUVEAU Morgane, *Fascicule 20 : blanchiment - conditions et constitution*, JurisClasseur Pénal des Affaires, Lexis Nexis, 2 mai 2020, 10°.

<sup>134</sup> MATSOPOULOU Haritini (dir.), MASCALA Corinne (dir.), *Le Lamy droit pénal des affaires*, Wolters Kluwer, 2020, 1737°.

<sup>135</sup> CUTAJAR Chantal, *Fascicule 20 : blanchiment - éléments constitutifs - répression*, JurisClasseur Pénal des Affaires, Lexis Nexis, 15 février 2010, mis à jour le 27 janvier 2020.



constitutifs. Cette analyse fut confirmée dans un arrêt rendu le 25 juin 2003<sup>137</sup> par la chambre criminelle de la Cour de cassation.

Cependant, dès 2004, la haute juridiction assouplissait sa jurisprudence en approuvant une Cour d'appel d'avoir jugé que le blanchiment : « *doit entraîner de la part de la juridiction de jugement la constatation de l'origine criminelle ou délictuelle des fonds*<sup>138</sup> ». Cette interprétation est aujourd'hui constante, la chambre criminelle ayant eu l'occasion de la confirmer depuis<sup>139</sup>. Il appartient donc désormais aux autorités de prouver l'origine infractionnelle des biens ou revenus, sans avoir à caractériser l'infraction source en tous ses éléments.

Qui plus est, la loi n° 2013-1117 du 6 décembre 2013 relative à la lutte contre la fraude fiscale et la grande délinquance économique et financière est allée plus loin en insérant dans le code pénal un nouvel article 324-1-1 qui pose une présomption d'origine illicite des biens ou revenus : « *dès lors que les conditions matérielles, juridiques ou financières de l'opération de placement, de dissimulation ou de conversion ne peuvent avoir d'autre justification que de dissimuler l'origine ou le bénéficiaire effectif de ces biens ou revenus* ». Saisie d'une question prioritaire de constitutionnalité, la chambre criminelle de la Cour de Cassation a jugé qu'il n'y avait pas lieu de la renvoyer au Conseil constitutionnel dès lors que : « *d'une part, la présomption d'illicéité, instituée par le texte contesté, de l'origine des biens ou revenus sur lesquels porte le délit de blanchiment prévu par l'article 324-1 du Code pénal n'est pas irréfragable, et d'autre part, nécessite, pour sa mise en œuvre, la réunion de conditions de fait ou de droit faisant supposer la dissimulation de l'origine ou du bénéficiaire effectif de ces biens ou revenus*<sup>140</sup> ».

Cette présomption présente une utilité tout particulière en terme de répression du blanchiment commis aux moyens de crypto-actifs tant l'utilisation de procédés complexes visant à opacifier l'origine infractionnelle des fonds est fréquente voir systématique<sup>141</sup>.

---

<sup>137</sup> Cass. crim., 25 juin 2003, n°02-86.182.

<sup>138</sup> Cass. crim., 7 avril 2004, n°03-84.889.

<sup>139</sup> Cass. crim. 8 sept. 2010, n°09-86.261 ; 17 fév. 2016, n°15-80.050 ; 6 déc. 2017, n°16-84.31.

<sup>140</sup> Cass. crim. 9 déc. 2015, n°15-90.019

<sup>141</sup> Cf. infra. n°33.

– **Caractère autonome de l’infraction principale** – Le caractère « *général, distinct, et autonome* » de l’infraction source a été consacré par la jurisprudence à l’occasion d’une question portant sur l’auto-blanchiment, soit celle du cumul de la qualité d’auteur de l’infraction source et de celle d’auteur de l’infraction de blanchiment consécutive (Cass. crim., 25 juin 2003, n°02-86.182). Par la suite, la chambre criminelle n’a eu de cesse de préciser les conséquences de ce principe d’autonomie.

Dans un arrêt en date du 20 février 2008 (n°07-82.977), elle a jugé que le principe d’autonomie de l’infraction de blanchiment a pour conséquence de ne pas soumettre sa poursuite aux conditions propres de l’infraction-source. Ainsi, la mise en mouvement de l’action publique pour des faits de blanchiment de fraude fiscale ne nécessite pas une plainte préalable de l’Administration fiscale, après avis conforme de la Commission des infractions fiscales, telle que nécessaire pour poursuivre le délit de fraude fiscale.

Au fil des décisions, la chambre criminelle a précisé que l’absence ou l’impossibilité de poursuivre l’infraction source<sup>142</sup> n’a aucune incidence sur les poursuites exercées contre l’auteur du blanchiment subséquent<sup>143</sup>.

**24. – Élément matériel** – L’article 324-1 du Code pénal réprime deux formes de blanchiment dont les éléments matériels se distinguent l’une de l’autre. Il s’agit d’une part de la facilitation, par tout moyen, de la justification mensongère de l’origine des biens ou des revenus de l’auteur d’un crime ou d’un délit (C. pén., art. 324-1, al. 1er) et, d’autre part, du concours à une opération de placement, dissimulation et conversion du produit d’un crime ou d’un délit (C. pén., art. 324-1, al. 2).

La question s’est posée de savoir si l’élément matériel du blanchiment pouvait être constitué par abstention compte tenu de sa proximité avec la complicité par aide ou assistance<sup>144</sup>. En effet, si cette complicité suppose en principe, un acte positif, la jurisprudence a exceptionnellement admis qu’elle pouvait être réalisée par abstention lorsque pesait sur le complice une obligation d’agir<sup>145</sup>. Toutefois, la doctrine s’accorde à dire que le blanchiment est une infraction de commission qui requiert un acte

---

<sup>142</sup> Extinction de l’action publique par le décès de l’auteur, Cass. crim., 31 mai 2012, n°12-80.715 ; par le jeu de la prescription extinctive, Cass. crim., 17 déc. 2004, n°13-86.477 ; impossibilité de poursuivre l’infraction-source devant une juridiction française, Cass. crim., 9 déc. 2015, n°15-83.204.

<sup>143</sup> MATSOPOULOU Haritini (dir.), MASCALA Corinne (dir.), *op. cit.*, 1795°.

<sup>144</sup> DAURY-FAUVEAU Morgane, *op. cit.*, 35°.

<sup>145</sup> Cass. crim., 21 octobre 1971, n°71-90.754 ; Cass. crim., 13 septembre 2016, n°15-85.046.

positif qui, soit facilite la justification mensongère de l'origine des biens illicites, soit matérialise un concours à une opération de placement, dissimulation ou conversion du produit de l'infraction source<sup>146</sup>.

– **Fait de faciliter la justification mensongère de l'origine des biens ou des revenus** – L'alinéa 1<sup>er</sup> de l'article 324-1 du Code pénal dispose que le blanchiment peut être constitué par : « *le fait de faciliter, par tout moyen, la justification mensongère de l'origine des biens ou des revenus de l'auteur d'un crime ou d'un délit ayant procuré à celui-ci un profit direct ou indirect* ».

La généralité du terme « *faciliter* » permet de considérer que l'infraction de blanchiment peut être caractérisée par tout commencement de justification mensongère bien qu'inachevée ou objectivement imparfaite<sup>147</sup>. Le terme de « *justification mensongère* » permet également de circonscrire de manière large les faits matériels d'autant plus qu'elle peut être réalisée par « *tous moyens* »<sup>148</sup>. Enfin, la répression de cette typologie de blanchiment est facilitée par le fait que la preuve de l'identité du produit procuré par l'infraction et celui dont l'origine est faussement justifiée n'a pas à être rapportée. La doctrine majoritaire considère que cette identité n'est pas un élément constitutif de l'infraction de blanchiment puisque le texte n'exige pas de démontrer le lien entre les biens ou les revenus obtenues par l'accomplissement de l'infraction source et les biens ou revenus blanchis<sup>149</sup>.

– **Concours à une opération de placement, dissimulation ou conversion d'un produit illicite** – L'alinéa 2 de l'article 324-1 du Code pénal vise : « *le fait d'apporter un concours à une opération de placement, de dissimulation ou de conversion du produit direct ou indirect d'un crime ou d'un délit* ». Ces trois formes de concours peuvent être apportés alternativement ou cumulativement<sup>150</sup>.

Il convient également de préciser que, pour cette forme de blanchiment, la chambre criminelle de la Cour de cassation a expressément admis la possibilité de cumuler la qualité d'auteur de l'infraction

---

<sup>146</sup> REBUT Didier, « Manquement du banquier à ses obligations professionnelles et commission du délit de blanchiment », *Banque et droit*, 2003, n°88, 11 p. ; BOULOC Bernard, « De quelques aspects du délit de blanchiment », *Revue de droit bancaire et financier*, 2002, 152 p.

<sup>147</sup> MATSOPOULOU Haritini (dir.), MASCALA Corinne (dir.), *op. cit.*, 1799°.

<sup>148</sup> CUTAJAR Chantal, *op. cit.*

<sup>149</sup> CONTE Philippe, *Droit pénal spécial*, 6<sup>e</sup> édition, LexisNexis, 5 septembre 2019.

<sup>150</sup> DAURY-FAUVEAU Morgane, *op. cit.*, 42°.

principale et de blanchisseur du produit direct ou indirect tirée de celle-ci<sup>151</sup> pourvu que « *les faits ne procèdent pas de manière indissociable d'une action unique caractérisée par une seule intention coupable*<sup>152</sup> ».

Cette seconde typologie de blanchiment est également définie largement ce qui permet d'appréhender toutes les formes de concours possibles, autant la réalisation d'actes matériels, intellectuels, ou l'apport de conseils et d'instructions. Plus précisément, l'auteur doit apporter son concours à une opération de placement, de dissimulation ou de conversion du produit d'un crime ou d'un délit. Il faut de nouveau préciser que le texte d'incrimination n'impose pas une identité de fait entre l'avantage économique tiré de l'infraction et les éventuels produits de substitution acquis grâce au gain illicite dès lors que la preuve de « *la chaîne des transformations* » peut être rapportée<sup>153</sup>. Enfin, à défaut de précisions fournies par le texte d'incrimination, il convient de définir ce qu'il faut entendre par opération de placement, de dissimulation ou de conversion.

La subtilité de la nuance de sens entre ces trois opérations conduit la chambre criminelle de la Cour de cassation à sanctionné « *toutes opérations ayant pour finalité de recycler des fonds illicites*<sup>154</sup> » sans distinguer l'opération précise à laquelle l'auteur a apporté son concours<sup>155</sup>. Alors que la placement désigne l'emploi de sommes acquises illégalement dans le système financier légal, la conversion consiste à transformer le produit criminel en autre chose, et la dissimulation à opacifier l'origine du produit afin d'empêcher toute traçabilité<sup>156</sup>.

**25. – Élément moral** – Enfin, le blanchiment est une infraction intentionnelle (C. pén. art. 121-3) dont la constitution nécessite de rapporter la preuve de la connaissance, par l'auteur, de l'origine illicite des fonds et sa volonté de participer tout de même à leur blanchiment<sup>157</sup>. A ce titre, la chambre criminelle de la Cour de cassation n'exige pas que le blanchisseur ait eu connaissance de l'infraction ayant généré

---

<sup>151</sup> Cass. crim., 14 janvier 2004, n°03-81.165.

<sup>152</sup> Cass. crim., 7 décembre 2016, n°15-87.335.

<sup>153</sup> MATSOPOULOU Haritini (dir.), MASCALA Corinne (dir.), *op. cit.*, 1801°.

<sup>154</sup> *Ibid.*

<sup>155</sup> Cass. crim., 26 janv. 2001, n°10-84.081 ; Cass. crim., 17 nov. 2010, n°09-88.751 ; Cass. crim., 17 déc. 2014, n°13-86.477.

<sup>156</sup> DAURY-FAUVEAU Morgane, *op. cit.*, 45° et suiv.

les fonds à blanchir, et juge que la simple conscience de leur caractère illicite suffit à caractériser l'élément intentionnel<sup>158</sup>. Enfin, consciente des difficultés de rapporter la preuve de la connaissance du caractère illicite des fonds par l'auteur, la Cour de cassation a considéré que cette connaissance peut « résulter de circonstances de fait qui, sans montrer irréfutablement la mauvaise foi, la font à tout le moins présumer ». Certains auteurs y voient le recours à un mécanisme de présomption judiciaire<sup>159</sup> tandis que d'autres l'analysent comme la mise en œuvre de la théorie de la connaissance obligée<sup>160</sup>.

**26. – Caractérisation du blanchiment de capitaux au moyen de crypto-actifs** – Le blanchiment de capitaux au moyen de crypto-actifs est généralement le fait d'un individu ayant commis une infraction préalable dont il en a tiré profit en actifs numériques, à l'image d'escroqueries à l'investissement en crypto-actifs ou d'extorsions commises par le biais d'attaques de *crypto-ransomwares*<sup>161</sup>. Cependant, le délinquant ayant tiré profit de son infraction en argent liquide peut également voir dans les crypto-actifs un intérêt tenant à la possibilité de les transférer rapidement vers des territoires à la surveillance financière moins importantes. Bien que le recours aux mules d'argent restent le moyen de blanchiment privilégié des délinquants pour faire transiter des fonds<sup>162</sup>, l'intensification des contrôles aux frontières voire leurs fermetures en raison de la pandémie actuelle pourrait rendre séduisant le recours aux crypto-actifs. Outre la mobilité, les crypto-actifs présentent d'une part, des avantages en matière logistique puisque la dissimulation d'une clé cryptographique est bien plus aisée que la dissimulation d'argent liquide qui échappe difficilement à l'odorat de chiens renifleurs. D'autre part, en raison de leur forte volatilité ils peuvent être considérés comme des moyens d'investissements criminels lucratifs<sup>163</sup>.

En pratique, l'utilisation de crypto-actifs à des fins de blanchiment se matérialise par des opérations de conversion intra-cryptos et d'actifs numériques en monnaie ayant cours légal (et inversement) dont le but est d'opacifier l'origine illicite des fonds afin d'empêcher toute traçabilité. Au terme d'un raisonnement par analogie, il est possible de considérer que si l'échange de billets en francs en billets

---

<sup>158</sup> Cass. crim., 3 déc. 2003, n°02-84.646 ; 11 oct. 2011, n°10-87.503 ; 20 mai 2015, n°14-81.964 ; 18 janv. 2017, n°15-84.003.

<sup>159</sup> CUTAJAR Chantal, *op. cit.* 75°.

<sup>160</sup> SEGONDS Marc, *Blanchiment*, Dalloz, octobre 2017, mise à jour en mars 2020, 95°.

<sup>161</sup> Cf. *supra*, n°12

<sup>162</sup> EUROPOL, *Internet organised crime threat assessment 2019*, 9 octobre 2019, p. 52.

<sup>163</sup> PIERSON Frédérique, Capitaine de Police, Responsable du Bureau des avoirs criminels d'Europol, entretien téléphonique mené par Alexandra Puertas, le 10 juin 2020.

en euros<sup>164</sup> ainsi que la conversion de monnaie scripturale en monnaie fiduciaire<sup>165</sup> peuvent être analysés comme une opération de conversion au sens du deuxième alinéa de l'article 324-1 du Code pénal ; l'opération de conversion d'actifs numériques en monnaie ayant cours légal (et inversement) ou en d'autres actifs numériques constitue également une opération de conversion au sens dudit article. Par conséquent, la qualification de l'infraction ne devrait pas constituer un obstacle à la poursuite des auteurs de blanchiment au moyen de crypto-actifs.

A titre comparatif, la Cour de 1<sup>ère</sup> instance de Rotterdam, dans un arrêt en date du 14 avril 2017, a considéré que la rémunération perçue en bitcoin en échange de la vente de drogues sur internet ne suffit pas, en soit, à caractériser l'infraction de blanchiment et permet seulement de constater la possession du produit de l'infraction. Il en va cependant autrement de l'opération de conversion des bitcoins reçus en euros qui s'analyse, selon la Cour, comme un acte de dissimulation caractérisant l'infraction de blanchiment<sup>166</sup>.

En outre, deux arrêts rendus respectivement le 6 mars 2018 par la Cour de 1<sup>ère</sup> instance de Rotterdam (n°10/960005-16), et le 3 avril 2018 par la Cour de 1<sup>ère</sup> instance de *Midden-Netherland*, apportent des précisions quant à la qualification de l'élément moral du blanchiment au moyen de crypto-actifs. En effet, les juges ont considéré que l'accusé, qui s'était prêté à des activités de conversion, ne pouvait ignorer l'origine illicite des fonds blanchis dès lors qu'il utilisait différents portefeuilles pour recevoir ces fonds, que les opérations de conversion étaient réalisées pour le compte de clients, inconnus de lui, rencontrés dans des lieux publics, et portaient sur de très grosses sommes d'argent pour lesquelles il accusait un montant inhabituellement élevé de commission.

En définitive, la spécificité du blanchiment commis au moyen de crypto-actifs n'engendre pas de difficultés en termes de qualification juridique, toutefois, la complexité accrue des processus infractionnels utilisés compliquent l'appréhension de ses auteurs.

---

<sup>164</sup> Cass. crim., 12 juin 2019, n°18-83.396.

<sup>165</sup> Cass. crim., 17 juin 2015, n°14-80.977.

<sup>166</sup> EUROJUST, *Cybercrime Judicial Monitor*, 3<sup>e</sup> éd., décembre 2017, p. 19-20.

## **B. Les processus infractionnels**

Le blanchiment commis au moyen de crypto-actifs témoigne d'une dématérialisation des modes opératoires traditionnelles (1) dont la détection est rendue d'autant plus difficile par l'utilisation de techniques d'opacification des flux (2).

### **1. Les modes opératoires**

**27 – Définition** – Le terme mode opératoire ne figure ni dans le code pénal, ni dans le code de procédure pénale. Souvent employé par les juridictions et la doctrine sans le définir<sup>167</sup>, il est absent de la majorité des ouvrages de droit pénal. La page de présentation d'un colloque du 28 juin 2019 portant sur le sujet proposait de le définir comme : « *la description détaillée permettant d'atteindre un résultat*<sup>168</sup> ». En d'autres termes, la notion de mode opératoire renvoie à l'infraction en mouvement. Elle consiste en la description détaillée de l'ensemble des actions permettant la réalisation de l'infraction.

A la faveur du cyberspace, les modes opératoires du blanchiment se sont considérablement complexifiés. Leur détection est rendue de plus en plus difficile à mesure de leurs dématérialisations. Le blanchiment de capitaux au moyen de crypto-actifs participe au mouvement d'adaptation d'une délinquance traditionnelle aux nouvelles technologies.

**28 – Recours limité aux plateformes d'échange** – A l'image des développements précédents, l'utilisation de crypto-actifs à des fins de blanchiment se matérialise par des opérations de conversion intra-cryptos et d'actifs numériques contre monnaie ayant cours légal (et inversement), dont le but est d'opacifier l'origine illicite des fonds et d'en empêcher toute traçabilité. Les plateformes de conversion étant assujetties aux obligations de lutte contre le blanchiment<sup>169</sup>, les délinquants se tournent vers d'autres portes d'entrées et de sortie entre le monde des crypto-actifs et le système financier traditionnel.

---

<sup>167</sup> DUTEIL Gilles, « Modes opératoires et évolutions », *AJ Pénal*, 2016, 171 p.

<sup>168</sup> BEAUSSONIE Guillaume (dir.), SEGONDS Marc (dir.), *Les modes opératoires de l'infraction*, Université Toulouse 1 Capitole, 28 juin 2019.

<sup>169</sup> Cf. *supra*. n°17.

Il convient toutefois de préciser qu'en l'absence de consensus international sur les obligations LCB à appliquer aux prestataires de services sur actifs numériques, les blanchisseurs ont parfois recours à des plateformes de conversion basées dans des territoires moins regardant, à la législation plus permissive. A titre illustratif, il est possible de citer le démantèlement de la plateforme costaricaine Liberty Reserve, accusée d'avoir blanchi plus de six milliards de dollars entre 2006 et 2013<sup>170</sup>. Plus d'un million d'utilisateurs situés dans dix-sept pays différents auraient fait appel aux services de la plateforme<sup>171</sup>.

**29 – Services de conversion entre particuliers** – A défaut des plateformes de conversion, les blanchisseurs ont recours à divers intermédiaires pour convertir le produit de leur infraction en monnaie fiat et inversement. Ils peuvent tout d'abord faire appel aux services proposés par des particuliers sur des sites internet tels que Localbitcoins.com. Ce « Leboncoin » finlandais de la crypto<sup>172</sup> propose à ses utilisateurs, enregistrés préalablement à l'aide d'une adresse email, d'acheter et de vendre des bitcoins entre particuliers. La transaction est réalisée selon le mode de paiement choisi par le client (espèces, virements, mandats cash). Un système de notation permet aux blanchisseurs de connaître la réputation de leur échangeur, pouvant potentiellement être poursuivi sur le terrain de la complicité.

Selon les conditions générales d'utilisation du site, la plateforme s'engage à respecter les obligations LCB/FT en procédant à une vérification plus ou moins approfondie de l'identité de ses clients au regard du volume annuel des échanges réalisés par ces derniers. Dans la limite d'un seuil de 1 000 € par an, il est possible d'utiliser les services proposés par la plateforme en se soumettant préalablement à un système de vérification par SMS. Des vérifications supplémentaires interviennent lorsque les transactions réalisées par l'utilisateur atteignent entre 1000 et 2000 € par an (envoi d'une pièce d'identité) et entre 2000 et 100 000 € par an (envoi d'une pièce d'identité et d'un justificatif de domicile). Enfin, seuls les comptes dépassant un volume d'échange de 100 000 € par an sont examinés manuellement et soumis à un « *questionnaire supplémentaire* ».

---

<sup>170</sup> Acte d'accusation déposée devant le tribunal de première instance de New-York, <https://krebsonsecurity.com/wp-content/uploads/2013/05/Liberty-Reserve-et-al.-Indictment.pdf>.

<sup>171</sup> CYPEL Sylvain, « L'affaire Liberty Reserve révèle les liens entre monnaies virtuelles et criminalité », Le Monde, 29 mai 2013, [https://www.lemonde.fr/economie/article/2013/05/29/l-affaire-liberty-reserve-revele-les-liens-entre-monnaies-virtuelles-et-criminalite\\_3420048\\_3234.html](https://www.lemonde.fr/economie/article/2013/05/29/l-affaire-liberty-reserve-revele-les-liens-entre-monnaies-virtuelles-et-criminalite_3420048_3234.html).

<sup>172</sup> DUBOIS Kévin, Analyste criminel à l'Office Central de Lutte contre la Cybercriminalité (OCLCTIC), Expert en crypto-actifs, entretien téléphonique mené par Alexandra Puertas, le 27 juin 2020



Le fait que ce type de plateformes ne soumet pas ses utilisateurs à des vérifications complémentaires tenant à leur permettre de s'assurer de la correspondance entre l'identité déclarée par le client au moyen de papiers d'identités et son identité réelle (par un procédé de vérification de correspondance des traits du visage par exemple) laisse craindre des risques d'utilisation de documents contrefaits ou volés<sup>173</sup>. Ces risques sont mis en avant par TRACFIN qui constate « *une augmentation sensible* » des déclarations de soupçons mentionnant des potentiels cas de fraude ou d'usurpation d'identité<sup>174</sup>. L'exposition significative des acteurs de l'écosystème crypto à ces procédés constitue une faille importante dans les procédures de connaissance client mis en œuvre par ces derniers<sup>175</sup>.

– **Utilisation de distributeurs automatiques** – En outre, des tendances récentes montrent une utilisation accrue de guichets automatiques, dits *coin ATM*, qui permettent de retirer des espèces à l'aide d'une clé cryptographique (vente de crypto-actifs) ou d'alimenter son portefeuille à partir d'un versement en espèces (achat de crypto-actifs). Le site CoinATMRadar.com dénombre, dans le monde, entier pas moins de 7 000 bornes d'échange

#### Répartition des *coins ATM* dans le monde



Source : « Bitcoin ATM MAP », sur CoinATMRadar [en ligne], <https://coinatmradar.com/>

<sup>173</sup> TRACFIN, *Tendances et analyse des risques de blanchiment de capitaux et de financement du terrorisme en 2016*, 13 avril 2018, p. 62.

<sup>174</sup> TRACFIN, *Tendances et analyse des risques de blanchiment de capitaux et de financement du terrorisme en 2018-2019*, 10 décembre 2019, p. 65-66.

<sup>175</sup> *Ibid.*

La France compte, quant à elle, sept distributeurs sur son territoire, dont un à Lille, un à Nice, un à Rouen et quatre à Paris. Le marché est disputé par deux opérateurs Shitcoins Club et General Bytes. Ces derniers imposent à leurs utilisateurs de scanner leurs cartes d'identité lorsqu'ils effectuent des opérations dépassant 999 € pour le premier (ATM permettant l'achat et la vente de crypto-actifs) , et 10 000 € pour le second (ATM permettant uniquement la vente de crypto-actifs)<sup>176</sup>. Toutefois, ces seuils varient d'un opérateur à l'autre et il s'avère tout à fait possible de convertir des crypto-actifs en cash (et inversement) sur des distributeurs basés dans des pays à la législation LCB plus permissive. Cependant, le montant important des frais de commissions associés aux opérations de change constitue un frein à l'utilisation plus large de ces distributeurs à des fins de blanchiment<sup>177</sup>.

**30 – Utilisation de cartes BTC2 Plastic** – Dans une optique similaire de conjugaison entre services de paiement en monnaie fiat et services en crypto-actifs, Tracfin soulignait dès 2016 les risques d'utilisations illicites de cartes de débit rechargés en crypto-actifs, dites BTC2 Plastic<sup>178</sup>. Apparues en 2013, les cartes BTC2 Plastic offrent à leurs détenteurs la possibilité d'effectuer des achats auprès de commerçants physiques, ou en ligne, et de retirer des espèces dans des distributeurs automatiques classiques. Cette dernière fonction, dite de *cash out*, est utilisée par les blanchisseurs qui souhaitent convertir le produit de leur infraction en espèces<sup>179</sup>. Le solde disponible sur ces cartes correspond à la contre-valeur en monnaie fiat du montant de crypto-actifs détenus par l'utilisateur.

L'atténuation des risques d'utilisation de ces cartes à des fins de blanchiment reposent sur l'efficacité des obligations de vigilances mises en œuvre par les sociétés émettrices. Toutefois, la délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces rapportent qu'en trois ans, le marché des cartes BTC2 Plastic s'est ouvert « à une vingtaine d'acteurs, sensibilisés de manière très disparate aux procédures de connaissance client »<sup>180</sup>.

---

<sup>176</sup> COIN ATM RADAR, « Bitcoin ATMs in France », sur *CoinATMRadar* [en ligne], <https://coinatmradar.com/country/73/bitcoin-atm-france/>.

<sup>177</sup> DUBOIS Kévin, Analyste criminel à l'Office Central de Lutte contre la Cybercriminalité (OCLCTIC), Expert en crypto-actifs, entretien téléphonique mené par Alexandra Puertas, le 27 juin 2020.

<sup>178</sup> TRACFIN, *Tendances et analyse des risques de blanchiment de capitaux et de financement du terrorisme en 2016*, 13 avril 2018, p. 58-59.

<sup>179</sup> *Ibid.*

<sup>180</sup> DELEGATION MINISTERIELLE AUX INDUSTRIES DE SECURITE ET A LA LUTTE CONTRE LES CYBERMENACES, *État de la menace liée au numérique en 2019*, mai 2019, p. 39-40.

En France, l'utilisation de ces cartes n'est pas soumise aux obligations de vigilance, prévues aux articles L. 561-4-1 et suivants du Code monétaire et financier, relatives à l'identification et à la vérification de l'identité du client avant l'entrée en relation d'affaires, ainsi qu'au recueil des informations liées à l'objet et à la nature de cette relation, lorsque la valeur minimale stockée sur le support n'excède pas 150 €. De plus, dans l'hypothèse où le support peut être rechargé, la carte est soumise à une limite maximale de stockage et de paiement de 150 € par période de trente jours et ne peut être utilisée que pour des paiements sur le territoire national<sup>181</sup>.

Bien que l'utilisation de ces cartes à des fins illicites, notamment par le contournement des seuils<sup>182</sup>, soit constatée ; leur assujettissement à la réglementation LCB à partir de montants relativement bas permet de réduire drastiquement ce risque. En ce sens, les montants des seuils sont fréquemment revus à la baisse, passant par exemple de 250 à 150 euros en février 2020<sup>183</sup>.

Cependant, l'absence de consensus international en matière LCB offre, une fois de plus, la possibilité pour les blanchisseurs de contourner la réglementation. Il convient enfin de souligner que l'utilisation de ces cartes a connu une forte baisse à la suite de la décision prise par VISA et Mastercard d'exclure de leur réseau le principal émetteur de ces cartes sur le marché européen, l'établissement de monnaie électronique Wavecrest Holdings Ltd basé à Gibraltar, pour manquement à ses obligations de vigilance. Toutes les cartes émises par cet établissement ont donc été désactivées début 2018<sup>184</sup>.

**31 – Conversion en cartes cadeaux** – Les blanchisseurs peuvent également avoir recours à des intermédiaires qui proposent de convertir leurs crypto-actifs en cartes cadeaux, à l'image de plateformes telles que LimonX ou Bitrefill<sup>185</sup>. Ces cartes cadeaux sont ensuite utilisées pour effectuer

---

<sup>181</sup> Article R. 561-16-1 du Code monétaire et financier.

<sup>182</sup> Le blanchiment d'une grosse somme d'argent passera par son fractionnement en de nombreuses petites transactions réglées avec diverses cartes, à l'image du *shtroumpfage* ou *smurfing* qui consiste à dissimuler le versement d'une importante somme d'argent liquide sur un compte bancaire en effectuant plusieurs petits versements pour éviter les déclarations de suspicion.

<sup>183</sup> Article 8 du décret n°2020-118 du 12 février 2020.

<sup>184</sup> TRACFIN, *Tendances et analyse des risques de blanchiment de capitaux et de financement du terrorisme en 2017-2018*, 28 novembre 2018, p. 59-60.

<sup>185</sup> PUTIGNY Hervé, Ancien cyber-enquêteur à la section de recherches de Dijon, Directeur général et co-fondateur de la société WebDrone, entretien téléphonique mené par Alexandra Puertas, le 11 juin 2020 ; DUBOIS Kévin, Analyste criminel à l'Office Central de Lutte contre la Cybercriminalité (OCLCTIC), Spécialiste en crypto-actifs, entretien téléphonique mené par Alexandra Puertas, le 27 juin 2020.

des achats de biens ou des services en ligne qui pourront éventuellement être revendus sur des sites de ventes d'occasions.

**32 – Investissement en jetons** – Enfin, Tracfin souligne, dans son rapport tendances et analyse 2017-2018, les risques de blanchiment de capitaux liés à l'investissement de fonds illicites en jetons émis dans le cadre d'ICO : « *lesquels seront revendus à d'autres investisseurs, puis convertis en monnaie légale. Le blanchisseur pourra alors justifier de ses fonds bancarisés en expliquant avoir financé un projet et avoir rentabilisé son investissement*<sup>186</sup> ».

Outre le recours à des modes opératoires de plus en plus complexes, les blanchisseurs utilisent divers procédés destinés à rendre leur appréhension impossible.

---

<sup>186</sup> TRACFIN, *Tendances et analyse des risques de blanchiment de capitaux et de financement du terrorisme en 2017-2018*, 28 novembre 2018, p. 60-61.

## 2. Les techniques d'opacification

**33 – Contexte** – La dématérialisation des modes opératoires conduit les services d'enquête à extraire et analyser une masse importante de données présentes sur différents supports dans le but de matérialiser l'infraction et rassembler les preuves numériques nécessaires à la poursuite des auteurs<sup>187</sup>.

En ce qui concerne le blanchiment commis au moyen de crypto-actifs, la mission des enquêteurs consiste à analyser l'ensemble des transactions suspectes passées sur la blockchain. Leur objectif est de retracer les flux illicites à la recherche d'un intermédiaire auquel ils pourront adresser des réquisitions afin que ce dernier leur communique les informations qu'il détienne sur le suspect en application de ses obligations de connaissance client. Afin d'empêcher les enquêteurs de remonter les transactions, les blanchisseurs ont recours à divers procédés destinés à casser la chaîne de transmission des crypto-actifs. L'utilisation de ces techniques impacte les enquêtes pénales, allant parfois jusqu'à conduire à leur abandon.

**34 – Les techniques d'anonymisation** – Tout d'abord, les blanchisseurs ont recours à diverses techniques destinées à masquer leur identité numérique.

– **Recours à des crypto-actifs dits anonymes** – Bien que le bitcoin reste le crypto-actif privilégié des criminels<sup>188</sup>, la blockchain bitcoin présente l'avantage (ou l'inconvénient) de permettre de remonter l'intégralité des transactions d'un utilisateur dès lors que sa clé publique est reliée à son identité. Les blanchisseurs ont donc tout intérêt à se tourner vers des blockchains spécialement conçues pour garantir l'anonymat de ses utilisateurs et rendre les transactions intraquables.

En ce sens, le 10 décembre 2019, Jarek Jakubcek, analyste près du Centre européenne de lutte contre la cybercriminalité, déclarait au cours d'un webinaire consacré aux crypto-actifs anonymes que, lors d'une enquête menée par ses services, l'utilisation combinée du crypto-actif Monero et du logiciel Tor<sup>189</sup> n'avait pas permis de retracer les fonds, ni de déceler une quelconque adresse IP<sup>190</sup>.

---

<sup>187</sup> PUTIGNY Hervé, Ancien cyber-enquêteur à la section de recherches de Dijon, Directeur général et co-fondateur de la société WebDrone, entretien téléphonique mené par Alexandra Puertas, le 11 juin 2020

<sup>188</sup> EUROPOL, *Internet organised crime threat assessment 2019*, 9 octobre 2019, 54 p.

<sup>189</sup> Cf. *Infra.* n°34 : utilisation du réseau Tor.

<sup>190</sup> L'adresse IP ou Internet Protocol Adresse, est l'adresse unique qui identifie tout matériel informatique connecté à internet.

Monero est un de ces crypto-actifs dits anonymes dont la blockchain rend les transactions intraquables par défaut (contrairement à Dash et Zcash). L'utilisation de trois technologies permet en effet de masquer l'expéditeur, le destinataire et le montant des transactions réalisées sur sa blockchain.

L'identité de l'expéditeur est dissimulée grâce à un procédé cryptographique appelé signature de cercle ou *ring signatures* qui a pour conséquence de faire apparaître toutes transactions émises sur la blockchain comme ayant été exécutées par un groupe de personnes, sans pouvoir déterminer l'identité du réel exécutant appartenant à ce groupe.

Ce procédé conduit à une anonymisation des transactions ; anonymisation renforcée par l'utilisation d'une technologie dites des adresses furtives ou *stealth addresses*, qui empêche d'associer les transactions effectuées par un utilisateur à sa clé publique en générant pour chaque transaction une nouvelle clé. Enfin, le montant des transactions effectuées sur la blockchain Monero<sup>191</sup> est cachée grâce à une technologie dites des transactions confidentielles en anneau<sup>192</sup> (Ring CT).

A titre comparatif, la blockchain du bitcoin est dite transparente en ce qu'elle affiche publiquement l'expéditeur, le destinataire et le montant de l'ensemble des transactions opérées en bitcoin.

---

<sup>191</sup> Pour en savoir plus sur les technologies de confidentialité utilisées par Monero : MONERO, « FAQ : How is Monero's privacy different from other coins », sur Monero [en ligne], <https://web.getmonero.org/get-started/faq/>

Pour en savoir plus sur les signatures de cercle : MONERO, « Monero : Ring Confidential Transactions » [vidéo en ligne], Youtube, 21 août 2017 2017, [consultée le 9 juin 2020], <https://www.youtube.com/watch?v=M3AHP9KgTkQ>.

Pour en savoir plus sur les adresses furtives : MONERO, « Monero : Stealth Addresses » [vidéo en ligne], Youtube, 4 avril 2017, [consultée le 9 juin 2020], <https://www.youtube.com/watch?v=bWst278J8NA>.

Pour en savoir plus sur les transactions confidentielles en anneau : MONERO, « Monero : Ring Signatures » [vidéo en ligne], Youtube, 12 juin 2017, [consultée le 9 juin 2020], [https://www.youtube.com/watch?v=zHN\\_B\\_H\\_fCs](https://www.youtube.com/watch?v=zHN_B_H_fCs)

<sup>192</sup> Les transactions confidentielles en anneau est un moyen de cacher le montant d'une transaction

Extrait des transactions effectuées sur la blockchain bitcoin par l'utilisateur détenant la clé publique :  
3FkenCiXpSLqD8L79intRNXUgjRoH9sjXa

Address ⓘ



Adresse	3FkenCiXpSLqD8L79intRNXUgjRoH9sjXa
Format	BASE58 (P2SH)
Transactions	1 345
Total reçu	362 467,56 \$US
Total envoyé	358 323,20 \$US
Solde final	4 144,36 \$US

Demande de paiement

Bouton de donateur

Clé publique appartenant au site internet bitcoin.org

Transactions ⓘ

Clé publique appartenant à Mr Dupont

Hachage	7302c7be9ac7cb7428e2e4e9227ae... bc1qjyOuk92a6e3j2ga... 13,77 \$US	2020-05-26 02:04	3FkenCiXpSLqD8L79in... 13,75 \$US
Frais	0,02 \$US (1.156 sat/B - 0.503 sat/WU - 192 bytes)		+13,75 \$US
Hachage	639093eb95b1a5d01d54910eb603b... bc1q87f8e7gvtzvnuzp9... 8,10 \$US	2020-05-26 12:49	3FkenCiXpSLqD8L79int... 7,69 \$US
Frais	0,41 \$US (21.911 sat/B - 9.540 sat/WU - 192 byte)		+7,69 \$US

Clé publique appartenant au site internet bitcoin.org

Source : Blockchain.com [en ligne], <https://www.blockchain.com/fr/explorer>.

**Explications** : la blockchain bitcoin est dite transparente puisque, à partir du moment où l'enquêteur a connaissance de l'identité de la personne qui se cache derrière une clé publique, il peut remonter l'ensemble des transactions effectués sur la blockchain par cette dernière.

Par exemple, si l'enquêteur sait que la clé publique « bc1qjyOuk92... » est détenue par Monsieur Dupont et que la clé publique « 3FkenCiXpSLqD8L79intRNXUgjRoH9sjXa » est détenue par le site internet bitcoin.org ; il pourra en déduire que Mr Dupont a envoyé, le 26 mai 2020 à 2h04, 13,75 dollars américains au site internet bitcoin.org.

Avec une capitalisation boursière estimée à près de 277 milliards de dollars américains<sup>193</sup>, Monero est le crypto-actif privé le plus populaire<sup>194</sup>. Toutefois, son utilisation nuit gravement aux enquêtes pénales, pouvant conduire à leur abandon<sup>195</sup>.

Au regard des risques blanchiment que font encourir ces crypto-actifs privés, des plateformes d'échange comme BitBay ont pris la décision d'exclure Monero de leurs plateformes<sup>196</sup>.

– **Utilisation du réseau Tor** – Tor est un logiciel, et un réseau informatique ouvert, qui permet de réduire une certaine forme de surveillance sur Internet. Cette surveillance, dite analyse du trafic réseau, permet de déterminer la source et la destination des informations auxquelles une personne accède<sup>197</sup>. Bien que son emploi soit licite, Tor est souvent utilisé par les blanchisseurs pour masquer leurs adresses IP dans le but d'empêcher leur identification par les services d'enquête.

Tor vient de l'acronyme The Onion Router, qui fonctionne sur la base du routage en oignon, développé au milieu des années 1990 par les informaticiens David Goldschlag et Georges Michael Reed et le mathématicien Paul Syverson du laboratoire de recherche des États-Unis. L'idée était de créer une connexion internet qui ne révèle pas l'adresse IP de l'utilisateur aux sites internet qu'il consulte<sup>198</sup>.

L'adresse IP ou Internet Protocol Adresse, est l'adresse unique qui identifie tout matériel informatique connecté à internet<sup>199</sup>. A partir de l'adresse IP d'un utilisateur, les autorités pourront identifier son fournisseur d'accès à internet, et potentiellement localiser le matériel informatique qu'il a utilisé.

---

<sup>193</sup> COINMARKETCAP, All cryptocurrencies, sur *coinmarketcap* [en ligne], consulté le 9 juin 2020.

<sup>194</sup> Ibid. Monero est classé 16<sup>ème</sup> rang en termes de capitalisation boursière des crypto-actifs.

<sup>195</sup> JAKUBCEK Jerek, *Blockchain Alliance webinar on Privacy Coins* [intervention], 10 décembre 2019.

<sup>196</sup> BitBay est la première plateforme européenne à interdire un crypto-actif en raison de l'anonymat qu'il procure. BITBAY, « *Ending Support for Monero (XMR)* », sur Bitbay [en ligne], le 19 février 2020, [consulté le 9 juin 2020], <https://bitbay.net/en/news/ending-support-for-moneroxmr-on-19022020>.

<sup>197</sup> *Tor Overview* [en ligne], [consulté le 6 juin 2020], <https://2019.www.torproject.org/about/overview.html.en>.

<sup>198</sup> *General FAQ* [en ligne], [consulté le 6 juin 2020], <https://2019.www.torproject.org/docs/faq.html.en>.

<sup>199</sup> « C'est quoi une adresse IP ? », sur Culture Informatique [en ligne], publié le 21 octobre 2012, [consulté le 6 juin 2020], <https://www.culture-informatique.net/c-est-quoi-une-adresse-ip-niv1/>.

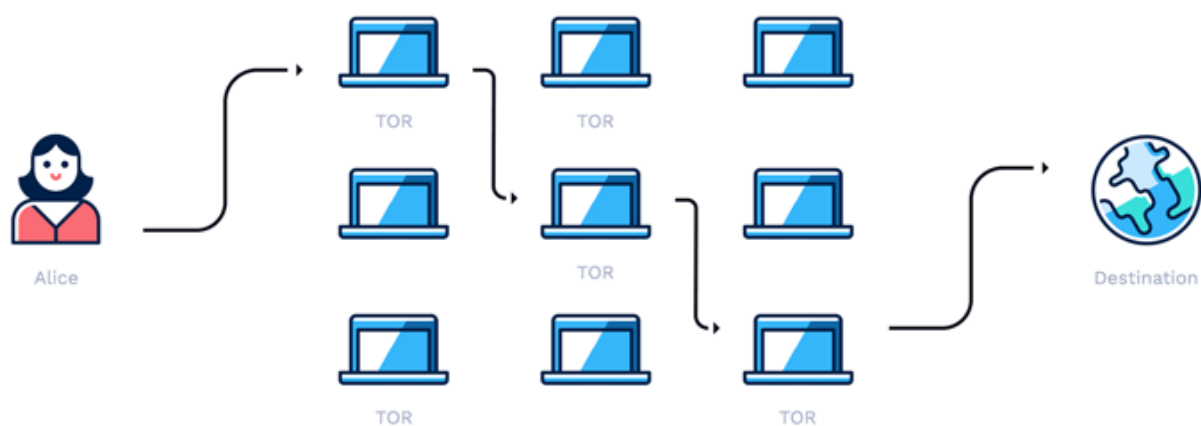


Lorsqu'un utilisateur effectue une demande d'informations sur internet, le routage en oignon va permettre d'acheminer cette demande au sein d'un réseau distribué de relais, appelés également nœuds. Ces nœuds ne sont rien d'autres que les ordinateurs de bénévoles composant le réseau Tor. L'idée est qu'au lieu d'établir une connexion directe entre la source et la destination, les données suivent un circuit aléatoire à travers plusieurs relais.

Chaque nœud du réseau aura connaissance de l'adresse IP de son prédécesseur et de son successeur mais ne pourra ni prendre connaissance de l'identité de la personne à l'origine de la demande d'informations, ni percevoir le contenu des données échangées qui sont cryptées lorsqu'elles passent par les nœuds.

Le réseau Tor permet donc de protéger l'identité de l'utilisateur puisqu'il sera impossible d'associer son ordinateur aux opérations de blanchiment réalisées sur internet.

#### Fonctionnement du réseau Tor

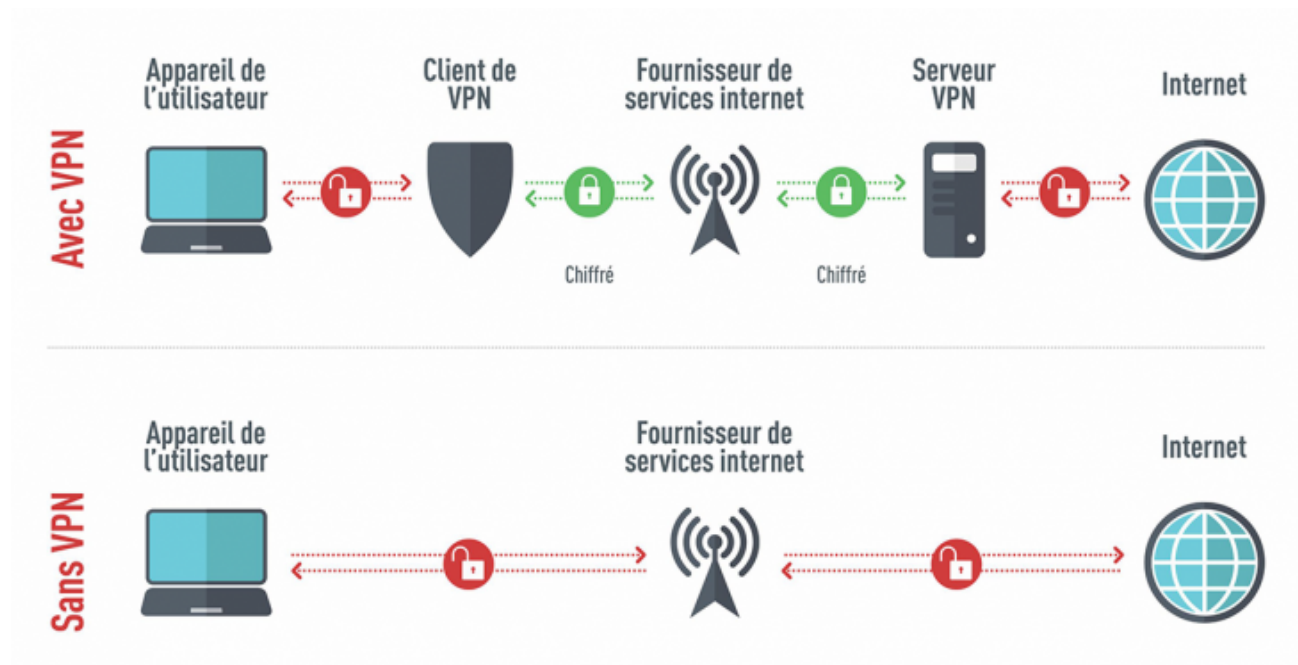


**Source :** « Bitcoin ATM MAP », sur CoinATMRadar [en ligne], <https://coinatmradar.com/>

– **Utilisation d'un VPN** – Outre l'utilisation de Tor, les blanchisseurs peuvent avoir recours à un VPN dans le but de masquer leur identité numérique. Un VPN (ou réseau privé virtuel) est un serveur qui sert d'intermédiaire entre l'utilisateur et internet. L'ordinateur est connecté au VPN, qui lui-même est connecté à internet. Ainsi, lorsque l'utilisateur souhaite consulter des informations en ligne, sa demande est traitée par le VPN qui effectuera les recherches sur internet et lui renverra les informations.

Le VPN permet donc de masquer l'adresse IP et la localisation du blanchisseur en « empruntant » l'adresse IP du serveur VPN qui peut être localisé à n'importe quel endroit sur le globe. Il devient alors impossible de connaître l'identité, la localisation et les opérations réalisées par l'utilisateur, seule sera visible sa connexion au VPN.

### Fonctionnement d'un VPN



**Source :** « VPN : Restez caché pour une meilleure vie privée », sur Emisoft Blog [en ligne], <https://blog.emisoft.com/fr/27548/vpn-reseau-prive-virtuel/>.

**35 – Les techniques destinées à opacifier la traçabilité des fonds** – Enfin, les blanchisseurs ont recours à des techniques destinées casser la chaîne de transmission des crypto-actifs afin d’empêcher les services d’enquête de remonter les transactions<sup>200</sup>.

– **Mixer** – Pour cela, la technique la plus utilisée par les blanchisseurs consistent à faire appel aux services de mixers ou tumblers. Ces derniers servent d’intermédiaire entre un portefeuille A et un portefeuille B afin d’empêcher l’établissement d’un quelconque lien entre ces derniers. Les services de mixage présentent l’intérêt de pouvoir faire transiter des fonds d’un portefeuille A à un portefeuille B, et ce, sans que les services d’enquête soit dans la capacité d’identifier le portefeuille B. Pour se faire, le mixer va demander au client A de lui envoyer les unités qu’il souhaite faire parvenir à B sur une clé publique lui appartenant (et sur laquelle tous les clients du mixer envoient des fonds). Le client pourra alors choisir différentes options assorties de coûts plus en moins élevés en fonction des techniques d’opacification qu’il souhaite utiliser. Ainsi, les crypto-actifs d’origine illicite de A seront mélangés aux unités propres appartenant à d’autres clients du mixer ou au mixer lui-même.

Représentation d’un mixer de bitcoins



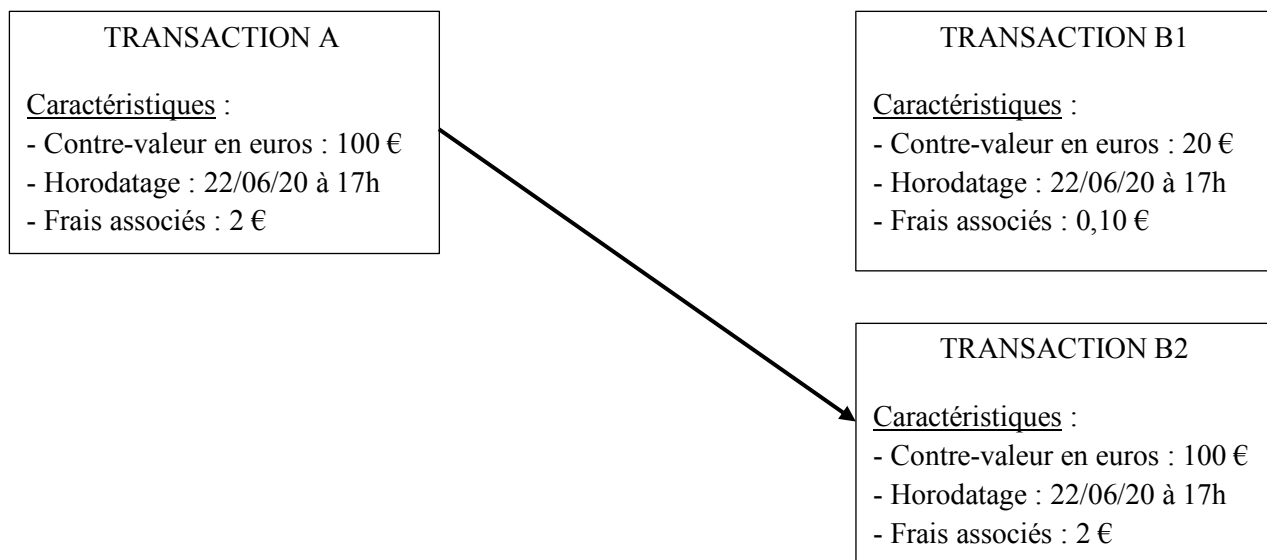
**Source** : « Rester anonyme avec les cryptomonnaies : Qu’est-ce qu’un mixeur de Bitcoin ? », sur CryptoActu [en ligne], <https://cryptoactu.com/bitcoinmix-anonyme/>.

Pour comprendre en quoi les services de mixage empêchent les enquêteurs de tracer les crypto-actifs, il convient de s’intéresser au fonctionnement des outils d’analyses utilisés par ces derniers, à savoir les explorateurs de blockchain.

<sup>200</sup> EUROPOL, *Internet organised crime threat assessment 2019*, 9 octobre 2019, 54 p.

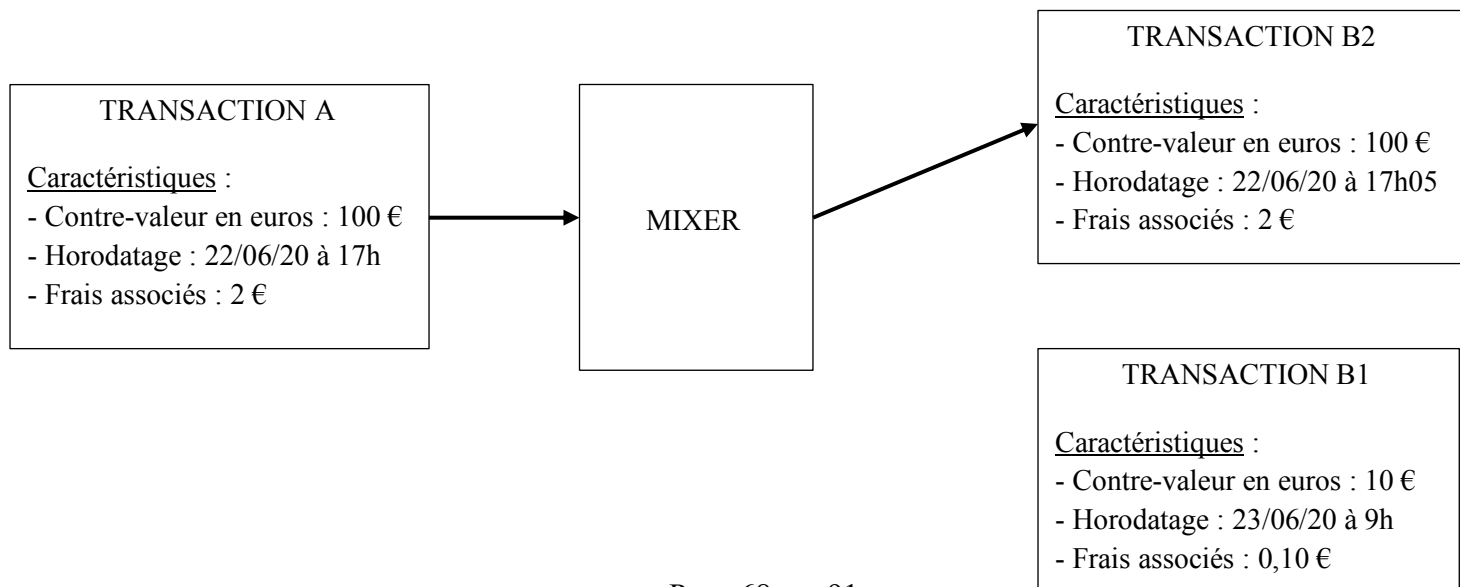
En effet, les algorithmes de ces outils d'analyse sont programmés pour suivre les transactions réalisées en crypto-actifs sur la blockchain en fonction de leurs caractéristiques (montant de la transaction, date, heure, frais liés à la transaction etc.)

### Représentation de la logique suivie par un explorateur de blockchain



A partir de la transaction A, l'analyseur de blockchain va suivre la transaction B2 puisque ses caractéristiques correspondent à la transaction initiale. Toutefois, cette logique ne fonctionne plus lorsque le blanchisseur utilise un service de mixage puisque le mixer se chargera de diviser la transaction A en une multitude de transactions (par exemple 10 transactions de 10 €), qu'il renverra à B à des intervalles de temps déterminés.

### Chemin suivi par l'outil d'analyse en présence d'un mixer



Par conséquent, le recours aux services de mixage empêche les enquêteurs de s'assurer que la transaction qu'ils suivent correspond, en réalité, à celle effectuée par le blanchisseur<sup>201</sup>. La seule solution pour les services d'enquête consiste alors à localiser le mixer, puis prouver que le flux principal généré sur sa plateforme est d'origine illicite. Ainsi, il sera possible de faire fermer la plateforme et de saisir ses serveurs afin d'analyser les patterns, c'est-à-dire les habitudes de l'algorithme du mixer, pour espérer pouvoir reconstruire le chemin réel des fonds et identifier les blanchisseurs.

En mai 2019, le service néerlandais de renseignements et d'enquêtes fiscales, en étroite coopération avec Europol et les autorités luxembourgeoises, a procédé à la fermeture d'un des plus importants services de mixage de crypto-monnaies au monde, Bestmixer.io. Ouvert en mai 2018, le service aurait permis le blanchiment de fonds illicites pour un montant estimé à 200 millions de dollars américains. L'opération a notamment permis de saisir six serveurs aux Pays-Bas et au Luxembourg<sup>202</sup>.

– **Plateforme de conversion intra-crypto** – Dans un même ordre d'idée, des plateformes de conversion intra-crypto telles que Changelly ou ShapeShift proposent à leurs clients de servir d'intermédiaire à l'image des mixers mais en incorporant, en plus, une opération de conversion intra-cryptos. Le recours à ces plateformes complexifie d'autant plus la traçabilité des fonds au regard d'opérations réalisés sur des blockchains différentes (donc indépendantes l'une de l'autre)<sup>203</sup>.

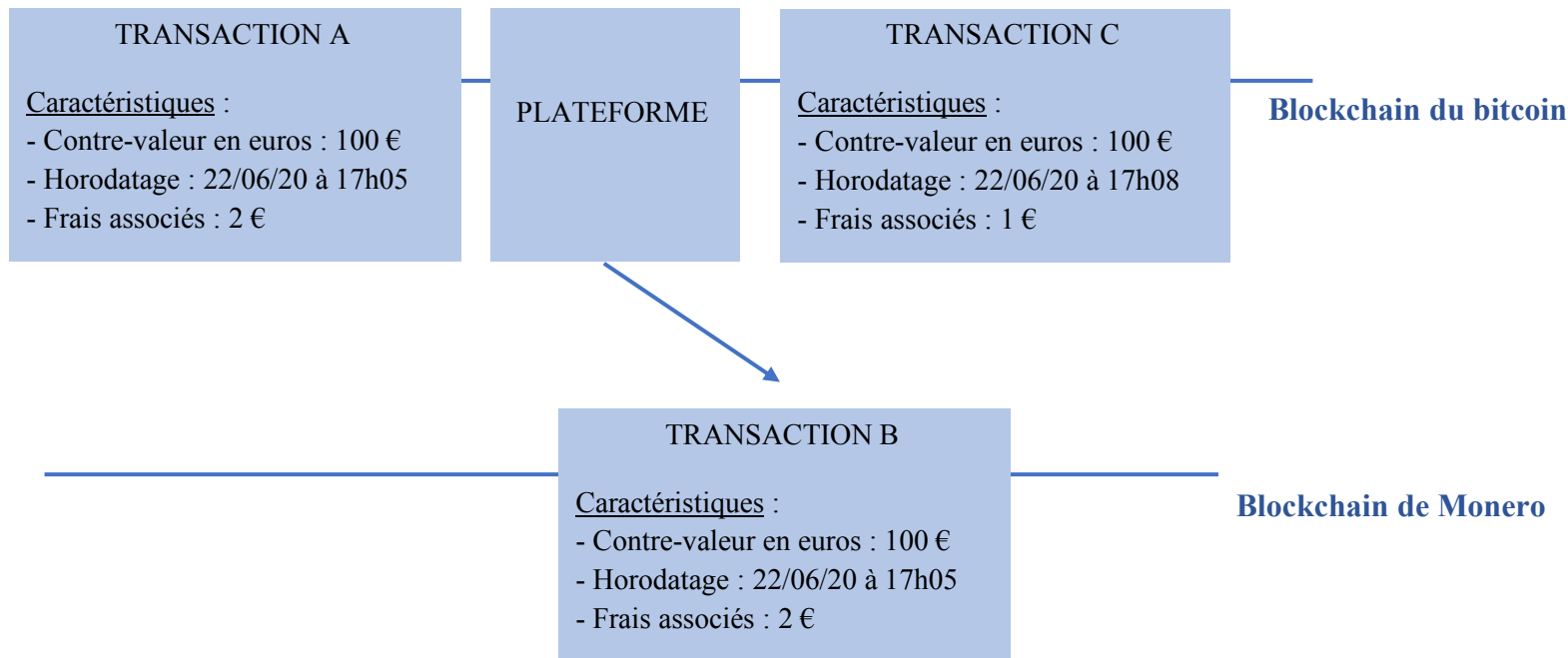
---

<sup>201</sup> DUBOIS Kévin, Analyste criminel à l'Office Central de Lutte contre la Cybercriminalité (OCLCTIC), Expert en crypto-actifs, entretien téléphonique mené par Alexandra Puertas, le 27 juin 2020

<sup>202</sup> EUROPOL, *Internet organised crime threat assessment 2019*, 9 octobre 2019, 54 p.

<sup>203</sup> DUBOIS Kévin, *Ibid.*

Représentation des opérations réalisées par des plateformes telles que Changelly ou Shapeshift



**Explications** : A souhaite envoyer 100 euros à B. Il envoie pour 100 € de bitcoins à la plateforme. Cette dernière se charge alors d'envoyer pour 100 euros d'un autre crypto-actif (ici Monero) à B. L'outil d'analyse utilisé par l'enquêteur suivra potentiellement la transaction C qui dispose des mêmes caractéristiques que la transaction A.

Pour conclure, l'utilisation de techniques d'opacification par les blanchisseurs entravent la capacité des autorités compétentes à collecter les preuves nécessaires à leurs identifications, poursuites et condamnations. Ce constat doit conduire les pouvoirs publics à renforcer les capacités d'investigation des enquêteurs.

Ces dernières années, les autorités de police judiciaire se sont dotées de services d'enquête spécialisée ayant une compétence nationale, à l'image de la cellule d'enquête spécialisée en cybercriminalité financière de Tracfin, l'Office Central de la Lutte contre la Cybercriminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC) relevant de la Direction Centrale de la Police Judiciaire, le Centre de Lutte contre les Criminalités Numériques relevant de la Gendarmerie Nationale ou encore la cyberdouane.

Pour mener à bien leurs missions, ces enquêteurs spécialisés sont dotés de puissants outils de *crypto-tracking*, dénommés explorateurs de blockchain. Ces nouveaux outils offrent, en plus des fonctionnalités d'exploration, des programmes d'analyse et d'investigation spécialement destinés à l'identification de suspects, la traçabilité des transactions, l'estimation des flux financiers et l'identification d'activités suspectes<sup>204</sup>. Cependant, les solutions d'analyse les plus performantes nécessitent l'achat de licences annuelles qui engendrent des coûts financiers importants (30 000 € / an pour le logiciel utilisé par OCLCTIC). Pour ces raisons, les pouvoirs publics réservent ces outils aux services centraux. Toutefois, cette logique de centralisation conduit à un manque de sensibilisation des équipes au niveau local, parfois aggravé par une stratégie négative de réductions des effectifs.

---

<sup>204</sup> DIRECTION DES AFFAIRES CRIMINELLES ET DES GRACES, *Fiche juridique et technique - Cryptoactifs*, janvier 2019, 5 p.

### III. La répression du blanchiment de capitaux au moyen de crypto-actifs

La répression du blanchiment de capitaux au moyen de crypto-actifs passe par le respect d'un ensemble de règles procédurales (A), et doit conduire à priver le délinquant du produit de son infraction (B).

#### A. Le régime juridique

Il convient d'étudier le régime des poursuites (1), avant de s'intéresser aux peines encourues par les auteurs.

##### 1. Les poursuites

**36 – Tentative de blanchiment** – La tentative de l'infraction générale de blanchiment est punie des mêmes peines que l'infraction consommée (C. pén., art. 222-40 ; C. pén. art. 324-6). Il en va de même de la tentative de blanchiment du trafic de stupéfiants et de la tentative de blanchiment douanier (C. douanes, art. 415).

**37 – Complicité** – Le droit commun de la complicité s'applique à l'infraction de blanchiment, son champ d'application est cependant restreint compte tenu de la définition large du blanchiment (C. pén., art. 121-6 et 121-7).

**38 – Auto-blanchiment** – Contrairement au recel, la chambre criminelle de la Cour de cassation a expressément admis la possibilité de cumuler la qualité d'auteur de l'infraction principale et de blanchisseur du produit direct ou indirect tirée de celle-ci<sup>205</sup> pourvu que « *les faits ne procèdent pas de manière indissociable d'une action unique caractérisée par une seule intention coupable*<sup>206</sup> ». Cette possibilité est cependant exclue s'agissant du blanchiment par facilitation de la justification de l'origine des fonds.

**39 – Prescription** – L'action publique de l'infraction générale de blanchiment se prescrit dans un délai de six ans à compter du jour où l'infraction a été commise (C. pr. pén. art. 7). Le blanchiment est une

---

<sup>205</sup> Cass. crim., 14 janvier 2004, n°03-81.165.

<sup>206</sup> Cass. crim., 7 décembre 2016, n°15-87.335.



infraction instantanée (Cass. crim. 11 sept. 2019, n°18-81.040) dont le point de départ de la prescription commence à courir au jour de la commission.

Toutefois, la chambre criminelle de la Cour de cassation a récemment précisé que : « *lorsqu'il consiste à faciliter la justification mensongère de l'origine de biens ou de revenus ou à apporter un concours à une opération de dissimulation du produit direct ou indirect d'un crime ou d'un délit, le blanchiment, qui a pour objet de masquer le bénéficiaire ou le caractère illicite des fonds ou des biens sur lesquels il porte, notamment aux yeux de la victime et de l'autorité judiciaire, constitue en raison de ses éléments constitutifs une infraction occulte par nature*<sup>207</sup> ». Dans ce cas, le point de départ du délai de prescription est fixé au jour où l'infraction a pu être constatée dans les conditions permettant l'exercice de l'action publique (C. pr. pén. art. 9-1). Le report du point de départ de la prescription s'applique également en présence d'une opération de placement ou de conversion du produit direct ou indirect d'un crime ou d'un délit lorsqu'elle est accompagnée de manœuvres caractérisées de dissimulation.

En tout état de cause, lorsque le point de départ du délai de prescription de l'action publique est retardé en application de l'article 9-1 du Code de procédure pénale, sa durée ne peut excéder douze années révolues à compter du jour où l'infraction a été commise.

**40 – Procédures spéciales** – En outre, les procédures pénales dérogatoires applicables à la criminalité organisée (C. pr. pén. art. 706-73, 14° et 706-73-1, 3 bis°) et au terrorisme (C. pr. pén. art. 706-16 à 706-25-2) peuvent s'appliquer au blanchiment.

**41 – Compétence internationale** – Enfin, le blanchiment en France d'une infraction principale commise à l'étranger relève de la compétences des juridictions françaises en application du principe de territorialité prévu à l'article 113-2 du Code pénal et du caractère autonome de l'infraction (Cass. crim., 24 février 2010, n°09-82.857 ; 17 novembre 2010, n°09-88.751).

Également, le blanchiment à l'étranger d'une infraction principale commise en France relève de la compétence des juridictions françaises (Cass. crim., 9 déc. 2015, n°15-83.204).

---

<sup>207</sup> Cass. crim. 11 sept. 2019, n°18-83.484

## **2. Les peines**

**42 – Pénalités applicables au blanchiment simple** – L’infraction générale de blanchiment est punie de cinq ans d’emprisonnement et 375 000 € d’amende (C. pén. art. 324-1, al. 3).

Lorsque l’infraction source est punie d’une peine d’emprisonnement supérieure à cinq ans, le blanchiment est puni des peines attachées à l’infraction dont son auteur a eu connaissance (C. pén. art. 324-2).

Il convient de préciser que la peine privative de liberté est réduite de moitié si, ayant averti l’autorité administrative ou judiciaire, l’auteur ou le complice a permis de faire cesser l’infraction ou d’identifier, le cas échéant, les autres auteurs ou complices (C. pén. art. 324-6-1).

En ce qui concerne la peine d’amende, elle peut être élevée jusqu’à la moitié de la valeur des biens ou des fonds sur lesquels ont porté les opérations de blanchiment (C. pén. art. 324-3). Lorsque l’infraction a été commise par une personne morale, l’amende encourue est égale au quintuple de celle prévue pour les personnes physiques, soit 1 875 000 €.

**43 – Pénalités applicables au blanchiment aggravé** – L’article 324-2 du Code pénal prévoit trois causes d’aggravation de l’infraction tenant à l’habitude, aux facilités procurées par l’exercice d’une activité professionnelle et la bande organisée. Dans ce cas, l’infraction est punie de 10 ans d’emprisonnement et 750 000 € d’amende.

Toutefois, lorsque l’infraction source est punie d’une peine d’emprisonnement supérieure à sept ans, le blanchiment est puni des peines attachées à l’infraction dont son auteur a eu connaissance et, si cette infraction est accompagnée de circonstances aggravantes, des peines attachées aux seules circonstances dont il a eu connaissance (C. pén. art. 324-2).

Enfin, l’auteur d’un blanchiment simple ou aggravé encoure les différentes peines complémentaires prévues à l’article 324-7. Parmi celles-ci, l’exécution de la peine complémentaire de confiscation peut poser des difficultés aux autorités compétentes en raison des caractéristiques spécifiques des crypto-actifs.

## **B. Les saisies pénales et la peine de confiscation**

**44. – Distinction** – La procédure pénale française distingue deux types de saisies pénales qui ont pour point commun de rendre le bien sur lesquelles elles portent indisponibles (C. pr. pén., art. 706-145). La première dite saisie investigation a pour but de contribuer à la manifestation de la vérité tout en participant à la preuve pénale. Elle peut porter sur tous les objets, papiers, documents ou données informatiques qui ont servi à l'infraction ou qui en constituent le produit (C. pr. pén., art. 54, 56, 76 et 97).

La seconde dite saisie confiscation a pour objet de garantir l'exécution d'une peine de confiscation en anticipant sur la condamnation à venir. Ici, l'idée est de priver le délinquant de toute forme d'enrichissement issue de l'infraction afin de garantir que le crime ne paie pas. Instituée par la loi n°2010-768 du 9 juillet 2010 visant à faciliter la saisie et la confiscation en matière pénale, la saisie confiscation est régie par les articles 706-141 et suivants du Code de procédure pénale.

La saisie-confiscation est donc le pendant procédural de la peine complémentaire de confiscation prévue à l'article 131-21 du Code pénal dont elle a vocation à garantir la pleine efficacité. S'agissant des infractions de blanchiment, cette peine porte tant sur l'instrument et le produit de l'infraction<sup>208</sup>, que sur les biens appartenant au condamné ou dont il a la libre disposition lorsque ni ce dernier, ni le propriétaire, n'est en mesure d'en justifier l'origine (C. pén. art. 131-21, al. 5), voir sur l'entier patrimoine du condamné<sup>209</sup>.

**45. – Saisie de crypto-actifs** – A ce stade, il convient de garder en mémoire que la possession de crypto-actifs n'est rien d'autre que la possession d'une paire de clés publique et privée qui permet d'utiliser les crypto-actifs qui lui sont associés. Le type de saisie à opérer diffèrera donc en fonction de la manière dont la clé privée est stockée. Cette clé, assimilable à un code PIN de carte bancaire, est stockée au sein d'un *wallet* ou portefeuille dont les caractéristiques diffèrent selon le type choisi.

Le propriétaire d'une paire de clés dispose de la liberté de choix entre quatre type de wallet : les *software wallets*, les *hardware wallets*, les *brain wallets* ou les *wallets online*.

---

<sup>208</sup> C. pén. art. 324-7, 8° pour le blanchiment général ; C. pén. art. 222-44 pour le blanchiment lié à un trafic de stupéfiants ; C. douane. art. 415 pour le blanchiment douanier.

<sup>209</sup> C. pén. art. 324-7, 12° pour le blanchiment général ; C. pén. art. 222-49 pour le blanchiment lié à un trafic de stupéfiants ; C. pén. art. 422-6 pour le blanchiment en lien avec un acte de terrorisme.

– **Software wallet** – Les software wallet sont des logiciels spécialement conçus pour le stockage de clés privées hors-ligne, dit cold storage<sup>210</sup>. Il en existe deux types : les *desktop wallets* qui sont des logiciels de stockage destinés à être utilisés sur ordinateur et les *mobile wallets* qui fonctionnent sur portable et tablette.

Les *software wallet* présentent l'avantage d'enregistrer la clé privée sur un support non connecté à internet, et de réduire ainsi les risques de subtilisation. Toutefois, ils restent sensibles aux logiciels malveillants et virus de type *spyware* (logiciel espion).

– **Hardware wallet** – Les *hardware wallets* sont des supports de stockage amovibles conçus pour stocker des clés privées hors ligne. Ils se présentent sous la forme de clés USB et sont l'un des moyens de stockage les plus sécurisés. C'est cet avantage qui a permis à Ledger, start-up française lancée en 2011, de devenir la société pionnière en la matière. Le 27 septembre 2019, son *hardware wallet*, Ledger Nano S, a reçu la Certification de Sécurité de Premier Niveau (CSPN) délivrée par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), faisant de lui le premier et le seul portefeuille certifié sur le marché<sup>211</sup>. La Certification de Sécurité de Premier Niveau (CSPN) est une des certifications délivrées par l'Agence Nationale de la Sécurité des Systèmes d'Information qui atteste qu'un produit numérique offre un niveau de sécurité éprouvé et résiste aux attaques de niveau modéré. Elle est un gage de sécurité pour les utilisateurs et un avantage concurrentiel pour les fournisseurs<sup>212</sup>. Le 27 septembre 2019, la société a de nouveau reçu une CSPN pour la nouvelle version de son *hardware wallet*, Ledger Nano X<sup>213</sup>. Dans les deux cas, la certification couvre quatre fonctions de sécurité intégrée aux appareils :

- Le générateur de nombres aléatoires réels (ou *true random number generator*) qui permet de générer aléatoirement une *seed* unique à partir de laquelle seront créées des paires de clés publiques et privées. La *seed* ou graine est une phrase de récupération de vingt-quatre mots qui

---

<sup>210</sup> Le cold storage désigne une technique de stockage de clés sur un support non connecté à un réseau.

<sup>211</sup> LEDGER, « Setting a New Standard: Ledger Nano S becomes the First and Only Certified Hardware Wallet on the Market », sur *Ledger* [en ligne], 18 mars 2019, [consulté le 14 juin 2020], <https://www.ledger.com/setting-a-new-standard-ledger-nano-s-becomes-the-first-and-only-certified-hardware-wallet-on-the-market/>.

<sup>212</sup> ANSSI, « La certification de sécurité de produits », sur ANSSI [en ligne], [consulté le 14 juin 2020], [https://www.ssi.gouv.fr/uploads/2018/01/certification\\_securite\\_produits\\_visa\\_securite\\_anssi.pdf](https://www.ssi.gouv.fr/uploads/2018/01/certification_securite_produits_visa_securite_anssi.pdf).

<sup>213</sup> LEDGER, « Ledger continues its security certification program with Ledger Nano X », sur *Ledger* [en ligne], 22 octobre 2019, [consulté le 14 juin 2020], <https://www.ledger.com/ledger-nano-x-recognized-as-certified-crypto-hardware-wallet>.

permet de restaurer ses données à partir d'un autre Ledger. L'infaillibilité du générateur de nombres aléatoires réels est donc essentielle puisqu'il garantit l'unicité de la seed créée ;

- La racine de confiance (ou *root of trust*) qui atteste de l'authenticité du produit et protège l'utilisateur contre les contrefaçons ;
- La vérification de l'utilisateur final (ou *end-user verification*) qui sécurise l'appareil en requérant à son démarrage un code PIN choisi par l'utilisateur ;
- La capacité post-émission sur un canal sécurisé (ou *post-issuance capability over a secure channel*) qui permet d'ajouter de nouvelles fonctionnalités à l'appareil, après sa fabrication, pour augmenter son niveau de sécurité ou le rendre compatible avec de nouveaux crypto-actifs.

Outre un atout sécuritaire, les *hardware wallets* présentent une certaine praticité en ce qu'ils permettent de gérer différents crypto-actifs à partir d'un même appareil. En effet, chaque crypto-actif nécessite une paire de clé différente compatible avec sa blockchain. Le ledger offre donc la possibilité d'utiliser ses diverses clés au moyen d'une *seed* unique qui lui sont associées. Toutefois, les *hardware wallets* présentent des risques en matière de destruction, vol, perte ou panne.

– **Brain wallet ou paper wallet** – Les *brain wallets* (littéralement portefeuille de cerveau) ou *paper wallets* (portefeuille en papier) sont, comme leur nom l'indique, le stockage de clés privées sur une feuille de papier ou tout simplement gardé en mémoire dans sa tête. Les clés privées sont alors générées sur des sites internet<sup>214</sup> ou par des logiciels, non connectés à internet, pour plus de sécurité. Les *brain wallets* présentent un avantage indéniable en matière sécuritaire mais sont sensibles à la destruction, le vol, la perte ou l'oubli.

– **Wallet online** – Enfin, les *wallet online* (ou portefeuilles en ligne) sont des portefeuilles stockés sur internet, généralement intégrés dans les services proposés par les plateformes d'échange. Ils présentent l'avantage de la simplicité et de la rapidité mais restent sensibles aux cyber-attaques.

---

<sup>214</sup> Des sites internet comme <https://www.bitaddress.org/> proposent des générateurs d'adresses bitcoin hors-ligne (les clés sur la blockchain Bitcoin sont appelés des adresses).

**46. – Défis liés à la saisie pénale de crypto-actifs** – La saisie pénale de crypto-actifs présente un double défi. Le premier réside dans la nécessité de former les services d'enquête au domaine. En effet, la répression du blanchiment par l'usage de crypto-actifs exige que les enquêteurs soient à même d'identifier, lors d'une perquisition, les indices d'un tel usage (identification d'un *hardware wallet* par exemple). Les faits de blanchiment étant généralement découverts à titre incident<sup>215</sup>, il s'avère donc indispensable que tous les services d'enquête soient sensibilisés au sujet<sup>216</sup>.

Le second défi relève de la saisie en elle-même, dont la procédure et les possibilités dépendront respectivement de la nature juridique des crypto-actifs et de la manière dont la clé privée est stockée.

**47. – Détermination de la saisie applicable** – Le Code de procédure pénale français ne comprend pas de dispositions pénales spécifiques relatives à la saisie des crypto-actifs, contrairement à la Hongrie ou encore à la Slovaquie<sup>217</sup>.

Pour déterminer le régime applicable à la saisie des crypto-actifs, il appartient aux autorités compétentes de déterminer leur nature juridique. Sur ce point, l'autonomie du droit pénal permet aux magistrats de ne pas être liés par les qualifications opportunes pouvant être retenues sur le terrain de leur réglementation<sup>218</sup>. Ainsi, il apparaît que les crypto-actifs ne sont, ni des créances au sens de l'article 706-155 du Code de procédure pénale, faute d'émetteur ; ni des instruments financiers au sens de l'article 706-156 du Code de procédure pénale (bien que s'agissant des *security tokens*, l'AMF privilégie cette qualification<sup>219</sup>). Relevant de l'incorporel, les crypto-actifs n'existent « *qu'en considération de leur valeur économique*<sup>220</sup> ». Ils sont par conséquent pénalement considérés comme

---

<sup>215</sup> HOUEL Jean-Luc, Ancien enquêteur financier à la section de recherches de Dijon, Ancien chef de la cellule régionale des avoirs criminels, entretien téléphonique mené par Alexandra Puertas, le 11 juin 2020 ; PEZENNEC Thierry, Commandant de Police, Chef du SIRASCO-financier, entretien téléphonique mené par Alexandra Puertas, le 8 juin 2020.

<sup>216</sup> PIERSON Frédérique, Capitaine de Police, Responsable du Bureau des avoirs criminels d'Europol, entretien téléphonique mené par Alexandra Puertas, le 10 juin 2020.

<sup>217</sup> EUROJUST, *Cybercrime Judicial Monitor*, décembre 2019, 32 p.

<sup>218</sup> Cf. *supra*. n°15.

<sup>219</sup> Cf. *supra*, n°15 : nature juridique des *security tokens*.

<sup>220</sup> LAMBERTYE-AUTRAND Marie-Christine, *Art. 516 - Fascicule unique : BIENS - Distinctions*, JurisClasseur Civil Code, Lexis Nexis, 12 mai 2011, mis à jour le 31 juillet 2017.

des biens meubles incorporels dont la saisie est régie par les articles 706-153 à 706-157 du Code de procédure pénale<sup>221</sup>.

D'un point de vue procédurale, leur saisie se matérialise par une ordonnance du juge des libertés et de la détention (en enquête) ou du juge d'instruction (en instruction) (C. pr. pén. art. 706-153). Cette ordonnance doit être motivée, ce qui signifie qu'elle doit exposer en quoi les crypto-actifs constituent l'instrument ou le produit du blanchiment (C. pén. art. 324-7, 8°), ou alors dans quelle mesure elle renvoie à la confiscation générale (C. pén. art. 324-7, 12°). Faute d'intermédiaire bancaire, l'officier de police judiciaire ne peut pas procéder d'initiative à la saisie de crypto-actifs qui n'entre pas dans le cadre des dispositions de l'article 706-154 du Code de procédure pénale.

**48. – Difficultés pratiques liées à la mise en œuvre de la saisie** – A l'image des développements précédents, il est nécessaire de bien comprendre que la possession de crypto-actifs n'est rien d'autre que la possession d'une paire de clés qui permet de les utiliser. Par conséquent, pour saisir des crypto-actifs, il convient de trouver cette clé privée afin d'accéder aux actifs illicites, puis les transférer sur un portefeuille étatique ce qui permettra de les rendre indisponibles.

En France, ce portefeuille est géré par l'Agence de Gestion et de Recouvrement des Avoirs Saisies et Confisqués (AGRASC). Au cours de ces six dernières années, l'AGRASC a été contactée à vingt-sept reprises pour procéder à la saisie de crypto-actifs, toutefois, seules huit saisies ont été effectuées<sup>222</sup>. C'est dans le cadre de la fermeture, en juillet 2014, d'une plateforme d'échange exerçant sans agrément que la première saisie de crypto-actifs a eu lieu en France. Elle avait conduit les gendarmes de la section de recherches de Toulouse à saisir 388 bitcoins pour une valeur totale avoisinant à l'époque 200 000 euros<sup>223</sup>.

---

<sup>221</sup> AGRASC, *Rapport annuel 2017*, 3 juin 2016, 40 p.

<sup>222</sup> Non-divulgarion de la source.

<sup>223</sup> CEILLES Mathilde et AFP AGENCE, « France : un trafic de bitcoins démantelé », *Le Figaro*, 7 juillet 2014, <https://www.lefigaro.fr/actualite-france/2014/07/07/01016-20140707ARTFIG00189-france-un-traffic-de-bitcoins-demantele.php>.

La première étape de la saisie consistera donc à identifier la manière dont la clé privée est stockée<sup>224</sup>. Une fois cette phase d'identification réalisée, les autorités compétentes cherchent à accéder au support de stockage de cette clé privée.

Si la clé est stockée sur un *software wallet* (logiciel) ou sur un *hardware wallet* (support de stockage amovible), les obstacles résideront dans l'accès au support protégé respectivement par des mots de passe et un code PIN. L'accès au support sera d'autant plus difficile puisque, tel que développé plus haut, les *hardware wallets* comme Ledger sont spécialement conçus pour offrir un niveau de sécurité éprouvé et résister aux attaques de niveau modéré. De plus, les fonctions de sécurité qu'il intègre obligent les enquêteurs à accéder rapidement au support saisi, aux risques que les crypto-actifs soient entre temps transférés sur un autre *wallet*. En effet, un complice de l'auteur pourrait parfaitement, à partir d'un autre appareil, régénérer les informations contenus dans le *ledger* saisi en utilisant la seed de ce dernier<sup>225</sup>.

En pratique, il apparaît que les services d'enquête ont bien du mal à casser le code PIN qui protège l'accès aux données contenues dans un Ledger<sup>226</sup>. La question se pose donc de savoir si l'auteur qui refuse de divulguer aux enquêteurs sa clé privée encourt l'infraction prévue à l'article 434-15-2 du Code pénal. Cette dernière réprime de trois ans d'emprisonnement et 270 000 euros d'amende<sup>227</sup> le fait de refuser de remettre aux autorités judiciaires la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisée pour préparer, faciliter ou commettre un crime ou un délit. Ces peines relativement lourdes pourraient inciter le délinquant à coopérer avec les enquêteurs.

A titre informatif, le Conseil constitutionnel a considéré, dans une décision en date du 30 mars 2008<sup>228</sup>, que l'infraction prévue à l'article 434-15-2 du Code pénal ne porte pas atteinte au droit de se taire et de ne pas s'auto-incriminer, et doit donc, à ce titre, être déclaré conforme à la Constitution. Cette

---

<sup>224</sup> LE GUEN Olivier, « Questions à Olivier Le Guen sur la perquisition et la saisie des crypto-actifs », *Dalloz IP/IT*, octobre 2019, 541 p.

<sup>225</sup> Cf, *supra*, n°45, Hardware wallet.

<sup>226</sup> PUTIGNY Hervé, *op. cit.* ; DEBOIS Kévin, *op. cit.*

<sup>227</sup> La peine peut être portée à cinq ans d'emprisonnement et 450 000 euros d'amende si la remise aurait permis d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets (C. pén. art. 434-15-2).

<sup>228</sup> Décision n°2018-696 QPC du 30 mars 2018.



décision semble toutefois critiquable, les juges constitutionnel faisant une interprétation extensive de la jurisprudence de la CEDH sur ce point<sup>229</sup>.

Pour répondre à cette question, il convient de déterminer si le code PIN d'un Ledger peut être considéré comme « *une convention secrète de déchiffrement d'un moyen de cryptologie* » au sens de l'article 434-15-2 du Code pénal. S'il apparaît que le Ledger peut, en lui-même, être considéré comme un moyen de cryptologie au sens de l'article 29 de la loi du 21 juin 2004 ; son code PIN s'apparente d'avantage à un code de déverrouillage qui permet d'accéder aux données qu'il contient. En ce sens, la Cour d'appel de Paris, dans un arrêt en date du 16 avril 2019 (n°18/09267), a considéré que le code de déverrouillage d'un téléphone portable ne constitue pas une convention secrète de déchiffrement puisqu'il ne permet pas de déchiffrer les données contenus sur l'appareil mais permet seulement leur accès. Cependant, il convient de prendre en considération le fait qu'un code PIN peut assurer à la fois une fonction de déverrouillage et de cryptage de l'appareil, à l'image des codes de verrouillage des smartphones d'Apple. Ces précisions devraient donc permettre aux magistrats de considérer que le fait pour l'auteur d'un blanchiment de refuser de divulguer aux enquêteurs le code PIN de son Ledger est passible des peines prévues à l'article 434-15-2 du Code pénal. Toutefois, ces derniers seront peut-être confrontés à des difficultés tenant à la qualification de l'élément moral de l'infraction face à un individu qui prétendrait avoir oublié ledit code.

Enfin, si la clé est stockée au sein d'un *brain wallet* ou d'un *paper wallet*, la possibilité de saisir les crypto-actifs illicites dépendra entièrement de la coopération du blanchisseur avec les autorités compétentes.

Il apparaît donc que la saisie de crypto-actifs illicite dépend de la capacité des autorités compétentes à accéder à la clé privée du délinquant. Au regard des multiples raisons évoquées, cette capacité peut s'avérer extrêmement réduite. Dans ce cas, la seule solution pour priver le délinquant de tout forme d'enrichissement issue de ses infractions réside dans la mise en œuvre d'une saisie en valeur, mais encore faut-il pouvoir déterminer cette valeur, en l'absence d'accès au solde du portefeuille qui détient les actifs illicites résultant du blanchiment<sup>230</sup>.

---

<sup>229</sup> LACAZE Marion, « Constitutionnalité du refus de remise d'une convention secrète de déchiffrement », *AJ pénal*, 27 mai 2018, n°5, 257 p.

<sup>230</sup> PIERSON Frédérique, Capitaine de Police, Responsable du Bureau des avoirs criminels d'Europol, entretien téléphonique mené par Alexandra Puertas, le 10 juin 2020 ; HOUEL Jean-Luc, Ancien enquêteur financier à la section de recherches de Dijon, Ancien chef de la cellule régionale des avoirs criminels, entretien téléphonique mené par Alexandra Puertas, le 11 juin 2020.

**49. – Difficultés pratiques diverses** – Enfin, la saisie de crypto-actifs présentent diverses difficultés tenant d'une part, à leur nature décentralisée qui complexifie la détermination, par les pays, de leur compétence pour saisir<sup>231</sup>, et d'autre part, à leur gestion une fois saisis.

Les pratiques en la matière sont variées<sup>232</sup>. Alors que certains états membres de l'Union Européenne font le choix de conserver les crypto-actifs sur un portefeuille étatique, d'autres considèrent qu'il est nécessaire de les convertir en monnaie fiat, avant jugement, afin que leur valeur soit détenue sur un compte bancaire pendant la durée de la procédure pénale. Cette première option fait courir le risque que les crypto-actifs saisis perdent de la valeur en raison de leur forte volatilité. De plus, la conversion de crypto-actifs génère des coûts de stockage pouvant être élevés (détention d'autant de clés privées qu'il existe de typologie de crypto-actifs à saisir). La seconde option présente, au contraire, le risque que les crypto-actifs saisis prennent beaucoup de valeur à la suite de la vente. Dans ce cas, en cas d'acquiescement ultérieur de l'accusé, la question se posera de savoir si l'état doit indemniser leur propriétaire à hauteur de la perte de valeur subie. Certains états ont fait le choix de compenser intégralement toute perte de valeur.

A l'heure actuelle, en France, il apparaît que l'AGRASC est en capacité de saisir uniquement des bitcoins en raison de l'absence de détention d'autres portefeuilles étatiques. Ces bitcoins « dorment » sur son portefeuille ouvert à la Caisse des dépôts et consignations, le pôle de gestion de l'AGRASC n'ayant pour le moment procédé à aucune vente aux enchères. Toutefois, une réflexion sur le sujet est en cours et devrait donner lieu à des propositions d'ici 2021<sup>233</sup>.

---

<sup>231</sup> EUROJUST, *Cybercrime Judicial Monitor*, décembre 2019, 33 p.

<sup>232</sup> EUROJUST, *Cybercrime Judicial Monitor*, décembre 2019, p. 31-36.

<sup>233</sup> DONAT Etienne, Chargé de communication et de formation à l'Agence de Gestion et de Recouvrement des Avoirs Saisis et Confisqués (AGRASC), interrogé par Alexandra Puertas, le 11 juin 2020.

## **CONCLUSION**

Pour conclure, la politique française de lutte contre le blanchiment commis au moyen de crypto-actifs est fondée sur une double appréhension du phénomène, à la fois préventive et répressive.

La loi PACTE du 22 mai 2019 a permis de poser les fondations d'une réglementation, équilibrée et cohérente, fondée sur les risques d'utilisations à des fins de blanchiment des services servant de passerelles entre l'économie légale et l'économie souterraine. Ce travail n'est cependant pas achevé. L'identification des risques de blanchiment que font encourir les divers usages des crypto-actifs doit se poursuivre afin de parvenir à une régulation plus fine et plus protectrice de l'intérêt général.

D'autre part, d'un point de vue répressif, la définition large de l'infraction de blanchiment retenue dans le Code pénal permet d'appréhender ce nouvel outil de blanchiment que constitue les crypto-actifs. Cependant, la sophistication croissante des procédés utilisés pour obscurcir les transactions financières opérées sur la blockchain entravent parfois gravement les procédures pénales. La répression des auteurs de blanchiment lié aux crypto-actifs est un combat de longue haleine qui nécessite l'octroi, par les pouvoirs publics, de moyens humains et financiers à la hauteur de la complexification des processus criminels.

En outre, l'utilisation des crypto-actifs à des fins de blanchiment tend à remettre en cause l'efficacité de l'approche répressive de la lutte contre le blanchiment. Leur développement en dehors de toute entité centrale de contrôle met à mal la possibilité de priver les délinquants du profit de leur infraction. De surcroît, l'absence de cadre précis quant à la procédure à suivre en matière de saisie et de gestion des crypto-actifs blanchies entraînent leur paralysie, faisant ainsi courir à l'État des risques de pertes de valeur.

En définitive, la politique de lutte anti-blanchiment menée par la France a su s'adapter aux nouveaux risques que constituent les crypto-actifs. Elle n'est cependant pas infaillible, mais remplit tout de même son objectif de prévention en faisant en sorte d'augmenter le coût du blanchiment.

## **BIBLIOGRAPHIE**

### **OUVRAGES JURIDIQUES**

BERGEL Jean-Louis, *Théorie générale du droit*, 5<sup>ème</sup> édition, Dalloz, 2012.

COURBE Patrick, LATINA Mathias, *Droit civil - Les biens*, 8<sup>ème</sup> édition, Dalloz, 2016.

LACROIX Frédéric, « Les places financières alternatives : propos relatifs aux approches réglementaires concernant les plateformes de crowdfunding et d'échanges de bitcoin », in FRISON ROCHE Marie-Anne (dir.), *Internet, espace d'interrégulation*, Dalloz, 2016.

TERRE François, SIMLER Philippe, *Droit civil - Les biens*, 10<sup>ème</sup> édition, Dalloz, 2018.

### **OUVRAGES NON JURIDIQUES**

ARISTOTE, *La Politique*, Jules Tricot (trad.), Paris, Vrin, 1962.

ARISTOTE, *Ethique à Nicomaque*, Jules Tricot (trad.), Paris, Vrin, 1990.

### **ENCYCLOPEDIES**

CAMOUS Éric, *Art. 706 à 706-147 - Fascicule 20 : des saisies pénales spéciales - régime général*, JurisClasseur Procédure pénale, Lexis Nexis, 1<sup>er</sup> janvier 2019, mis à jour le 5 février 2020.

CAMOUS Éric, *Art. 706-148 à 706-158 - Fascicule 20 : des saisies pénales spéciales - régime particuliers*, JurisClasseur Procédure pénale, Lexis Nexis, 19 août 2019, mis à jour le 5 février 2020.

CHOPIN Frédérique, *Cybercriminalité*, Répertoire de droit pénal et de procédure pénale, Dalloz, Janvier 2020.

CUTAJAR Chantal, *Fascicule 10 : blanchiment - prévention du blanchiment*, JurisClasseur Pénal des Affaires, Lexis Nexis, 24 juillet 2020, mis à jour le 31 janvier 2017.

DAURY-FAUVEAU Morgane, *Fascicule 20 : blanchiment - conditions et constitution*, JurisClasseur Pénal des Affaires, Lexis Nexis, 2 mai 2020, 10<sup>°</sup>.

LAMBERTYE-AUTRAND Marie-Christine, *Art. 516 - Fascicule unique : BIENS - Distinctions*, JurisClasseur Civil Code, Lexis Nexis, 12 mai 2011, mis à jour le 31 juillet 2017.

LEGEAIS Dominique, *Fascicule 535 : actifs numériques et prestataires sur actifs numériques*, JurisClasseur Commercial, Lexis Nexis, 14 octobre 2019.

MATSOPOULOU Haritini (dir.), MASCALA Corinne (dir.), *Le Lamy droit pénal des affaires*, Wolters Kluwer, 2020, 1737<sup>°</sup>.

SEGONDS Marc, *Blanchiment*, Dalloz, octobre 2017, mise à jour en mars 2020, 95<sup>°</sup>.

## RAPPORTS ET ETUDES

AGRASC, *Rapport annuel 2017*, 3 juin 2016.

AUTORITE BANCAIRE EUROPEENNE, *Report with advice for the European Commission on crypto-assets*, 9 janvier 2019.

AUTORITE BANCAIRE EUROPEENNE, *Opinion on 'virtual currencies'*, 4 juillet 2014.

AUTORITE DES MARCHES FINANCIERS, *Synthèse des réponses à la consultation publique portant sur les Initial Coin Offerings (ICO) et point d'étape sur le programme « UNICORN »*, février 2018.

AUTORITE EUROPEENNE DES MARCHES FINANCIERS, *Initial coin offerings and crypto-assets*, 9 janvier 2019.

BANQUE CENTRALE EUROPEENNE, *Virtual Currency schemes - a further analysis*, février 2015.

BANQUE CENTRALE EUROPEENNE, *Crypto-Assets : Implications for financial stability, monetary policy, and payments and market infrastructures*, mai 2019.

BANQUE DE FRANCE, *Les dangers liés au développement des monnaies virtuelles : l'exemple du bitcoin*, 5 décembre 2013.

BANQUE DES REGLEMENTS INTERNATIONAUX, *Rapport économique annuel 2018*, 24 juin 2018.

BANQUE MONDIALE, *Remittance Prices Worldwide*, mars 2020.

CHAINANALYSIS, *The 2020 state of crypto crime*, janvier 2020.

COMMISSION EUROPEENNE, *Rapport de la Commission au Parlement européen et au Conseil sur l'évaluation des risques de blanchiment de capitaux et de financement du terrorisme pensant sur le marché intérieur et liés aux activités transfrontières*, 3 p.

CONSEIL DE STABILITE FINANCIERE, *Crypto-assets*, mai 2019.

DELEGATION MINISTERIELLE AUX INDUSTRIES DE SECURITE ET A LA LUTTE CONTRE LES CYBERMENACES, *État de la menace liée au numérique en 2019*, mai 2019.

DIRECTION DES AFFAIRES CRIMINELLES ET DES GRACES, *Fiche juridique et technique - Cryptoactifs*, janvier 2019.

EUROJUST, *Cybercrime judicial monitor*, n°3, décembre 2017.

EUROJUST, *Cybercrime judicial monitor*, n°4, décembre 2018.

EUROJUST, *Common challenges in combating cybercrime as identified by Eurojust and Europol*, juin 2019.

EUROJUST, *Cybercrime Judicial Monitor*, décembre 2019.

EUROPOL, *Internet organised crime threat assessment 2019*, 9 octobre 2019.

FAURE-MUNTIAN Valéria, GANAY Claude, LE GLEUT Ronan, *Les enjeux technologiques des blockchain*, Rapport au nom de l'office parlementaire d'évaluation des choix scientifiques et technologiques, Assemblée nationale, 20 juin 2018.

FOND MONETAIRE INTERNATIONAL, *Global Financial Stability Report*, avril 2018.

GROUPE D'ACTION FINANCIERE, *Virtual currencies: Key definitions and potential AML/CFT Risks*, juin 2014.

GROUPE D'ACTION FINANCIERE, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, juin 2019.

JEANNEAU Clément, *Impact écologique des blockchains et cryptomonnaies : idées reçues et réalités*, Blockchain Partner.

LANDAU Jean-Pierre avec la collaboration de GENAIS Alban, *Les crypto-monnaies*, Rapport au Ministre de l'Économie et des Finances, 4 juillet 2018.

LE MOIGN Caroline, *Ico françaises : un nouveau mode de financement ?*, AMF, novembre 2018.

MONTAUGE Franck, LONGUET Gérard, CHAIZE Patrick, ROBERT Sylvie, MORIN-DESAILLY Catherine, COLLIN Yvon, GATTOLIN André, OUZOULIAS Pierre, BIGNON Jérôme, ARTIGALAS Viviane Artigalas, BASCHER Jérôme, BONNE Bernard, FILLEUL Martine, FRASSA Christophe-André, HERVE Loïc, LAFON Laurent, MAZUIR Rachel, PIEDNOIR Stéphane, PRIMAS Sophie, PUISSAT Frédérique, SAURY Hugues, *Le devoir de souveraineté numérique*, Rapport au nom de la commission d'enquête sur la souveraineté numérique, Sénat, 1<sup>er</sup> octobre 2019.

STALINSKY Steven, *The coming storm : terrorists using cryptocurrency*, MEMRI, 21 août 2019.

TRACFIN, *Rapport d'activité 2011*.

TRACFIN, *Tendances et analyse des risques de blanchiment de capitaux et de financement du terrorisme en 2016*, 13 avril 2018.

TRACFIN, *Tendances et analyse des risques de blanchiment de capitaux et de financement du terrorisme en 2017-2018*, 28 novembre 2018.

WOERTH Eric, PERSON Pierre, BARROT Jean-Noël, BRICOUT Jean-Louis, COQUEREL Eric, DUFREGNE Jean-Paul, VIGIER Philippe, *Monnaies virtuelles*, Rapport au nom de la commission des finances, de l'économie générale et du contrôle budgétaire, Assemblée nationale, janvier 2019.

## ARTICLES JURIDIQUES

ALMASEANU Stephen, « Le traitement pénal du Bitcoin et des autres monnaies virtuelles », *Gazette du Palais*, 30 août 2014, n°242.

BALI Mehdi, « Les crypto-monnaies, une application des block chain technologies à la monnaie », *Revue de Droit bancaire et financier*, n°2, janvier 2015, étude 8.

BONNEAU Thierry, « Tokens, titres financiers ou biens divers ? » *Revue de Droit bancaire et financier*, janvier 2018.

BOULOC Bernard, « De quelques aspects du délit de blanchiment », *Revue de droit bancaire et financier*, 2002.

BROSSET Jérôme, LORENTZ Philippe, BARBET-MASSIN Alice, « Les activités sur actifs numériques issues de la loi PACTE », *Revue Lamy droit des affaires*, n°151, 1<sup>er</sup> septembre 2019.

CABON Sarah-Marie, « L'influence du cyber espace sur la criminalité économique et financière », *Droit pénal*, mars 2018, n°3.

CHAMBRE DE COMMERCE INTERNATIONALE, « Virtual money laundering threat identified », sur *Service de la criminalité commerciale de la Chambre de commerce internationale* [en ligne], 12 novembre 2017, [consulté le 17 mars 2020], [https://icc-ccs.org/icc\\_2527/index.php/388-virtual-money-laundering-threat-identified](https://icc-ccs.org/icc_2527/index.php/388-virtual-money-laundering-threat-identified).

CORBION-CONDE Lycette, « De la défiance à l'égard des monnaies nationales au miroir du bitcoin », *Revue de Droit bancaire et financier*, mars 2014, dossier 13, n°2.

DE VAUPLANE Hubert, « La qualification juridique de certains tokens en titre de créance », *Revue trimestrielle de droit financier*, n°4, 2017.

DUTEIL Gilles, « Modes opératoires et évolutions », *AJ Pénal*, 2016.

LACAZE Marion, « Constitutionnalité du refus de remise d'une convention secrète de déchiffrement », *AJ pénal*, 27 mai 2018, n°5.

LE GUEN Olivier, « Questions à Olivier Le Guen sur la perquisition et la saisie des crypto-actifs », *Dalloz IP/IT*, octobre 2019.

MARRAUD DES GROTTES Gaëlle, « Prestataires de services sur actifs numériques : le décret est paru ! », *Wolters Kluwer France - Actualités du droit*, 22 mai 2019.

MARRAUD DES GROTTES Gaëlle, « Anne Maréchal, directrice des affaires juridiques de l'AMF : Avec ce visa optionnel, nous espérons créer un écosystème attractif qui permette d'attirer en France les beaux projets d'ICO », *Wolters Kluwer France - Actualités du droit*, 22 mai 2019

MARRAUD DES GROTTES Gaëlle, « Loi PACTE : point sur l'encadre des prestataires de services sur actifs numériques », *Wolters Kluwer France - Actualités du droit*, 23 mai 2019.

MARTINON Jacques, « Crypto-actifs : la justice pénale à l'épreuve des cryptomonnaies », *Dalloz IP/IT*, octobre 2019.

MOREIL Sophie, « Le tribunal de commerce de Nanterre prend position sur la nature du prêt de bitcoins », *Gazette du Palais*, 9 juin 2020, n°21.

NJABOUM Jessica Joyce, « Régime juridique des ICOs et nature juridique des tokens », *Revue internationale des services financiers*, 2020, n°1.

NJABOUM Jessica Joyce, *op. cit.* ; SOLERANSKI Louis, « Réflexions sur la nature juridique des tokens », *Bulletin Joly Bourse*, 1<sup>er</sup> mai 2018, n°3.

O’RORKE William, « La mise en œuvre des obligations LCB-F par l’industrie crypto », *Revue internationale de la compliance et de l’éthique des affaires*, février 2020, n°1, étude 38.

POLROT Simon, « La régulation LCB-FT face à l’émergence des cryptomonnaies », *Revue internationale de la compliance et de l’éthique des affaires*, février 2020, n°1, étude 38.

REBUT Didier, « Manquement du banquier à ses obligations professionnelles et commission du délit de blanchiment », *Banque et droit*, 2003, n°88.

ROUSSILLE Myriam, « Le bitcoin : objet juridique non identifié », *Banque et Droit*, janvier 2015, n°159.

SOLERANSKI Louis, « Réflexions sur la nature juridique des tokens », *Bulletin Joly Bourse*, 1<sup>er</sup> mai 2018, n°3.

## ARTICLES NON JURIDIQUES

AGLIETTA Michel, « La confiance dans la monnaie est l’alpha et l’oméga de la société », sur le blog de *Deloitte France* [en ligne], le 17 février 2016, <https://blog.deloitte.fr/michel-aglietta-cepii-la-confiance-dans-la-monnaie-est-l-alpha-et-l-omega-de-la-societe/>.

CEILLES Mathilde et AFP AGENCE, « France : un trafic de bitcoins démantelé », *Le Figaro*, 7 juillet 2014, <https://www.lefigaro.fr/actualite-france/2014/07/07/01016-20140707ARTFIG00189-france-un-traffic-de-bitcoins-demantele.php>.

CYPEL Sylvain, « L’affaire Liberty Reserve révèle les liens entre monnaies virtuelles et criminalité », *Le Monde*, 29 mai 2013, [https://www.lemonde.fr/economie/article/2013/05/29/l-affaire-liberty-reserve-revele-les-liens-entre-monnaies-virtuelles-et-criminalite\\_3420048\\_3234.html](https://www.lemonde.fr/economie/article/2013/05/29/l-affaire-liberty-reserve-revele-les-liens-entre-monnaies-virtuelles-et-criminalite_3420048_3234.html).

DE MENTHON Pierre-Henri et SYFUSS-ARNAUD Sabine, « Brexit, inflation, dettes... Les premières vérités de Christine Lagarde » [Interview], *Challenges*, 8 janvier 2020, [https://www.challenges.fr/economie/brexit-inflation-dettes-les-premieres-verites-de-christine-lagarde\\_692623](https://www.challenges.fr/economie/brexit-inflation-dettes-les-premieres-verites-de-christine-lagarde_692623).

HABER Stuart et STORNETTA W. Scott, « How to time-stamp a digital document », *Journal of Cryptology*, janvier 1991, n°3.

LA TRIBUNE AVEC AFP, « Karpelès, le baron français du bitcoin, condamné au Japon », *La Tribune* [en ligne], 15 mars 2019, <https://www.latribune.fr/economie/international/karpeles-le-baron-francais-du-bitcoin-condamne-au-japon-810794.html>.



MC GARRY Dan, NANUA Richard et MALAPA Terence, « Six chinese face deportation », *Vanuatu Daily Post* [en ligne], juin 2019, [https://dailypost.vu/news/six-chinese-face-deportation/article\\_fef7f311-679d-5d1b-9ec5-4f44e73118bb.html](https://dailypost.vu/news/six-chinese-face-deportation/article_fef7f311-679d-5d1b-9ec5-4f44e73118bb.html).

PASQUIER Julie, « Virus à l'agglo de grand cognac : une attaque sans précédent », *Charente Libre*, 22 octobre 2019, <https://www.charentelibre.fr/2019/10/22/virus-a-l-agglo-de-grand-cognac-une-attaque-sans-precedent,3505276.php>.

PEBEREAU Michel, « La monnaie, une affaire de confiance », *Les Échos*, le 1<sup>er</sup> juillet 2013, <http://archives.lesechos.fr/archives/2013/Enjeux/00302-021-ENJ.htm>.

POPPER Nathaniel, « Terrorists Turn to Bitcoin for Funding and They're Learning Fast », *The New York Times*, 18 août 2019, <https://www.nytimes.com/2019/08/18/technology/terrorists-bitcoin.html>.

R. Remy, « AMLD5 aux Pays-Bas : un désastre pour les petites crypto-entreprises », *Journal du coin* [en ligne], 29 avril 2020, <https://journalducoin.com/regulation/loi-amld5-pays-bas-desastre-pour-les-petites-crypto-entreprises>

TRIOILLIER Gilles, « Frappé par une cyberattaque massive, le CHU de Rouen forcé de tourner sans ordinateurs », *Le Monde*, le 18 novembre 2019, [https://www.lemonde.fr/pixels/article/2019/11/18/frappe-par-une-cyberattaque-massive-le-chu-de-rouen-force-de-tourner-sans-ordinateurs\\_6019650\\_4408996.html](https://www.lemonde.fr/pixels/article/2019/11/18/frappe-par-une-cyberattaque-massive-le-chu-de-rouen-force-de-tourner-sans-ordinateurs_6019650_4408996.html).

VAN DAMME Ingrid, « Une monnaie singulière, le cauri », sur *Musée de la Banque nationale de Belgique* [en ligne], 11 janvier 2007, [consulté le 11 mars 2020], <https://www.nbbmuseum.be/fr/2007/01/cowry-shells.htm>.

WILLIAMS Jessica, « Cyberattack has cost New Orleans \$7.2 million; city email still not fully restored; tax payment deadline delayed », *The Times-Picayune*, 15 janvier 2020, [https://www.nola.com/news/politics/article\\_8dbed526-37d0-11ea-9998-bbe9bfc93b5b.html](https://www.nola.com/news/politics/article_8dbed526-37d0-11ea-9998-bbe9bfc93b5b.html).

## SITES INTERNET

ANSSI, « La certification de sécurité de produits », sur ANSSI [en ligne], [consulté le 14 juin 2020], [https://www.ssi.gouv.fr/uploads/2018/01/certification\\_securite\\_produits\\_visa\\_securite\\_anssi.pdf](https://www.ssi.gouv.fr/uploads/2018/01/certification_securite_produits_visa_securite_anssi.pdf).

BLOCKCHAIN FRANCE, « Qu'est-ce que la blockchain ? », sur *Blockchain France* [en ligne], [consulté le 13 mars 2020], <https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/>.

COINMARKETCAP, All cryptocurrencies, sur *Coinmarketcap* [en ligne], [consulté le 10 juin 2020], <https://coinmarketcap.com/all/views/all/>.

CULTURE INFORMATIQUE, « C'est quoi une adresse IP ? », publié le 21 octobre 2012, [consulté le 6 juin 2020], <https://www.culture-informatique.net/c-est-quoi-une-adresse-ip-niv1/>.

LEDGER, « Setting a New Standard: Ledger Nano S becomes the First and Only Certified Hardware Wallet on the Market », sur *Ledger* [en ligne], 18 mars 2019, [consulté le 14 juin 2020], <https://www.ledger.com/setting-a-new-standard-ledger-nano-s-becomes-the-first-and-only-certified-hardware-wallet-on-the-market/>.

LEDGER, « Ledger continues its security certification program with Ledger Nano X », sur *Ledger* [en ligne], 22 octobre 2019, [consulté le 14 juin 2020], <https://www.ledger.com/ledger-nano-x-recognized-as-certified-crypto-hardware-wallet>.

MONERO, « FAQ : How is Monero's privacy different from other coins », sur *Monero* [en ligne], <https://web.getmonero.org/get-started/faq/>

MONERO, « Monero : Stealth Addresses » [vidéo en ligne], Youtube, 4 avril 2017, [consultée le 9 juin 2020], <https://www.youtube.com/watch?v=bWst278J8NA>.

MONERO, « Monero : Ring Signatures » [vidéo en ligne], Youtube, 12 juin 2017, [consultée le 9 juin 2020], [https://www.youtube.com/watch?v=zHN\\_B\\_H\\_fCs](https://www.youtube.com/watch?v=zHN_B_H_fCs)

MONERO, « Monero : Ring Confidential Transactions » [vidéo en ligne], Youtube, 21 août 2017 2017, [consultée le 9 juin 2020], <https://www.youtube.com/watch?v=M3AHp9KgTkQ>.

TETHER, « Tether : Fiat currencies on the Bitcoin blockchain », sur *Tether* [en ligne], [consulté le 10 juin 2020], <https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf>.

THE STABLECOIN INDEX, « Market cap » [en ligne], sur *The stablecoin index* [consulté le 10 juin 2020], <https://stablecoinindex.com/marketcap>.

TOR, « Tor: overview » [en ligne], sur *Tor*, <https://2019.www.torproject.org/about/overview.html.en>.

## **COURRIEL**

NAKAMOTO Satoshi, *Bitcoin P2P e-cash paper* [courriel], 1<sup>er</sup> novembre 2008 sur The Cryptography Mailing List.

## **DISCOURS**

VILLEROY DE GALHAU François, Gouverneur de la Banque de France, *Bitcoin* [déclaration], Pékin, 1<sup>er</sup> décembre 2017.

VILLEROY DE GALHAU François, *Monnaies digitale de banque centrale et paiements innovants* [discours], Paris, 4 décembre 2019.

## **LISTE DES PERSONNES INTERROGÉES**

**AZENCOTH Jeremy**, Étudiant en économie gestion à l'université Paris 2 Panthéon-Assas, Membre du pôle blockchain, fintech et cryptoactifs au sein de l'association Assas Legal Innovation

**DONAT Etienne**, Chargé de communication et de formation à l'Agence de Gestion et de Recouvrement des Avoirs Saisis et Confisqués (AGRASC)

**DUBOIS Kévin**, Analyste criminel à l'Office Central de Lutte contre la Cybercriminalité (OCLCTIC), Expert en crypto-actifs

**HOUEL Jean-Luc**, Ancien enquêteur financier à la section de recherches de Dijon, Ancien chef de la cellule régionale des avoirs criminels, Expert en investigations numériques au sein des sociétés WebDrone et Check & Trust

**O'RORKE William**, Avocat fondateur du Cabinet ORWL Avocats

**PEZENEC Thierry**, Commandant de Police, Chef du SIRASCO-financier

**PIERSON Frédéric**, Capitaine de Police, Responsable du Bureau des avoirs criminels d'Europol

**PUTIGNY Hervé**, Ancien cyber-enquêteur à la section de recherches de Dijon, Directeur général et co-fondateur de la société WebDrone

**STACHTCHENKO Alexandre**, Co-fondateur et Directeur général de Blockchain Partner

**VERNIER Eric**, Docteur ès sciences de gestion HDR, Spécialiste du blanchiment de capitaux

**Authors: Vandana Beessoo**

**Lecturer in law**

**Middlesex university**

**Flic en flac**

**Zaynab Foondun**

**Student in law**

**Flic en flac**

## **Money Laundering through Bitcoin: The emerging implications of Technological Advancement.**

### **Abstract**

Bitcoin, conceived by the pseudonymous software developer Satoshi Nakamoto, is the world's first cryptocurrency. This invention of peer-to-peer electronic cash has triggered a series of apprehension in the financial world. The fact that it has enabled alternative means of transacting to conventional banking has steered a new source of stress within the financial arena. Bitcoin, in terms of technology and currency, has been defined in many ways. Albeit Paul Vigna and Michael Casey describe it as borderless, pseudo-anonymous, decentralised, and outside of regulatory monetary systems, other researches also suggest that these attributes potentially give rise for criminals to evade law enforcement. The focal point of this paper is to provide an insight on the emergence of illicit financial crimes particularly through money laundering, caused by the increasing use of bitcoins. The research paper explicates on two very common ways for "bitcoin laundering" namely: either through bitcoin mixes or bitcoin exchanges or by using both methods. The risk of money laundering is facilitated by the anonymous feature of bitcoin especially when coupled with sophisticated money laundering services, also known as bitcoin mixing, provided on the Darknet. The second strategy of cashing-out dirty bitcoin

through bitcoin exchanges unfolds the issue of regulated and unregulated bitcoin exchanges businesses. The other issue with bitcoin exchanges is that they have now turned to a new shadow banking system of doing off-chain transactions on behalf of their customers to outsiders without any regulations in place. The process of laundering money through bitcoin has become easier and accessible to a greater audience, especially when existing laws are not being applied appropriately. In this context, this paper is of the view that the European Union is the best platform to study cybercrimes, especially crimes related to bitcoin. This paper shall discuss the existing legal and regulatory frameworks provided by the European Union to curb cybercrimes but also, by illustrating the attempts (and the lack of attempts) made by the English and German governments to regulate risks of cybercrimes posed by cryptocurrency.

## **Introduction**

The emergence of cryptocurrencies, primarily bitcoin, could be attributed to the global financial crisis of 2008 where the banking system was rescued by governments which had to provide significant loans to major banks.<sup>1</sup> Before the major downfall, economies in many countries went through a period of recession and the remedies executed to stimulate economic growth were not strong enough to pull those economies out of that slumping phase.<sup>2</sup> In this respect, many economies, such as Iceland, were thrust to use the digital economy as a boost.<sup>3</sup> This alternative virtual economy gave rise to online markets, such as Silk Road which was created by an entrepreneur, Ross Ulbricht.<sup>4</sup> That online market was only available on an encrypted part of the Internet dubbed the Darknet. This innovative platform quickly became a double-edged sword catering for both legal and illegal services and products to be sold.<sup>5</sup> However, Silk Road was an illicit website which used the cryptocurrency, bitcoin, to keep its users anonymous via the blockchain technology, a decentralised ledger which works by

---

<sup>1</sup> Andres Guadamuz and Chris Marsden, 'Blockchains and Bitcoin: Regulatory Responses to Cryptocurrencies' (2015) 20(12) *Sussex Research Online*.

<sup>2</sup> *ibid.*

<sup>3</sup> *ibid.*

<sup>4</sup> Daniel Decary-Hetu and Benoit Dupont, 'Reputation in a Dark Network of Online Criminals' (2013) 14 (2/3) *Global Crime* <<https://www.tandfonline.com/doi/abs/10.1080/17440572.2013.801015>> accessed 5 June 2018.

<sup>5</sup> *ibid.*

transcending state regulations thus skirting government intervention.<sup>6</sup> In 2013, the FBI, finally, unearthed all the illicit activities that were conducted on Silk Road which eventually led to its shut down and brought bitcoin in the limelight.<sup>7</sup>

This research paper will only focus on one particular illicit activity, i.e, money laundering which is further exacerbated on the Darknet. This paper sheds light on the various ways bitcoin laundering is facilitated through the innovative digital currency exchanges services available on the Darknet.<sup>8</sup> The cryptocurrency market capitalisation was valued at over \$200 billion in early 2018 and \$1.36 billion were already stolen by cryptocurrency scammers in that same period.<sup>9</sup> It is thought that if that trend were to continue until the end of the year, bitcoin misuse would amount to \$3.25 billion<sup>10</sup> which is almost the GDP of a small country such as Eritrea.<sup>11</sup> Again in 2017, AlphaBay and Hansa, two of the most popular Darknet marketplaces were taken down due to the illicit transactions occurring such as the sale of illegal drugs, toxic chemicals and fraudulent services.<sup>12</sup> The preferred currency was none other but bitcoin, which unintentionally has helped to expand a major underground criminal economy with the potential of affecting millions of lives.<sup>13</sup> This shadow banking system intentionally uses cryptocurrency to obfuscate authorities from identifying cybercriminals to eventually evade effective criminal prosecution.

Therefore, this research paper will expound on two different methods namely of cashing-out strategy through bitcoin mixes and bitcoin exchanges. Cybercriminals prefer bitcoin for digital criminal enterprise because of its easy access, low transactional costs and especially for being borderless or unhindered by jurisdictions. Bitcoin, nowadays, is said to be the enabler of the two below types of cybercrimes:<sup>14</sup>

---

<sup>6</sup> *ibid.*

<sup>7</sup> *ibid.*

<sup>8</sup> Yaya J Fanusie and Tom Robinson, 'Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services' (2018) <<https://info.elliptic.co/whitepaper-fdd-bitcoin-laundering>> accessed on 19 May 2018.

<sup>9</sup> *ibid.*

<sup>10</sup> *ibid.*

<sup>11</sup> Eritrea Economic Forecasts – 2018-2020 <<https://tradingeconomics.com/eritrea/forecast>> accessed on 5 June 2018.

<sup>12</sup> Europol, 'Massive Blow to Criminal Dark Web Activities after Globally Coordinated Operation' (2017) <<https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation>> accessed 5 June 2018.

<sup>13</sup> Yaya J Fanusie and Tom Robinson, 'Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services' (2018) <<https://info.elliptic.co/whitepaper-fdd-bitcoin-laundering>> accessed on 19 May 2018.

<sup>14</sup> Ross Anderson, Ilia Shumailov, Mansoor Ahmed and Alessandro Rietmann, 'Bitcoin Redux' (2018) WEIS <[https://weis2018.econinfosec.org/wp-content/uploads/sites/5/2018/05/WEIS\\_2018\\_paper\\_38.pdf](https://weis2018.econinfosec.org/wp-content/uploads/sites/5/2018/05/WEIS_2018_paper_38.pdf)> accessed 1 June 2018.

- 1) Crimes that the Internet and computers **enable** such as ransomware or hacking;<sup>15</sup> and
- 2) Crimes such as drug trafficking on online forums whereby cybercriminals use the Internet and computers to **assist** those illicit transactions.<sup>16</sup>

It is observed that bitcoin has become the preferred method of payment on the criminal underground economy, for instance, victims attacked by ransomware are forced to send an amount of fiat currency converted into bitcoin to the required bitcoin address provided by those cybercriminals.<sup>17</sup> The newest tactic employed is to use the cash-out strategy to facilitate money laundering.<sup>18</sup> As stated by Levi, the cybercrime proceeds of criminals need to be covered by a secured cash-out strategy without the chance of being traced back to the associated crime and bitcoin fits the job squarely.<sup>19</sup> Usually, a cybercriminal will not start his cash-out tactic with bitcoin but will rather use the bitcoin ecosystem as a means of anonymisation of what the cash-out strategy involves.<sup>20</sup> This anonymisation process is further solidified by two key services provided on the Darknet, namely: bitcoin mixers and bitcoin exchanges which will facilitate to launder those cybercrime proceeds.<sup>21</sup> The mixing services aim at obfuscating bitcoin from its criminal sources and the exchanges services are provided to change bitcoin to fiat money or vice-versa anonymously.

Following that, as assessed by the Elliptic research paper in early 2018,<sup>22</sup> this paper views the European Union as the best platform to assess cybercrimes as bitcoin exchanges located in the European region has gathered the most important percentage share of 37.33 % to a less significant percentage share of 7.10% as compared to North American markets.<sup>23</sup> Europol has also estimated a rise of 3-4% of crime proceeds being laundered through bitcoin in Europe.<sup>24</sup> In a similar vein, existing legal and regulatory frameworks of the European Union will also be discussed throughout this paper to show if applied correctly, they could be used to curb cryptocurrency cybercrimes. It will seek to also endeavour to demonstrate the attempts (or lack

---

<sup>15</sup> *ibid.*

<sup>16</sup> *ibid.*

<sup>17</sup> *ibid.*

<sup>18</sup> *ibid.*

<sup>19</sup> Michael Levi, 'Money for crime and money from crime: financing crime and laundering crime proceeds', (2015) 21(2) *European Journal on Criminal Policy and Research*.

<sup>20</sup> Ross Anderson, Ilia Shumailov, Mansoor Ahmed and Alessandro Rietmann, 'Bitcoin Redux' (2018) WEIS <[https://weis2018.econinfosec.org/wp-content/uploads/sites/5/2018/05/WEIS\\_2018\\_paper\\_38.pdf](https://weis2018.econinfosec.org/wp-content/uploads/sites/5/2018/05/WEIS_2018_paper_38.pdf)> accessed 1 June 2018.

<sup>21</sup> *ibid.*

<sup>22</sup> Yaya J Fanusie and Tom Robinson, 'Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services' (2018) <<https://info.elliptic.co/whitepaper-fdd-bitcoin-laundering>> accessed on 19 May 2018.

<sup>23</sup> *ibid.*

<sup>24</sup> *ibid.*

thereof) by the English and German governments to regulate risks of cybercrimes posed by cryptocurrency. As submitted by Europol, international collaboration in terms of operational and technical expertise to set up a law enforcement strategy will only gain leverage if there is an open data-sharing policy in place between jurisdictions.<sup>25</sup> The take-down of the two major illicit marketplaces on the Darknet was only possible due to the good faith of collective global law enforcement power which brought a halt to these major criminal activities.

Digital payments are mainly used for legal services and goods because of its easy traceability aspect. The advent of cryptocurrencies, however, which also allow for e-commerce, has additional features to it as it combines digitisation of trade with anonymity of transactions by adopting the new technology of blockchain. The blockchain, a decentralised system, allows for the cross-border commerce to take place with complete anonymity which grants cybercriminals a chance of escaping conventional law enforcement watchdogs. For potential cybercrimes to take place unnoticed, this opportunity is the perfect structural shift from regulated conventional banking systems to the cryptocurrency mechanism on the Darknet.

The internet uses standard means of communications using data packets.<sup>26</sup> These standards are internet protocols, e.g. 'http', whereas the Darknet works similar to the internet except that its access is only granted through specific communications protocols which are created to anonymise data send over it.<sup>27</sup> It uses The Onion Router (TOR) which was developed initially by the US Navy.<sup>28</sup> Transactions occurred between two clients on this network pass through different nodes on the TOR network and in turn, TOR obfuscates the IP address of the transaction between the customers and, anonymity is eventually guaranteed.<sup>29</sup> As can be observed, Bitcoin has ultimately made possible what PayPal did for EBay, but the latter for illicit purposes on the Darknet.<sup>30</sup> This combination of bitcoin and Darknet, has led to the

---

<sup>25</sup> Europol, 'Exploring tomorrow's organised crime' (2015) < [www.europol.europa.eu/sites/default/files/Europol\\_OrgCrimeReport\\_web-final.pdf](http://www.europol.europa.eu/sites/default/files/Europol_OrgCrimeReport_web-final.pdf).> accessed 5 June 2018.

<sup>26</sup> Roger Dingledine, Nick Mathewson and Paul Syverson, 'Tor: the second-generation onion router' 13 Proceedings of the 13th Conference on USENIX Security Symposium < <https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf> > accessed on 5 June 2018

<sup>27</sup> *ibid.*

<sup>28</sup> *ibid.*

<sup>29</sup> *ibid.*

<sup>30</sup> *ibid.*



proliferation of Darknet marketplaces such as Silk Road.<sup>31</sup> Despite its shutdown in 2013 and numerous new take downs and seizures such as ‘Operation Onymous’ in 2014 which took down 410 hidden services and seized \$1 million worth of bitcoin, other illegal services keep springing up.<sup>32</sup> For instance, in 2007 one of the largest marketplaces that were shut down was AlphaBay which had on its platform more than 350,000 illicit items for sale.<sup>33</sup> Hence, there is no doubt that Bitcoin has helped the facilitation of Darknet marketplaces.<sup>34</sup>

Researches such as Koshy et al are of the view that even though bitcoin is the preferred currency of these illicit transactions, it has actually made it easier for law enforcement to uncover these unlawful activities due to the public nature of the blockchain, despite the cryptocurrency’s anonymity feature.<sup>35</sup> They argue that monitoring transactions that were effectuated from computers to the blockchain enable regulators to link individual transactions to the IP address of the sender.<sup>36</sup> Meiklejohn et al further state ‘that tracing bitcoin theft on the blockchain from bitcoin exchanges could be used by authorities with subpoena powers, to potentially identify perpetrators’.<sup>37</sup> Hence, many other methods have been developed by cybercriminal enthusiasts to circumvent these ‘loopholes’ of the bitcoin and also, to further secure their transactions even though they use the TOR network.<sup>38</sup> Hence, law enforcement have discovered that there are increasingly new mix methodologies of laundering money being invented, as criminals try to take opportunity of the weaknesses of different sectors.<sup>39</sup> The rationale behind those methodologies varies from the intention to confuse audit trail or to continue investing into illicit activities.<sup>40</sup> This paper seeks to put in the limelight two different methodologies employed by criminals to launder money: 1) bitcoin mixing and 2) bitcoin exchanges.

---

<sup>31</sup> *ibid.*

<sup>32</sup> *ibid.*

<sup>33</sup> Europol, ‘Massive Blow to Criminal Dark Web Activities after Globally Coordinated Operation’ (2017) <<https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation>> accessed 5 June 2018.

<sup>34</sup> *ibid.*

<sup>35</sup> Philip Koshy, Diana Koshy, and Patrick McDaniel, ‘An Analysis of Anonymity in Bitcoin Using P2P Network Traffic’ (2014) Financial Cryptography and Data Security: 18th International Conference, FC 2014 <<https://pdfs.semanticscholar.org/c277/62257f068fdbb2ad34e8f787d8af13fac7d1.pdf>> accessed 5 June 2018.

<sup>36</sup> *ibid.*

<sup>37</sup> Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey Voelcker, and Stefan Savage, ‘A Fistful of Bitcoins: Characterising Payments Among Men with no Names’ (IMC ,2013).

<sup>38</sup> *ibid.*

<sup>39</sup> Yaya J Fanusie and Tom Robinson, ‘Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services’ (2018) <<https://info.elliptic.co/whitepaper-fdd-bitcoin-laundering>> accessed on 19 May 2018.

<sup>40</sup> *ibid.*

## Bitcoin Mixing Strategy

Research by a group of academics from Cambridge University has demonstrated that bitcoin mixings is one way for cybercriminals to launder bitcoin to engage in illicit activities on the Darknet as a way of laundering money.<sup>41</sup> As explained, the blockchain allows for traceability of transactions which is used by law enforcement to identify and trace back criminals by using cryptocurrency exchanges to screen their client's funds transactions linking to crime proceeds. 'Bitcoin mixing' also known as 'bitcoin tumbling', are actually a means of preventing such tracing, by making it nearly impossible to identify the transaction source.<sup>42</sup>

This method is run by a centralised service which takes a fee of 1-10% of the amount mixed and can be implemented in different ways, but the basic principle involves a number of people coming together and pooling their bitcoins.<sup>43</sup> Finally, they then take back bitcoin of the same value.<sup>44</sup> These bitcoins are most likely to have come from different sources than the ones they have brought to the mixer.<sup>45</sup> In this light, this process of mixing bitcoins can be seen as equivalent of using bank accounts in certain jurisdictions to launder "dirty" money whereby the launderers rely on the laws of bank secrecy such as in Switzerland to ensure that the source of the funds cannot be identified.<sup>46</sup> In a similar way, bitcoin mixer users rely on these service providers to not disclose the source of each bitcoin going through the mixing process or even any information about its users.<sup>47</sup>

Although, bitcoin mixing has a negative connotation of being attached to illicit transactions, there are also completely innocent reasons to use such services. As is known, the public nature of the blockchain publishes every bitcoin holder's transaction on its ledger and thus, could sometimes provide an uncomfortable level of transparency as compared to traditional payment systems.<sup>48</sup> For instance, payments in bitcoin for a pair of shorts or pizza could be queried on the blockchain. The mixing service can therefore prevent such snooping and give a sense of financial privacy.<sup>49</sup>

---

<sup>41</sup> Ross Anderson, Ilia Shumailov, Mansoor Ahmed and Alessandro Rietmann, 'Bitcoin Redux' (2018) WEIS <[https://weis2018.econinfosec.org/wp-content/uploads/sites/5/2018/05/WEIS\\_2018\\_paper\\_38.pdf](https://weis2018.econinfosec.org/wp-content/uploads/sites/5/2018/05/WEIS_2018_paper_38.pdf)> accessed 1 June.

<sup>42</sup> *ibid.*

<sup>43</sup> *ibid.*

<sup>44</sup> *ibid.*

<sup>45</sup> *ibid.*

<sup>46</sup> *ibid.*

<sup>47</sup> *ibid.*

<sup>48</sup> *ibid.*

<sup>49</sup> *ibid.*

There are other ways of reclaiming this degree of financial privacy such as by simply depositing bitcoins at an exchange or wallet service, which allow you to prevent tracing of funds by third parties.<sup>50</sup> This is so because those services work similarly as the mixing services with the only difference is that these services keep a record of transactions made and corresponds it to which client in contrast to the mixing services.<sup>51</sup> The information recorded are not for public knowledge, but are kept in case of disclosure of information is needed by law enforcement authorities to trace funds.<sup>52</sup> Albeit these options are available, money launderers prefer mixing services available on the Darknet through bitcoin laundering to evade law enforcement.<sup>53</sup>

### Bitcoin Exchange Strategy

The second method used by cybercriminals to launder money via bitcoin is to use the cash-out strategy which can occur in two different generic techniques.<sup>54</sup> As noted, there are numerous types of services offered on the dark market facilitating money laundering.<sup>55</sup> Laundering enthusiasts provide the bitcoin exchange services whereby they accept ‘dirty’ cryptocurrency and arrange to convert them into fiat money such as pounds.<sup>56</sup> Europol, in 2016, arrested individuals connected with laundering bitcoin on the Darknet for euros.<sup>57</sup> Dutch authorities also stated that drug dealers allegedly converted bitcoin proceeds from the sale of drugs into euros which they then withdrew at ATMS.<sup>58</sup> The other way this strategy works is when criminals would try to “cleanse” their dirty fiat currency into a bank and then using a cryptocurrency exchange to convert the funds into bitcoin. They would subsequently engage in numerous cryptocurrency purchases or transfers to cover the illegal origin of their funds.<sup>59</sup>

---

<sup>50</sup> *ibid.*

<sup>51</sup> *ibid.*

<sup>52</sup> *ibid.*

<sup>53</sup> *ibid.*

<sup>54</sup> Rolf van Wegberg, Jan-Jaap Oerlemans, Oskar van Deventer, ‘Bitcoin Money Laundering: Mixed Results? An Explorative Study on Money Laundering of Cybercrime Proceeds using Bitcoin’ (2008) 25(2) *Journal of Financial Crime*.

<sup>55</sup> *ibid.*

<sup>56</sup> David Meyer, ‘South Korea Reportedly Plans to Hit Bitcoin Exchanges with Massive Tax Bills’ *Fortune* (New York City, January 2018) < <http://fortune.com/2018/01/22/south-korea-bitcoin-exchange-tax/> > accessed 5 June 2018.

<sup>57</sup> *ibid.*

<sup>58</sup> *ibid.*

<sup>59</sup> *ibid.*

## CASE STUDIES

### Case Studies

#### 1. Case of AlphaBay:

The largest criminal dark-market, AlphaBay, was taken down in 2017. It had a traffic of more than 200,000 users and 40,000 vendors.<sup>60</sup> According to Europol, the value of transactions on the site since its inception in 2014 was more than 860 million euros.<sup>61</sup> This operation was also dubbed Operation Bayonet in collaboration with global actors such as the FBI and DEA succeeded in identifying its creator and administrator who was residing in Thailand and was found dead before being extradited to the US.<sup>62</sup> The platform was ultimately shutdown and millions of euros worth of bitcoin and cryptocurrencies were seized which were the payment methods of the dark boutique.<sup>63</sup> The servers in the Netherlands and Canada were also seized. Many of the transactions on AlphaBay were enabled due to bitcoin mixing as was found by the US Justice Department.<sup>64</sup> Unsurprisingly, the Bitmixer.io, a bitcoin mixing service provided also shut down as soon as AlphaBay went down.<sup>65</sup> This mission was accomplished only due

---

<sup>60</sup> Alistair Walsh 'Alphabay and Hansa Darknet Markets Shut Down after International Police Operation' (2017) < <https://www.dw.com/en/alphabay-and-hansa-darknet-markets-shut-down-after-international-police-operation/a-39776885>> accessed 6 June 2018.

<sup>61</sup> *ibid.*

<sup>62</sup> *ibid.*

<sup>63</sup> *ibid.*

<sup>64</sup> *ibid.*

<sup>65</sup> *ibid.*

to the global concerted efforts of law enforcement agencies in the Netherlands, Canada, United States and Thailand.<sup>66</sup>

## 2. Case of Hansa:

Hansa also known as the third-largest criminal marketplace on the Darknet was disrupted and identified by Dutch police in 2017.<sup>67</sup> It offered a platform for the illicit sales of drugs and other illegal services in high volume, as confirmed by Europol.<sup>68</sup> The High Tech Crime Unit in the Netherlands stated that it took 10 months of intense investigation working in collaboration with international cybercrimes units globally.<sup>69</sup> During their investigation also known as Operation Bayonet, it was realised that this decentralised international dark market spanned until Germany.<sup>70</sup> The Dutch police hijacked the perpetrators accounts on Hansa and took full control of the site.<sup>71</sup> They believed a change in tactic, i.e instead of shutting it down abruptly, they would take over covertly to uncover other similar activities on the Darknet. In their search, they have found that the number of members on Hansa increased 8 times the number after the shutdown of AlphaBay.<sup>72</sup> As remarked by Europol, the seizure and takedowns of dark-markets only force criminals to migrate to new trading platform. Unsurprisingly, payments were made in bitcoin.<sup>73</sup>

---

<sup>66</sup> *ibid.*

<sup>67</sup> Europol, 'Massive Blow to Criminal Dark Web Activities after Globally Coordinated Operation' (2017) <<https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation>> accessed 5 June 2018.

<sup>68</sup> *ibid.*

<sup>69</sup> *ibid.*

<sup>70</sup> *ibid.*

<sup>71</sup> *ibid.*

<sup>72</sup> *ibid.*

<sup>73</sup> *ibid.*

### 3. Case of Carbanak/Cobalt

Carbanak and Cobalt criminal operation attacked financial institutions in more than 40 countries.<sup>74</sup> The mastermind behind this criminal act was arrested in 2018 only after an arduous investigation carried out by the Spanish, Moldovan, Romanian, Belarusian and Taiwanese authorities, the FBI, with the support of private cybersecurity companies and Europol.<sup>75</sup> The cybercriminals had targeted numerous banks, e-payments systems since 2013 through the Carbanak and Cobalt malware.<sup>76</sup> They succeeded in stealing over 1 billion euros from the financial world.<sup>77</sup> It had a significant impact in the financial industry as the malware allowed criminals to scoop up to 10 million euros per heist.<sup>78</sup> This high-tech criminal operation initially started with Anunak malware which was later developed into the more sophisticated malware, Carbanak and Cobalt.<sup>79</sup> The same mode of operation was used for all three.<sup>80</sup> At first, the criminals would send financial institutions' employees emails with a malicious attachment copying legitimate companies and once the phishing attachment was downloaded, the cybercriminals could remotely control the infected computers.<sup>81</sup> They ultimately had access to the intranet of these instructions and infecting their servers.<sup>82</sup> This allowed them to acquire they needed to cash out money. They had different three ways of cashing out the money.<sup>83</sup>

Firstly, they would remotely instruct ATMs to dish out cash at a specific time and actors of the organized crime would collect them who happen to be there at the time payment was due.<sup>84</sup> Secondly, criminals would control the internal network of the bank to transfer money to their personal bank accounts.<sup>85</sup> Thirdly, they would modify account

---

<sup>74</sup> Europol, 'Mastermind behind Eur 1 Billion Cyber Bank Robbery Arrested in Spain'(2018) <<https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain>> accessed 5 June 2018.

<sup>75</sup> *ibid.*

<sup>76</sup> *ibid.*

<sup>77</sup> *ibid.*

<sup>78</sup> *ibid.*

<sup>79</sup> *ibid.*

<sup>80</sup> *ibid.*

<sup>81</sup> *ibid.*

<sup>82</sup> *ibid.*

<sup>83</sup> *ibid.*

<sup>84</sup> *ibid.*

<sup>85</sup> *ibid.*

information to inflate other bank accounts, with the money being collected by money mules at the Bank.<sup>86</sup>

Unsurprisingly, the cashed out money and profits from criminal proceeds were then laundered through bitcoin and other cryptocurrencies via the means of prepaid cards which were linked to their cryptocurrency wallets.<sup>87</sup>

## **Chapter 1: Introduction on Bitcoin and Blockchain**

In order to elucidate on the ways bitcoin acts as a facilitator to launder proceeds of criminal activities, it is essential to understand the mechanism of the bitcoin ecosystem. This chapter endeavours to explicate on the indispensable technology of the blockchain, the backbone of bitcoin. It proceeds on explaining the *modus operandi* used by bitcoin money launderers, i.e the cash-out strategy enabled by bitcoin exchanges and bitcoin mixing.

### **1.1 Bitcoin and Blockchain**

Nakamoto designed the blockchain software which operates as a decentralised bank for bitcoin.<sup>88</sup> Bitcoins are therefore traded and transacted between addresses of bitcoin users without passing through a centralised institution such as a bank.<sup>89</sup> Instead, the blockchain acts as a ledger openly verifiable and publicly visible.<sup>90</sup> The blockchain logs every input and output transactions effectuated by bitcoin users, which can be supervised through open source websites, such as blockchain.info.<sup>91</sup> The fact that it is an open source technology running on the World Wide Web means that transactions can be made and seen by any one, transcending jurisdictions and geographical borders.<sup>92</sup> Therefore, the current balance of a bitcoin user is also publicly visible on the blockchain, which is linked to the bitcoin address of the user.<sup>93</sup> In a

---

<sup>86</sup> *ibid.*

<sup>87</sup> *ibid.*

<sup>88</sup> Satoshi Nakamoto, 'Bitcoin: A peer-to-peer electronic cash system' [2009] <<https://bitcoin.org/bitcoin.pdf>> accessed 1 April 2018.

<sup>89</sup> *ibid.*

<sup>90</sup> *ibid.*

<sup>91</sup> *ibid.*

<sup>92</sup> *ibid.*

<sup>93</sup> *ibid.*

nutshell, this system helps the bitcoin cryptocurrency to be transacted anonymously or as argued by other enthusiasts pseudonymously without encountering the issue of double spending.<sup>94</sup> Arguably, the most favoured feature of criminal enthusiasts is the possibility of transacting anonymously.<sup>95</sup> In contrast to conventional banking system, the bitcoin does not require user's bitcoin address to be registered to individuals, thereby keeping high degree of anonymity.<sup>96</sup> In contrast to the system of numbered bank accounts in Switzerland which require the client to physically open the bank account with a set amount of funds, bitcoin users can simply open an account once they have downloaded the blockchain software on their devices and their electronic address acts as their unique identifier whilst all their login details are kept in their wallet, which is only accessible by them.<sup>97</sup> Additionally, the bitcoin system allows for instantaneous creation of bitcoin accounts which contrary to banks accounts are time consuming to set-up in thanks to the mandatory requirement of registering personal details of the client before opening an account.<sup>98</sup> To recapitulate, bitcoin offers an anonymous, free, decentralised and quick system to transact and trade. These features might be the reason why launderers and criminal enthusiasts see bitcoin as being the perfect cryptocurrency to conduct their criminal proceeds.<sup>99</sup> The blockchain technology has some features that make the system attractive for illegal activities and the other features powered by it, from a criminal perspective, are seen as stumbling blocks.<sup>100</sup> The reason is simple: the fact that all transactions are published on the decentralised public ledger and all bitcoin can be traced back means that actors of illicit activities are not completely safe of being caught by law enforcement agencies.<sup>101</sup> Hence, cashing out the illicit proceeds using cryptocurrency is not without complications.

## **1.2 Bitcoin and Money Laundering**

---

<sup>94</sup> *ibid.*

<sup>95</sup> Rolf van Wegberg, Jan-Jaap Oerlemans, Oskar van Deventer, 'Bitcoin Money Laundering: Mixed Results? An Explorative Study on Money Laundering of Cybercrime Proceeds using Bitcoin' (2008) 25(2) *Journal of Financial Crime*.

<sup>96</sup> *ibid.*

<sup>97</sup> Satoshi Nakamoto, 'Bitcoin: A peer-to-peer electronic cash system' [2008] <<https://bitcoin.org/bitcoin.pdf>> accessed 1 April 2018.

<sup>98</sup> Tara Mandjee, 'Bitcoin, its Legal Classification and its Regulatory Framework' (2015) 15(2) *Journal of Business & Securities Law*.

<sup>99</sup> Yaya J Fanusie and Tom Robinson, 'Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services' (2018) <<https://info.elliptic.co/whitepaper-fdd-bitcoin-laundering>> accessed on 19 May 2018.

<sup>100</sup> Rolf van Wegberg, Jan-Jaap Oerlemans, Oskar van Deventer, 'Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin' (2008) 25(2) *Journal of Financial Crime*.

<sup>101</sup> *ibid.*



Money laundering has always been in existence and is the process by which profits from illicit activities are converted into money or assets, as though they were initially derived from legitimate proceeds.<sup>102</sup> The only difference is that the mode of money-laundering operation keeps on changing as business models keep on evolving.<sup>103</sup> Criminals are always on the lookout for the possibility of laundering their illicit proceeds to be put to use; otherwise conducting illegal activities to make a profit would be useless if the dirty money cannot be spent.<sup>104</sup> In the mind of a launderer, it is crucial to design a well thought-out cash-out strategy in order to steer clear of potential criminal prosecutions.<sup>105</sup> This thesis presents an alternative method of laundering money through cryptocurrency in contrast to conventional means of money laundering which were facilitated by offshore accounts or money mules or even, alternative payment means through Perfect Money or Western Union, also renowned as effective ways of getting away with converting laundered money.<sup>106</sup> However, with strong anti-money laundering regulations worldwide, it has become increasingly difficult to conduct money laundering without running the high risk of getting caught. As reported by Europol, criminals are more and more using cashing-out cryptocurrency for their grand schemes of laundering money but also, using bitcoins to conduct their criminal activities.<sup>107</sup> Europol has also concluded in its digital crime proceed analysis that bitcoin is the preferred form of payment as “it accounts for more than 40% of all identified criminal-to-criminal payments”.<sup>108</sup> All of this is further facilitated by underground markets on the Darknet.<sup>109</sup> These undergrounds markets use the Tor-protocol which encrypts the network between users and so, it allows users to use the internet without showing the originating IP address of their computer as only the previous

---

<sup>102</sup> Jeffrey Simser, "Money laundering: emerging threats and trends" [2012] 16 *Journal of Money Laundering Control*.

<sup>103</sup> Yaya J Fanusie and Tom Robinson, 'Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services' (2018) <<https://info.elliptic.co/whitepaper-fdd-bitcoin-laundering>> accessed on 19 May 2018.

<sup>104</sup> Rolf van Wegberg, Jan-Jaap Oerlemans, Oskar van Deventer, 'Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin' (2008) 25(2) *Journal of Financial Crime*.

<sup>105</sup> Michael Levi, 'Money for crime and money from crime: financing crime and laundering crime proceeds', (2015) 21(2) *European Journal on Criminal Policy and Research*.

<sup>106</sup> *ibid*.

<sup>107</sup> Europol, 'Exploring tomorrow's organised crime' (2015) <[www.europol.europa.eu/sites/default/files/Europol\\_OrgCrimeReport\\_web-final.pdf](http://www.europol.europa.eu/sites/default/files/Europol_OrgCrimeReport_web-final.pdf)> accessed 5 June 2018.

<sup>108</sup> Europol, 'The internet organised crime threat assessment' (2015) <[www.europol.europa.eu/sites/default/files/publications/europol\\_iocta\\_web\\_2015.pdf](http://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web_2015.pdf)> accessed 5 June 2018.

<sup>109</sup> Roger Dingledine, Nick Mathewson and Paul Syverson, 'Tor: the second-generation onion router' () 13 *Proceedings of the 13th Conference on USENIX Security Symposium* <<https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf>> accessed on 5 June 2018.

node in the chain is visible on a connecting computer.<sup>110</sup> Coupling this possibility with the features of the bitcoin, cybercriminals have been able to counteract the ‘stumbling blocks’ they earlier found and hence, more and more illicit activities have been shifted underground.<sup>111</sup> Unsurprisingly, Holt<sup>112</sup> and Smirnova<sup>113</sup> reported that all kinds of new business set-ups have emerged on the Darknet giving rise to an online underground economy which had been already indicated by Eeten<sup>114</sup> and Bauer<sup>115</sup> back in 2008. It finally became a platform for the creation and trade of criminal techniques and services enabling money laundering. As observed by More and Rid, their quantitative research demonstrated that more than 50% activities occurring on the Darknet are illegal.<sup>116</sup> As Moser has discussed in his paper, users of Darknet uses the platform to offer specialised services such as bitcoin exchange and bitcoin mixing as ways to launder proceeds obtained through cybercrimes.<sup>117</sup> Europol has also noted that users with advanced IT skills advertised their services on the Darknet in return for their payments in cryptocurrencies.<sup>118</sup> As explained above, all bitcoin transactions are published on the blockchain, i.e the blockchain records all inputs and outputs and also, holds the cryptographic information (bitcoin address of the user) of each transaction.<sup>119</sup> In other words, all inputs are automatically the outputs of a previous transaction; this is how bitcoins can be traced back to a previous transaction.<sup>120</sup> This is detrimental for criminals and so, in order to evade law enforcers or financial intelligence agencies which can link back those transactions associated with illegal

---

<sup>110</sup> Rolf van Wegberg, Jan-Jaap Oerlemans, Oskar van Deventer, ‘Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin’ (2008) 25(2) *Journal of Financial Crime*.

<sup>111</sup> *ibid.*

<sup>112</sup> Thomas J Holt, ‘Exploring the social organisation and structure of stolen data markets’ (2013) 14 (2) *Global Crime* < <https://www.tandfonline.com/doi/abs/10.1080/17440572.2013.787925>> accessed 5 June 2018.

<sup>113</sup> Thomas J Holt and Olga Smirnova, ‘Examining the Structure, Organization, and Processes of the International Market for Stolen Data Report’ (2014) US Department of Justice < <https://www.ncjrs.gov/pdffiles1/nij/grants/245375.pdf>> accessed 5 June 2018.

<sup>114</sup> Michel Van Eeten and Johannes Bauer, ‘Economics of malware: security decisions, incentives and externalities’ (2008) OECD Science, Technology and Industry Working Papers.

<sup>116</sup> Daniel Moore and Thomas Rid, ‘Cryptopolitik and the Darknet: Survival’ [2016] 58 < <https://www.tandfonline.com/doi/abs/10.1080/00396338.2016.1142085>> accessed 6 June 2018.

<sup>117</sup> Malte Möser, Rainer Böhme and Dominic Breuker, ‘An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem’ (2013) eCrime Researchers Summit (IEEE, 2013) < <https://maltemoeser.de/paper/money-laundering.pdf>> accessed 5 June 2018.

<sup>118</sup> Europol, ‘The Internet Organised Crime Threat Assessment’ (2015) <[www.europol.europa.eu/sites/default/files/publications/europol\\_iocta\\_web\\_2015.pdf](http://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web_2015.pdf).> accessed 5 June 2018.

<sup>119</sup> Satoshi Nakamoto, ‘Bitcoin: A peer-to-peer electronic cash system’ [2009] 2012 <<https://bitcoin.org/bitcoin.pdf>> accessed 5 June 2018.

<sup>120</sup> *ibid.*

activities, cybercriminals use two strategies that can break the transnational link of the money trail of bitcoins: bitcoin mixing and bitcoin exchange or combining both techniques.<sup>121</sup>

### **1.3 Bitcoin Exchange and Bitcoin Mixing Services.**

Wegberg, Oerlemans and Deventer collected and analysed data on the services offered on the Darknet through the crawling technique which provided a robust explorative research on over 25,000 hidden services on Tor for both bitcoin exchange and bitcoin mixing services.<sup>122</sup> They submitted that bitcoin mixes differentiate from bitcoin exchanges in service percentage, time delays and authentication process.<sup>123</sup> Customers using bitcoin exchanges services are able to use Western Union or Paypal or Perfect Money to retrieve their money.<sup>124</sup> The exchange service converts their bitcoins into fiat currency which are received anonymously by using these payment services.<sup>125</sup> The mixing services operate by providing their customers with a newly generated bitcoin address where they are required to make a deposit of the bitcoins they want to launder.<sup>126</sup> The service provider then uses its bitcoin reserves to remit the mixed bitcoins to the address provided by the customer, after deducting a mixing fee.<sup>127</sup> Subsequently, using a bitcoin mixer service together with an unregulated bitcoin exchange service makes it the perfect strategy for criminals to launder their proceeds into legitimate money without the worry of being traced back to its illegitimate origin.<sup>128</sup> That being the case, the paper endeavours to shed light on the two different methods of bitcoin exchange and bitcoin mixing in their contribution to the cash-out strategy used by criminals, in chapters 2 and 3 respectively.

## **Chapter 2: Bitcoin laundering**

### **Bitcoin Mixes**

---

<sup>121</sup> Rolf van Wegberg, Jan-Jaap Oerlemans, Oskar van Deventer, 'Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin' (2008) 25(2) Journal of Financial Crime.

<sup>122</sup> *ibid.*

<sup>123</sup> *ibid.*

<sup>124</sup> *ibid.*

<sup>125</sup> *ibid.*

<sup>126</sup> *ibid.*

<sup>127</sup> *ibid.*

<sup>128</sup> *ibid.*

Albeit the market for Bitcoin has garnered much regulatory attention from financial and legal sectors, services such as bitcoin mixes are also used as a means of laundering money could still be seen to be running openly, especially on Darknet markets. This suggests that bitcoin mixes services are facilitating money laundering without raising the suspicion of concerned authorities and also, the reluctance of firms offering due diligence services to give straightforward negative feedback on tainted cryptocurrencies are not helping to mitigate risks of money laundering, as will be further explained below.

## **2.1 The Process of Mixing Bitcoin**

The system of mixes, also known as remailers, was invented by Chaum in 1982 which cryptocurrency enthusiasts have been reworking on improving in the context of bitcoin mixes.<sup>129</sup> In a non-technical definition, remailer is the method of sending and receiving emails by anonymising completely the analysis of message traffic to and fro.<sup>130</sup> It is found that if A wants to send B an email anonymously, A could send it to C first, to then ask him to send it to B. Nobody would know that the email received by B was actually a message from A. In this case, Chaum established the means to obfuscate message traffic is to culminate and mix up a number of encrypted messages before sending them to the destined receiver.<sup>131</sup> So, when A sends the email to C but doesn't want him to read it, he has the option of encrypting the message first with B's public key.<sup>132</sup> If A wants to have complete anonymity also from his Internet Service Provider (ISP/ police wiretap) then he could further encrypt the encrypted message that was sent to B to C with the latter's public key, so the ISP would only see an email to C. This is a simple but effective way of covering one's track from police wiretap.<sup>133</sup> The advent of the Tor system as explained in Chapter 1 means that a more complex and secured anonymous platform is now within the reach of criminal enthusiasts.

Similarly, this is how cryptocurrency mixes such as 'tumblebit' work and has been on the rise ever since the emergence of bitcoin.<sup>134</sup> There are other more complex cryptocurrency such as the Zcash which uses the Aladdin's laundry which allows customers to 're-mine' their coins to

---

<sup>129</sup> Ross Anderson, Ilia Shumailov, Mansoor Ahmed and Alessandro Rietmann, 'Bitcoin Redux' (2018) WEIS < [https://weis2018.econinfosec.org/wp-content/uploads/sites/5/2018/05/WEIS\\_2018\\_paper\\_38.pdf](https://weis2018.econinfosec.org/wp-content/uploads/sites/5/2018/05/WEIS_2018_paper_38.pdf)> accessed 1 June 2018.

<sup>130</sup> *ibid.*

<sup>131</sup> *ibid.*

<sup>132</sup> *ibid.*

<sup>133</sup> *ibid.*

<sup>134</sup> *ibid.*

come out with indistinguishable ones from other freshly mined coins.<sup>135</sup> Researchers such as Moser observed that some bitcoin mixes are in fact just a single wallet retaining all bitcoins and other services use tricks such as ‘ring signatures’ as a scheme to launder bitcoins.<sup>136</sup> It can all be boiled down to a simple explanation, i.e, if one user puts one green coin in a bag along with nine black ones and shake the bag hard enough, the outcome will be ten black coins. In the case of bitcoin, as put by Fox, the blockchain ledger administers all transactions publicly and hence, in order to acquire good title, one need to acquire his bitcoins in good faith or else the blockchain would alarm subsequent users that something is wrong.<sup>137</sup> This chapter of the thesis expounds on how this system is getting even more complex in reality, even though there is coin checking services available online which bitcoin exchanges claim to use, there is still no proper sharing of information in regards to the tracing of proceeds of crime on the blockchain. The issue of ‘information avoidance’ by many of these services means that they are not hundred per cent reliable as they seem to be on paper.<sup>138</sup>

### **Suggestions**

- 1) Perhaps there should be more in depth research in the profitability of criminal business models using this new money laundering technique. As was seen, laundering money through cryptocurrency is low, at least in theory. This could be the major plus point for cybercriminals to use this business model which is more profitable for them. Furthermore, this paper concluded that the cash-out strategy posed a challenging situation for law enforcement as the money trail completely becomes obfuscated.<sup>139</sup> Further research is needed to grasp the extent to which this strategy is widespread and also focus on the impact of such strategies both financially and legally.
  
- 2) Future research might also tackle the possibility of police measures if provided the appropriate means go gather evidence at cryptocurrency exchanges. This may lead to

---

<sup>135</sup> Malte Möser, Rainer Böhme and Dominic Breuker D, ‘An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem’ (2013) eCrime Researchers Summit (IEEE, 2013) < <https://maltemoeser.de/paper/money-laundering.pdf> > accessed 5 June 2018.

<sup>136</sup> *ibid.*

<sup>137</sup> David Fox, ‘Cyber-currencies in private law,’ (2016) University of Edinburgh.

<sup>138</sup> Russell Golman, David Hagmann, and George Loewenstein, ‘Information avoidance’ [2017] 55 Journal of Economic Literature.

<sup>139</sup> Rolf van Wegberg, Jan-Jaap Oerlemans, Oskar van Deventer, ‘Bitcoin Money Laundering: Mixed Results? An Explorative Study on Money Laundering of Cybercrime Proceeds using Bitcoin’ (2008) 25(2) Journal of Financial Crime.

the seizure of tainted wallets of the identified criminals to identify bitcoin addresses and use it as a means of tracing back bitcoin transfers.<sup>140</sup> Just as in the Hansa case whereby the Dutch police took over and down the whole underground website. Nonetheless, more research would enable the means and techniques to help and safeguard individual crime victims as well.

Finally, this paper calls for greater international cooperation from a legal perspective because as long as bitcoin will remain in a twilight zone, it will be very difficult to establish a good practice because of its decentralised nature. In other words, the fact in some countries, it is regulated and in other it is not, anti-money laundering rules and regulations such as KYC would not apply to all companies from different jurisdictions and hence, criminals will continue to use bitcoin as their preferred currency underground and launder money through bitcoin exchanges services which are located in jurisdictions which have more or less bitcoin or cryptocurrency regulations.

---

<sup>140</sup> *ibid.*

STUDY

Requested by the TAX3 committee



# Cryptocurrencies and blockchain

---

Legal context and implications for  
financial crime, money laundering  
and tax evasion



Policy Department for Economic, Scientific and Quality of Life Policies  
Authors: Prof. Dr. Robby HOUBEN, Alexander SNYERS  
Directorate-General for Internal Policies  
PE 619.024 - July 2018

EN





# Cryptocurrencies and blockchain

---

Legal context and implications for  
financial crime, money laundering  
and tax evasion

## **Abstract**

More and more regulators are worrying about criminals who are increasingly using cryptocurrencies for illegitimate activities like money laundering, terrorist financing and tax evasion. The problem is significant: even though the full scale of misuse of virtual currencies is unknown, its market value has been reported to exceed EUR 7 billion worldwide. This paper prepared by Policy Department A elaborates on this phenomenon from a legal perspective, focusing on the use of cryptocurrencies for financial crime, money laundering and tax evasion. It contains policy recommendations for future EU standards.

This document was requested by the European Parliament's Special Committee on Financial Crimes, Tax Evasion and Tax Avoidance.

### **AUTHORS**

Prof. Dr. Robby HOUBEN, University of Antwerp, Research Group Business & Law, Belgium.  
Alexander SNYERS, University of Antwerp, Research Group Business & Law, Belgium.

### **ADMINISTRATOR RESPONSIBLE**

Dirk VERBEKEN

### **EDITORIAL ASSISTANT**

Janetta CUJKOVA

### **LINGUISTIC VERSIONS**

Original: EN

### **ABOUT THE EDITOR**

Policy departments provide in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact the Policy Department or to subscribe for updates, please write to:

Policy Department for Economic, Scientific and Quality of Life Policies

European Parliament

B-1047 Brussels

Email: [Poldep-Economy-Science@ep.europa.eu](mailto:Poldep-Economy-Science@ep.europa.eu)

Manuscript completed in June 2018

© European Union, 2018

This document is available on the internet at:

<http://www.europarl.europa.eu/supporting-analyses>

### **DISCLAIMER AND COPYRIGHT**

The opinions expressed in this document are the sole responsibility of the authors and do not necessarily represent the official position of the European Parliament.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

© Cover image used under licence from Shutterstock.com

# CONTENTS

<b>LIST OF ABBREVIATIONS</b>	<b>6</b>
<b>LIST OF BOXES</b>	<b>8</b>
<b>LIST OF FIGURES</b>	<b>8</b>
<b>LIST OF TABLES</b>	<b>8</b>
<b>EXECUTIVE SUMMARY</b>	<b>9</b>
<b>1. GENERAL INFORMATION</b>	<b>11</b>
1.1. Background	11
1.2. Scope of the research	12
1.3. Overview of policy recommendations for future EU standards	14
<b>2. CRYPTOCURRENCIES AND BLOCKCHAIN</b>	<b>15</b>
2.1. What is blockchain?	15
2.1.1. Defining blockchain: a technology with many faces	15
2.1.2. How a blockchain works: the basics	16
2.1.3. The blockchain consensus mechanisms	18
2.1.4. Blockchain technology can have many applications	19
2.2. What are cryptocurrencies?	20
2.2.1. Introduction	20
2.2.2. The policy makers: ECB, IMF, BIS, EBA, ESMA, World Bank and FATF	20
2.2.3. Cryptocurrencies – Tokens – Cryptosecurities	23
2.2.4. Cryptocurrencies – Blockchain	24
2.3. Who are the players involved?	24
2.3.1. Cryptocurrency users	25
2.3.2. Miners	25
2.3.3. Cryptocurrency exchanges	26
2.3.4. Trading platforms	27
2.3.5. Wallet providers	27
2.3.6. Coin inventors	28
2.3.7. Coin offerors	28
<b>3. CLASSIFYING CRYPTOCURRENCIES</b>	<b>29</b>
3.1. Scoping the Crypto-Market	29
3.2. Bitcoin and beyond: the 10 cryptocurrencies with the highest market capitalisation	31
3.2.1. Bitcoin (BTC)	31
3.2.2. Ethereum (ETH)	33

3.2.3. Ripple (XRP)	35
3.2.4. Bitcoin Cash (BCH)	36
3.2.5. Litecoin (LTC)	37
3.2.6. Stellar (XLM)	39
3.2.7. Cardano (ADA)	40
3.2.8. IOTA (MIOTA)	42
3.2.9. NEO (NEO)	43
3.2.10. Monero (XMR)	45
3.2.11. Dash (DASH)	48
3.3. Conclusion: a taxonomy and timeline of cryptocurrencies	49
<b>4. EU REGULATORY FRAMEWORK</b>	<b>53</b>
4.1. Setting the scene: similar regulatory challenges in the fight against money laundering, terrorist financing and tax evasion via cryptocurrencies	53
4.1.1. Anonymity	53
4.1.2. Cross-border nature	54
4.1.3. Often no central intermediary	54
4.1.4. Cryptocurrencies are falling between the cracks	54
4.1.5. A difficult dividing line with cybersecurity, data protection and privacy	55
4.1.6. Don't throw the baby out with the bathwater: the technology	56
4.1.7. The tide is changing: AMLD5	57
4.2. Money laundering and terrorist financing	58
4.2.1. Background	58
4.2.2. AMLD4	59
4.2.3. Cryptocurrencies under AMLD4	62
4.2.4. The coming of age of the inclusion of cryptocurrencies into AMLD5	62
4.2.5. Funds Transfer Regulation	68
4.2.6. Cash Control Regulation	69
4.3. Tax evasion	70
<b>5. ADEQUACY OF THE REGULATORY FRAMEWORK</b>	<b>73</b>
5.1. Introduction	73
5.2. Is the definition of virtual currencies under AMLD5 sufficient?	73
5.2.1. Conclusions on the basis of the taxonomy	73
5.2.2. Other virtual currencies than cryptocurrencies	74
5.3. Is it enough to include only custodian wallet providers and virtual currency exchanges in the list of obliged entities?	76
5.3.1. State of play	76
5.3.2. Users	76

---

5.3.3. Miners	76
5.3.4. Cryptocurrency exchanges	77
5.3.5. Trading platforms	77
5.3.6. Wallet providers	78
5.3.7. Coin inventors	78
5.3.8. Offerors	78
5.3.9. The initial question	79
5.4. Does the AMLD5 framework allow to pull enough cryptocurrency users into the light?	79
5.5. Would it make sense to extend the scope of the Funds Transfer Regulation and/or the Cash Control Regulation as to include cryptocurrency transactions?	81
5.6. Is there a need for a more comprehensive approach, introducing license requirements for cryptocurrencies?	81
5.7. Is it not best to introduce an outright ban for some aspects linked to some cryptocurrencies?	82
5.8. Is the European level the appropriate one to tackle money laundering, terrorist financing and tax evasion via cryptocurrency transactions?	83
<b>6. WHAT ABOUT BLOCKCHAIN?</b>	<b>85</b>
<b>REFERENCES</b>	<b>86</b>

## LIST OF ABBREVIATIONS

<b>AMLD1</b>	First Anti-Money Laundering Directive
<b>AMLD2</b>	Second Anti-Money Laundering Directive
<b>AMLD3</b>	Third Anti-Money Laundering Directive
<b>AMLD4</b>	Fourth Anti-Money Laundering Directive
<b>AMLD5</b>	Fifth Anti-Money Laundering Directive
<b>BIS</b>	Bank for International Settlements
<b>CPMI</b>	Committee on Payments and Market Infrastructures
<b>DACS</b>	Fifth revision of the Directive on administrative cooperation in taxation
<b>DLT</b>	Distributed ledger technology
<b>EBA</b>	European Banking Authority
<b>ECB</b>	European Central Bank
<b>EIOPA</b>	European Insurance and Occupational Pensions Authority
<b>ESMA</b>	European Securities and Markets Authority
<b>FATF</b>	Financial Action Task Force
<b>FIU</b>	Financial intelligence unit
<b>FTR</b>	Funds Transfer Regulation
<b>IMF</b>	International Monetary Fund
<b>ITO</b>	Initial Token Offering
<b>MTF</b>	Multilateral trading facility
<b>OTF</b>	Organised trading facility
<b>P2P</b>	Peer to Peer
<b>PoS</b>	Proof of Stake

**PoW** Proof of Work

**PSD2** Second revision of the Directive on Payment Services

## LIST OF BOXES

Box 1:	The Kovri-project	48
Box 2:	The PrivateSend mixing-process explained	49
Box 3:	Some thoughts on the TITANIUM project	54

## LIST OF FIGURES

Figure 1:	How a blockchain works	17
Figure 2:	Coin timeline	52

## LIST OF TABLES

Table 1:	Overview of coins	30
Table 2:	Coin taxonomy	51



## EXECUTIVE SUMMARY

More and more regulators are worrying about criminals who are increasingly using cryptocurrencies for illegitimate activities like money laundering, terrorist financing and tax evasion. The problem is significant: even though the full scale of misuse of virtual currencies is unknown, its market value has been reported to exceed EUR 7 billion worldwide.<sup>1</sup> This research elaborates on this phenomenon, focusing on the use of cryptocurrencies for financial crime, money laundering and tax evasion.

The key issue that needs to be addressed is the anonymity surrounding cryptocurrencies. This anonymity, varying from complete anonymity to pseudo-anonymity, prevents cryptocurrency transactions from being adequately monitored, allowing shady transactions to occur outside of the regulatory perimeter and criminal organisations to use cryptocurrencies to obtain easy access to "clean cash". Anonymity is also the major issue when it comes to tax evasion. When a tax authority does not know who enters into the taxable transaction, because of the anonymity involved, it cannot detect nor sanction this tax evasion.

The existing European legal framework is failing to deal with this issue. There are simply no rules unveiling the anonymity associated with cryptocurrencies. However, the tide is changing. The fifth revision of the directive on money laundering and terrorist financing, AMLD5, is in the final phase of being adopted. AMLD5 includes a definition of virtual currencies and subjects virtual currency exchange services and custodian wallet providers to customer due diligence requirements and the duty to report suspicious transactions to financial intelligence units. The information obtained, can also be used by tax authorities to combat tax evasion.

AMLD5's definition of virtual currencies is sufficient to combat money laundering, terrorist financing and tax evasion via cryptocurrencies. Nevertheless, it is important to closely follow-up on the use cases of virtual currencies to ascertain that the definition remains to be a sufficient one going forward.

When we look at the key players in cryptocurrency markets, we can see that a number of those are not included in AMLD5, leaving blind spots in the fight against money laundering, terrorist financing and tax evasion. The examples are numerous and include miners, pure cryptocurrency exchanges that are not also custodian wallet providers, hardware and software wallet providers, trading platforms and coin offerors. Persons with malicious intent could look up these blind spots. If that would happen and it would appear to have a (material) adverse effect on the fight against money laundering, terrorist financing and tax evasion, expanding the scope of AMLD5 should be considered.

With respect to unveiling the anonymity of users in general (i.e. also outside of the context of virtual currency exchanges and custodian wallet providers), no immediate action is taken. Only in its next supranational risk assessment, the Commission will assess a system of voluntary registration of users. This approach is not very convincing if the legislator is truly serious about unveiling the anonymity of cryptocurrency users to make the combat against money laundering, terrorist financing and tax evasion more effective. A mandatory registration and a pre-set date as of which it applies, would be a better approach, albeit of course more intrusive. For reasons of proportionality, mandatory registration could be made subject to a materiality threshold.

---

<sup>1</sup> COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document "Proposal for a Directive of the European Parliament and the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC", SWD/2016/0223 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0223&from=EN>.

For some aspects relating to some cryptocurrencies a ban should be considered. To mind come the features that are designed to make cryptocurrency users untraceable. Why is such degree of anonymity truly necessary? Would allowing this not veer too far towards criminals? In any event, imposing a ban should always be focused on specific aspects facilitating the illicit use of cryptocurrency too much.

The European level is appropriate to address money laundering, terrorist financing and tax evasion via cryptocurrencies. Even more appropriate is the international level, as crypto activity is not limited by the European border. International collaboration is crucial to successfully impose and enforce rules on combating money laundering, terrorist financing and tax evasion. From a regulatory perspective, the ongoing G20 attention paid to regulating cryptocurrencies is therefore welcome.

As regards blockchain, it would be too blunt to associate blockchain with money laundering, terrorist financing or tax evasion. It is just technology, on which a large number of cryptocurrencies run, but which is not designed to launder money, facilitate terrorist financing or evade taxes. Blockchain has numerous applications throughout the whole lawful economy. It would not be wise to discourage future innovations in this respect by submitting blockchain and fintech's exploring its use cases to burdensome requirements, simply because of one of the applications using blockchain technology, cryptocurrencies, is used illicitly by some. Therefore, blockchain should be left untouched from a money laundering, terrorist financing and tax evasion perspective. The fight against money laundering, terrorist financing and tax evasion should focus on the illicit use cases of cryptocurrencies.

## 1. GENERAL INFORMATION

### KEY FINDINGS

- The key issue that needs to be addressed in the fight against money laundering, terrorist financing and tax evasion via cryptocurrencies is the anonymity surrounding cryptocurrencies.
- The existing European legal framework is failing to deal with this issue.
- The tide is changing: the fifth revision of the directive on money laundering and terrorist financing, AMLD5 includes a definition of virtual currencies and subjects virtual currency exchange services and custodian wallet providers to customer due diligence requirements and the duty to report suspicious transactions to financial intelligence units.
- A number of key players in cryptocurrency markets are not included in the scope of AMLD5, leaving blind spots in the fight against money laundering, terrorist financing and tax evasion.
- With respect to unveiling the anonymity of users in general, no immediate action is taken. The Commission will assess only in its next supranational risk assessment a system of voluntary registration of users. A mandatory registration and a pre-set date as of which it applies would be a better approach to unveil the anonymity of cryptocurrency users.
- For some aspects relating to some cryptocurrencies a ban should be considered.
- The European level is appropriate to address money laundering, terrorist financing and tax evasion via cryptocurrencies, but even more more appropriate is the international level, as crypto activity is not limited by the European border.
- Blockchain is technology, on which a large number of cryptocurrencies run, but which is not designed to launder money, facilitate terrorist financing or evade taxes. Blockchain has numerous applications throughout the whole lawful economy. The fight against money laundering, terrorist financing and tax evasion should focus on the illicit use cases of cryptocurrencies and not on blockchain.

### 1.1. Background

With the growing popularity of the crypto market, the large number of unregulated cryptocurrencies (several hundreds), greater attention is now being paid by governments and other stakeholders around the world. Illustrative is that the total market capitalisation of the 100 largest cryptocurrencies is reported to exceed the equivalent of EUR 330 billion globally by early 2018. The total market capitalisation of all cryptocurrencies together in that period peaked at an even higher USD 728 billion, dropping just three weeks later to approximately USD 360 billion.<sup>2</sup> Regulators are looking at whether — and how — to regulate cryptocurrencies. Up till now there is no univocal view on how to do that. In any event, there are compelling reasons why cryptocurrencies should be under more

<sup>2</sup> R.M. BRATSPIES, "Cryptocurrencies and the Myth of the Trustless Transaction", March 2018, 6-7 (electronically available via <https://ssrn.com/abstract=3141605>).

scrutiny by regulators and supervisors. The threat of price volatility, speculative trading, hack attacks, money laundering and terrorist financing all call for stricter regulation.

This research deep dives into the latter issue. According to many, aside from the instability of cryptocurrency prices, these cryptocurrencies must have greater regulatory oversight in order to prevent illegal activity and illegitimate use. Aside from the instability of cryptocurrency prices, regulators are worrying about criminals who are increasingly using cryptocurrencies for activities (trading away from official channels) like fraud and manipulation, tax evasion, hacking, money laundering and funding for terrorist activities. The problem is a significant one: even though the full scale of misuse of virtual currencies is unknown, its market value has been reported to exceed EUR 7 billion worldwide.<sup>3</sup>

## 1.2. Scope of the research

Cryptocurrencies and blockchain are a monstrous topic. There are several hundreds of cryptocurrencies and the applications of blockchain technology are also numerous. To make this research a useful and focused one, we have to narrow it down. To do this, the research attaches to multiple connecting factors, defining its scope.

Firstly, the research is limited to *cryptocurrencies and blockchain*. This means that other types of assets than cryptocurrencies, such as tokens or crypto securities, are not within the scope of this research. We will explain how these assets differ from cryptocurrencies further on. We will also not elaborate on derivatives of cryptocurrencies, which are essentially investment instruments. Blockchain will be scrutinized to the extent cryptocurrencies run on this technology. Therefore, blockchain technology will not be looked at outside of the context of cryptocurrencies, such as it being used as a technique to eliminate intermediaries in the financial, public or other sector. This would lead to far and exceeds the scope of this research.

Secondly, the research relates to the *legal context* of cryptocurrencies and blockchain. The focus is, hence, a legal one. This means that we will not elaborate on all the technical aspects – and there are many – relating to cryptocurrencies and blockchain. We will only touch upon those to the extent necessary to understand the legal context. We will also not take an economic, criminological or any other approach than a legal one. We focus on the *EU legal context*. Therefore, we will not elaborate on the international<sup>4</sup> or national context, unless it is relevant to better understand the European context.

Thirdly, the legal context is addressed *in connection with the implications for financial crime, money laundering and tax evasion*. Therefore, we will only scrutinize the legal context of cryptocurrencies and blockchain to the extent relevant in connection with financial crime, money laundering and tax evasion. We will do this by assessing what exactly cryptocurrencies and blockchain are, which challenges they bring from the perspective of combating financial crime, money laundering and tax evasion, to which extent they are caught by legislation at European level and what could be done to improve the legal framework. We will not deep dive into other legal queries than those related to

<sup>3</sup> COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document “Proposal for a Directive of the European Parliament and the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC”, SWD/2016/0223 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0223&from=EN>.

<sup>4</sup> See for a number of examples on non-EU measures on cryptocurrencies: T. KEATINGE, D. CARLISLE and F. KEEN, “Virtual currencies and terrorist financing: assessing the risks and evaluating responses”, study commissioned by the Directorate General for Internal Policies, Policy Department for Citizens’ Rights and Constitutional Affairs, May 2018, 47-50 (electronically available via [http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL\\_STU\(2018\)604970\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf)). See also: P. VALENTE, “Bitcoin and Virtual Currencies Are Real: Are Regulators Still Virtual?”, INTERTAX, Volume 46, Issue 6 & 7, 546-547.

money laundering, terrorist financing and tax evasion, such as the qualification of cryptocurrencies under tax laws or the protection of investors in cryptocurrencies (whether or not consumers) under financial services laws.<sup>5</sup> Although very interesting, these queries exceed the scope of this research.

Lastly, the research relates to *financial crime, money laundering and tax evasion*. Financial crime is no term of art. Generally speaking, it is used as an umbrella term to designate all sorts of crimes relating to the use of finances, such as fraud, theft, tax evasion, bribery, money laundering, terrorist financing, etc.. In an EU context, financial crime includes *inter alia* crimes against the integrity of the financial sector, such as money laundering and insider dealing, and crimes against the financial interest of the Union, such as fraud. In this research we will not elaborate on all imaginable financial crimes. On the contrary, we will focus on money laundering, terrorist financing and tax evasion as subtypes of financial crime. This focus can be justified for a number of reasons. Firstly, money laundering, terrorist financing and tax evasion are at the forefront of the EU's efforts on combating financial crime.<sup>6</sup> Furthermore, the EU is clearly taking the approach to address cryptocurrency issues via anti-money laundering and counter terrorism financing legislation. This research acknowledges that approach and takes the same one. Secondly, leaving theft aside, money laundering, terrorist financing and tax evasion are probably the three types of financial crimes that are likely to be most associated with cryptocurrencies and blockchain, *i.e.* when persons commit a crime relating to cryptocurrencies and blockchain, the likelihood of that crime being money laundering, terrorist financing and/or tax evasion is high. Cryptocurrencies are thought to be very suitable for money laundering, terrorist financing and tax evasion purposes because of their anonymity, cross-borders nature and quick transferability<sup>7</sup>. Thirdly, some crimes simply cannot be committed at this stage via cryptocurrencies. Financial crimes such as market abuse and insider dealing are for instance of no relevance for cryptocurrencies. Market abuse rules relate to financial instruments traded on a regulated market, a multilateral trading facility ("**MTF**") or an organised trading facility ("**OTF**"). For the application to cryptocurrencies this poses two problems: cryptocurrencies are not financial instruments and they are not traded on a regulated market, MTF or OTF.

The research starts with a definition of cryptocurrencies and blockchain. After that, a taxonomy of cryptocurrencies will be given on the basis of an analysis of the 10 cryptocurrencies with the highest market capitalisation. This taxonomy will serve as a benchmark throughout this research and will allow to verify the adequacy of the existing and upcoming legal framework.

This study has been completed on 20 June 2018.

---

<sup>5</sup> Another interesting query, which we will also not deep dive into in the context of this study, is how cryptocurrencies affect monetary policy. For more information on this topic we refer to: D. HELLER, "The implications of digital currencies for monetary policy", in-depth analysis commissioned by the Directorate General for Internal Policies, Policy Department A: Economic and Scientific Policy, May 2017, 12p. (electronically available via [http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/602048/IPOL\\_IDA\(2017\)602048\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/602048/IPOL_IDA(2017)602048_EN.pdf)).

<sup>6</sup> See e.g. E. HERLIN-KARNELL and N. RYDER, "The robustness of EU Financial Crimes Legislation: A Critical review of the EU and UK Anti-Fraud and Money Laundering Scheme", 2017, *European Business Law Review*, No. 4, 1-39.

<sup>7</sup> See e.g. S. ROYER, "Bitcoins in het Belgische strafrecht en strafprocesrecht", *RW* 2016-17, No. 13, 486.

### 1.3. Overview of policy recommendations for future EU standards

This study sets out a number of policy recommendations for future EU standards. The main ones are outlined below.

#### Policy recommendations for future EU standards

- To unveil the anonymity of cryptocurrency users the EU should consider a system of mandatory registration of users and a pre-set date as of which it applies rather than a system of voluntary registration of users.
- The EU should also think about expanding the list of “obliged entities” under AMLD5 with those players that are identified in this study as the weak spots or have great potential of being weak spots, including miners, pure cryptocurrency exchanges that are not also custodian wallet providers, software and hardware wallet providers, trading platforms and coin offerors.
- Furthermore, the EU should think about imposing a specific ban on such aspects surrounding cryptocurrencies that are aimed at making it impossible to verify their users (e.g. mixing) and criminally sanctioning these aspects.
- In addition, the EU could consider extending the scope of the Funds Transfer Regulation to make sure that all relevant information accompanying cryptocurrency transactions is there, allowing an adequate money laundering and terrorist financing check. The entities that would have to fulfil the requirements could be the intermediaries through which the transactions run.
- In the longer term, the EU should consider developing a tailored and more comprehensive framework for cryptocurrencies, and setting EU standards for cryptocurrencies in line with suggestions and recommendations made by the EBA, including license requirements for cryptocurrency service providers. Part of such framework could be to create or impose a “middleman”, where the use of blockchain or other distributed ledger technology has cut out such middleman, as this will allow the regulator to attach regulation to an identifiable person, thus contributing to enhanced compliance and effective enforcement.
- With a view of achieving unified regulation of cryptocurrencies at G20 level, it is recommended that the EU leads further initiatives by example.
- The EU should leave blockchain be from a money laundering, terrorist financing and tax evasion perspective and focus on the illicit use cases of cryptocurrencies. Blockchain is just technology and can have beneficial effects in a wide array of sectors. Its development as such should not be discouraged.

## 2. CRYPTOCURRENCIES AND BLOCKCHAIN

### 2.1. What is blockchain?

#### 2.1.1. Defining blockchain: a technology with many faces

Blockchain is a particular type or subset of so-called distributed ledger technology (“**DLT**”).<sup>8</sup> DLT is a way of recording and sharing data across multiple data stores (also known as ledgers), which each have the exact same data records and are collectively maintained and controlled by a distributed network of computer servers, which are called nodes.<sup>9</sup>

Blockchain is a mechanism that employs an encryption method known as cryptography<sup>10</sup> and uses (a set of) specific mathematical algorithms to create and verify a continuously growing data structure – to which data can only be added and from which existing data cannot be removed – that takes the form of a chain of “transaction blocks”<sup>11</sup>, which functions as a distributed ledger.<sup>12</sup>

In practice, blockchain is a technology with many “faces”. It can exhibit different features and covers a wide array of systems that range from being fully open and permissionless, to permissioned<sup>13</sup>:

- On an *open, permissionless blockchain*, a person can join or leave the network at will, without having to be (pre-)approved by any (central) entity.<sup>14</sup> All that is needed to join the network and add transactions to the ledger is a computer on which the relevant software has been installed. There is no central owner of the network and software, and identical copies of the ledger are distributed to all the nodes in the network.<sup>15</sup> The vast majority of cryptocurrencies currently in circulation is based on permissionless blockchains (e.g. Bitcoin, Bitcoin Cash, Litecoin, ...).
- On a *permissioned blockchain*, transaction validators (i.e. nodes) have to be pre-selected by a network administrator (who sets the rules for the ledger) to be able to join the network.<sup>16</sup> This allows, amongst others, to easily verify the identity of the network participants.<sup>17</sup> However, at the same time it also requires network participants to put trust in a central coordinating entity to

<sup>8</sup> Another example of distributed ledger technology is “*directed acyclic graph*”, the underlying technology of the IOTA-platform (see below). See also: M. VAN DE LOOVERBOSCH, “Crypto-effecten: tussen droom en daad”, TRV-RPS 2018, 193, footnote 2.

<sup>9</sup> See: World Bank Group (H. NATARAJAN, S. KRAUSE, and H. GRADSTEIN), “Distributed Ledger Technology (DLT) and blockchain”, 2017, FinTech note, no. 1. Washington, D.C., <http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf>, 1. See also: CPMI, “Digital currencies”, November 2015, <https://www.bis.org/cpmi/publ/d137.pdf>, 5.

<sup>10</sup> This technique is discussed and defined further below.

<sup>11</sup> Hence the name “blockchain”.

<sup>12</sup> See: World Bank Group (H. NATARAJAN, S. KRAUSE and H. GRADSTEIN), “Distributed Ledger Technology (DLT) and blockchain”, 2017, FinTech note, no. 1. Washington, D.C., <http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf>, 1.

<sup>13</sup> Some authors also distinguish so-called “consortium blockchains”, which operate as closed, cryptographically secured databases (i.e. the ledger can only be accessed by the nodes that are participating in the network and different rules apply on who can update the state of the ledger). *Inter alia*: P. WITZIG and V. SALOMON, “Cutting out the middleman: a case study of blockchain-induced reconfigurations in the Swiss Financial Services Industry”, Working Paper 1, 2018/E, the Circulation of Wealth, Université de Neuchâtel, [http://www.unine.ch/files/live/sites/maps/files/shared/documents/wp/WP-1\\_2018\\_Witzig%20and%20Salomon.pdf](http://www.unine.ch/files/live/sites/maps/files/shared/documents/wp/WP-1_2018_Witzig%20and%20Salomon.pdf), 7.

<sup>14</sup> World Bank Group (H. NATARAJAN, S. KRAUSE and H. GRADSTEIN), “Distributed Ledger Technology (DLT) and blockchain”, 2017, FinTech note, no. 1. Washington, D.C., <http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf>, 1.

<sup>15</sup> *Ibid.*

<sup>16</sup> Permissioned blockchains are built so that “*they grant special permissions to each participant for specific functions to be performed—like read, access and write information on the blockchains*” (hence the name “permissioned” blockchains). See: S. SHOBHIT, “Public, Private, Permissioned Blockchains Compared”, April 2018, <https://www.investopedia.com/news/public-private-permissioned-blockchains-compared/>.

<sup>17</sup> World Bank Group (H. NATARAJAN, S. KRAUSE and H. GRADSTEIN), “Distributed Ledger Technology (DLT) and blockchain”, 2017, FinTech note, no. 1. Washington, D.C., <http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf>, 11.

select reliable network nodes.<sup>18</sup> In general, permissioned blockchains can be further divided into two subcategories. On the one hand, there are *open or public permissioned blockchains*, which can be accessed and viewed by anyone, but where only authorised network participants can generate transactions and/or update the state of the ledger.<sup>19</sup> On the other hand, there are *closed or “enterprise” permissioned blockchains*<sup>20</sup>, where access is restricted and where only the network administrator can generate transactions and update the state of the ledger.<sup>21</sup> What is important to note is that just like on an open permissionless blockchain, transactions on an open permissioned blockchain can be validated and executed without the intermediation of a trusted third-party. Some cryptocurrencies, like Ripple and NEO utilise public permissioned blockchains.<sup>22</sup>

### 2.1.2. How a blockchain works: the basics

#### a. The blockchain is a distributed database

In simple terms, the blockchain can be thought of as a distributed database. Additions to this database are initiated by one of the members (i.e. the network nodes), who creates a new “block” of data, which can contain all sorts of information. This new block is then broadcasted to every party in the network in an encrypted form (utilising cryptography) so that the transaction details are not made public.<sup>23</sup> Those in the network (i.e. the other network nodes) collectively determine the block’s validity in accordance with a pre-defined algorithmic validation method, commonly referred to as a “consensus mechanism”<sup>24</sup>. Once validated, the new “block” is added to the blockchain, which essentially results in an update of the transaction ledger that is distributed across the network.<sup>25</sup>

In principle, this mechanism can be used for any kind of value transaction and can be applied to any asset that can be represented in a digital form<sup>26</sup>. We illustrate this in Figure 1 below.

#### b. Transaction “blocks” are signed with a digital signature using a private key

Every user on a blockchain network has a set of two keys. A private key, which is used to create a digital signature for a transaction, and a public key, which is known to everyone on the network. A

<sup>18</sup> *Ibid.*

<sup>19</sup> P. WITZIG and V. SALOMON, “Cutting out the middleman: a case study of blockchain-induced reconfigurations in the Swiss Financial Services Industry”, Working Paper 1, 2018/E, the Circulation of Wealth, Université de Neuchâtel, [http://www.unine.ch/files/live/sites/maps/files/shared/documents/wp/WP-1\\_2018\\_Witzig%20and%20Salomon.pdf](http://www.unine.ch/files/live/sites/maps/files/shared/documents/wp/WP-1_2018_Witzig%20and%20Salomon.pdf), 6-7.

<sup>20</sup> These blockchains are sometimes also referred to as “private blockchains”. See *Inter alia*: P. JAYACHANDRAN, “The difference between public and private blockchain”, May 2017, <https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/>; S. ШОВИТ, “Public, Private, Permissioned Blockchains Compared”, April 2018, <https://www.investopedia.com/news/public-private-permissioned-blockchains-compared/>; P. WITZIG and V. SALOMON, “Cutting out the middleman: a case study of blockchain-induced reconfigurations in the Swiss Financial Services Industry”, Working Paper 1, 2018/E, the Circulation of Wealth, Université de Neuchâtel, [http://www.unine.ch/files/live/sites/maps/files/shared/documents/wp/WP-1\\_2018\\_Witzig%20and%20Salomon.pdf](http://www.unine.ch/files/live/sites/maps/files/shared/documents/wp/WP-1_2018_Witzig%20and%20Salomon.pdf), 7.

<sup>21</sup> P. WITZIG and V. SALOMON, “Cutting out the middleman: a case study of blockchain-induced reconfigurations in the Swiss Financial Services Industry”, Working Paper 1, 2018/E, the Circulation of Wealth, Université de Neuchâtel, [http://www.unine.ch/files/live/sites/maps/files/shared/documents/wp/WP-1\\_2018\\_Witzig%20and%20Salomon.pdf](http://www.unine.ch/files/live/sites/maps/files/shared/documents/wp/WP-1_2018_Witzig%20and%20Salomon.pdf), 6-7.

<sup>22</sup> Also see below under 3.2.9 NEO (NEO).

<sup>23</sup> World Bank Group (H. NATARAJAN, S. KRAUSE and H. GRADSTEIN), “Distributed Ledger Technology (DLT) and blockchain”, 2017, FinTech note, no. 1. Washington, D.C., <http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf>, 1.

<sup>24</sup> *Ibid.*, 1. Also see below 2.1.3. The blockchain consensus mechanisms.

<sup>25</sup> CPMI, “Digital currencies”, November 2015, <https://www.bis.org/cpmi/publ/d137.pdf>, 5.

<sup>26</sup> See: World Bank Group (H. NATARAJAN, S. KRAUSE and H. GRADSTEIN), “Distributed Ledger Technology (DLT) and blockchain”, 2017, FinTech note, no. 1. Washington, D.C., <http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf>, 1.

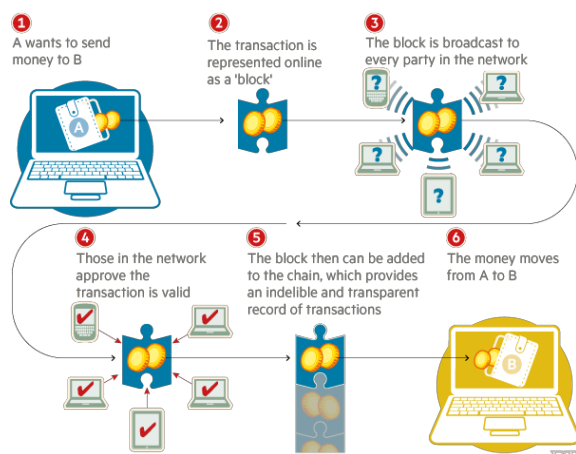


public key has two uses: 1) it serves as an address on the blockchain network; and 2) it is used to verify a digital signature / validate the identity of the sender.<sup>27</sup>

On the Bitcoin blockchain, this translates into the following example. Suppose that Anna wants to send 100 Bitcoins to Jeff, then first of all she will have to digitally sign this transaction using her private key (which is only known to her). She will have to address the transaction to Jeff's public key, which is Jeff's address on the Bitcoin network. Next, the transaction, which will be collated into a "transaction block", will have to be verified by the nodes within the Bitcoin network. Here, Anna's public key will be used to verify her signature. If Anna's signature is valid, the network will process the transaction, add the block to the chain and transfer 100 Bitcoins from Anna to Jeff.

A user's public and private keys are kept in a digital wallet or e-wallet. Such wallet can be stored or saved online (online storage is often referred to as "hot storage") and/or offline (offline storage is commonly referred to as "cold storage").<sup>28</sup>

Figure 1: How a blockchain works



Source: "Technology: Banks seeks the key to blockchain", by J. Wild, M. Arnold and P. Stafford, 1 November 2015, Financial Times, <https://www.ft.com/content/eb1f8256-7b4b-11e5-a1fe-567b37f80b64?seqid=0100320#axzz3qK4rCVQP>.

### c. Bye-bye middleman?

One of the key advantages of blockchain technology is that it allows to simplify the execution of a wide array of transactions that would normally require the intermediation of a third party (e.g. a custodian, a bank, a securities settlement system, broker-dealers, a trade repository, ...). In essence, blockchain is all about decentralizing trust and enabling decentralized authentication of transactions.<sup>29</sup> Simply put, it allows to cut out the "middleman".<sup>30</sup>

In many cases this will likely lead to efficiency gains. However, it is important to underscore that it may also expose interacting parties to certain risks that were previously managed by these

<sup>27</sup> *Ibid.*, 8-9.

<sup>28</sup> *Inter alia*: ECB, "Virtual Currency Schemes – a further analysis", February 2015, <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>, 8; FATF, "Virtual Currencies – Key Definitions and Potential AML/CFT Risks", June 2014, <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>, 8.

<sup>29</sup> P. WITZIG and V. SALOMON, "Cutting out the middleman: a case study of blockchain-induced reconfigurations in the Swiss Financial Services Industry", Working Paper 1, 2018/E, the Circulation of Wealth, Université de Neuchâtel, [http://www.unine.ch/files/live/sites/maps/files/shared/documents/wp/WP-1\\_2018\\_Witzig%20and%20Salomon.pdf](http://www.unine.ch/files/live/sites/maps/files/shared/documents/wp/WP-1_2018_Witzig%20and%20Salomon.pdf), 5.

<sup>30</sup> It should be noted that on permissioned blockchains there is still a role for a central party (see also above).

intermediaries. For instance, the Bank for International Settlements (“**BIS**”) recently warned in a report of 2017 titled *Distributed ledger technology in payment, clearing and settlement*<sup>31</sup>, that the adoption of blockchain technology could introduce new liquidity risks.<sup>32</sup> More in general it seems that when an intermediary functions as a buffer against important risks, such as systemic risk, he cannot simply be replaced by blockchain technology.

### 2.1.3. The blockchain consensus mechanisms

In principle, any node within a blockchain network can propose the addition of new information to the blockchain. In order to validate whether this addition of information (for example a transaction record) is legitimate, the nodes have to reach some form of agreement. Here a “consensus mechanism” comes into play. In short, a consensus mechanism is a predefined specific (cryptographic) validation method that ensures a correct sequencing of transactions on the blockchain.<sup>33</sup> In the case of cryptocurrencies, such sequencing is required to address the issue of “double-spending” (i.e. the issue that one and the same payment instrument or asset can be transferred more than once if transfers are not registered and controlled centrally<sup>34</sup>).

A consensus mechanism can be structured in a number of ways. Hereinafter, the two best-known – and in the context of cryptocurrencies also most commonly used – examples of consensus mechanisms will be briefly discussed: the Proof of Work (“**PoW**”) mechanism and the Proof of Stake (“**PoS**”) mechanism.

#### a. Proof of Work (PoW)

In a PoW system, network participants have to solve so-called “cryptographic puzzles” to be allowed to add new “blocks” to the blockchain. This puzzle-solving process is commonly referred to as “mining”.<sup>35</sup> In simple terms, these cryptographic puzzles are made up out of all information previously recorded on the blockchain and a new set of transactions to be added to the next “block”.<sup>36</sup> Because the input of each puzzle becomes larger over time (resulting in a more complex calculation), the PoW mechanism requires a vast amount of computing resources, which consume a significant amount of electricity.<sup>37</sup>

<sup>31</sup> CPMI, “Distributed ledger technology in payment, clearing and settlement – An analytical framework”, February 2017, <https://www.bis.org/cpmi/publ/d157.pdf>.

<sup>32</sup> *Ibid.*, 19.

<sup>33</sup> See: World Bank Group (H. NATARAJAN, S. KRAUSE and H. GRADSTEIN), “Distributed Ledger Technology (DLT) and blockchain”, 2017, FinTech note, no. 1. Washington, D.C., <http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf>, 6.

<sup>34</sup> R. HOUBEN, “Bitcoin: there two sides to every coin”, ICCLR, Vol. 26, Issue 5, 2015, 195.

<sup>35</sup> See: World Bank Group (H. NATARAJAN, S. KRAUSE and H. GRADSTEIN), “Distributed Ledger Technology (DLT) and blockchain”, 2017, FinTech note, no. 1. Washington, D.C., <http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf>, 6.

<sup>36</sup> EY, “IFRS – Accounting for crypto-assets”, March 2018, <http://eyfinancialservicesthoughtgallery.ie/wp-content/uploads/2018/03/EY-IFRS-Accounting-for-crypto-assets.pdf>, 17.

<sup>37</sup> For example, the current estimated annual electricity consumption of Bitcoin (one of the best-known examples of a cryptocurrency based on a PoW mechanism) is equivalent to the annual electricity consumed in the Czech Republic. *Inter alia*: <https://digiconomist.net/bitcoin-energy-consumption>; S. LEE, “Bitcoin’s Energy Consumption Can Power An Entire Country -- But EOS Is Trying To Fix That”, April 2018, <https://www.forbes.com/sites/shermanlee/2018/04/19/bitcoins-energy-consumption-can-power-an-entire-country-but-eos-is-trying-to-fix-that/>.

If a network participant (i.e. a node) solves a cryptographic puzzle, it proves that he has completed the work, and is rewarded with digital form of value (or in the case of a cryptocurrency, with a newly mined coin). This reward serves as an incentive to uphold the network.<sup>38</sup>

The cryptocurrency Bitcoin is based on a PoW consensus mechanism. Other examples include Litecoin, Bitcoin Cash, Monero, etc.<sup>39</sup>

#### b. Proof of Stake (PoS)

In a PoS system, a transaction validator (i.e. a network node) must prove ownership of a certain asset (or in the case of cryptocurrencies, a certain amount of coins) in order to participate in the validation of transactions. This act of validating transactions is called “forging”<sup>40</sup> instead of “mining”. For example, in the case of cryptocurrencies, a transaction validator will have to prove his “stake” (i.e. his share) of all coins in existence to be allowed to validate a transaction. Depending on how many coins he holds, he will have a higher chance of being the one to validate the next block (i.e. this all has to do with the fact that he has greater seniority within the network earning him a more trusted position).<sup>41</sup> The transaction validator is paid a transaction fee for his validation services by the transacting parties.<sup>42</sup>

Cryptocurrencies such as Neo and Ada (Cardano) utilize a PoS consensus mechanism<sup>43</sup>.

#### c. Other mechanisms

The PoW and PoS mechanisms are far from the only consensus mechanisms currently in existence.<sup>44</sup> Other examples include proof of service, proof of elapsed time and proof of capacity. A further analysis of these mechanisms falls outside the scope of this study.

### 2.1.4. Blockchain technology can have many applications

While blockchain technology is often associated with digital or virtual currency schemes, payments and financial services, its scope is much wider. Blockchain can theoretically be applied in a large variety of sectors<sup>45</sup> (e.g. trade and commerce, healthcare, governance, ...). In addition, it has numerous potential applications. It could have an impact on the pledging of collateral, on the registration of shares, bonds and other assets<sup>46</sup>, on the transfer of property titles, on the operation of land registers<sup>47</sup>, etc. An analysis of these applications falls outside the scope of this study.

<sup>38</sup> World Bank Group (H. NATARAJAN, S. KRAUSE and H. GRADSTEIN), “Distributed Ledger Technology (DLT) and blockchain”, 2017, FinTech note, no. 1. Washington, D.C., <http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf>, 6

<sup>39</sup> Also see below under 3.2. Bitcoin and beyond: the 10 cryptocurrencies with the highest market capitalisation.

<sup>40</sup> One node “forges” each block. See: EY, “IFRS – Accounting for crypto-assets”, March 2018, <http://eyfinancialservicesthoughtgallery.ie/wp-content/uploads/2018/03/EY-IFRS-Accounting-for-crypto-assets.pdf>, 17.

<sup>41</sup> EY, “IFRS – Accounting for crypto-assets”, March 2018, <http://eyfinancialservicesthoughtgallery.ie/wp-content/uploads/2018/03/EY-IFRS-Accounting-for-crypto-assets.pdf>, 17.

<sup>42</sup> In principle, cryptocurrencies that utilise a PoS mechanism are already pre-mined. Hence, forging does not create new coins. See: *ibid*.

<sup>43</sup> It should be noted that the cryptocurrency Ethereum is a special case. Ethereum has been based on a PoW mechanism from the start, but its community of developers is now planning on updating that mechanism and overlaying it with a PoS mechanism. See for example: S. JAGATI, “Ethereum’s Proof of Stake Protocol Under Review”, April 2018, <https://cryptoslate.com/ethereums-proof-of-stake-protocol-in-review/>. Also see below under 3.2.9. NEO (NEO) and 2.2.7. Cardano (ADA).

<sup>44</sup> See also: *ibid*.

<sup>45</sup> See: World Bank Group (H. NATARAJAN, S. KRAUSE and H. GRADSTEIN), “Distributed Ledger Technology (DLT) and blockchain”, 2017, FinTech note, no. 1. Washington, D.C., <http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf>, 21.

<sup>46</sup> CPMI, “Digital currencies”, November 2015, <https://www.bis.org/cpmi/publ/d137.pdf>, 15.

<sup>47</sup> See for example: W. HOLDEN, “Bringing Blockchain to Land Registry”, January 2018, <https://www.blockchain-expo.com/2018/01/blockchain/bringing-blockchain-land-registry/>.

As pointed out above, this study will only touch upon the subject of blockchain technology where this is meaningful for the research on cryptocurrencies and can be deemed relevant from the perspective of combating money laundering, terrorist financing and/or tax evasion.

## 2.2. What are cryptocurrencies?

### 2.2.1. Introduction

Establishing a definition of cryptocurrencies is no easy task. Much like blockchain, cryptocurrencies has become a “buzzword” to refer to a wide array of technological developments that utilise a technique better known as cryptography. In simple terms, cryptography is the technique of protecting information by transforming it (i.e. encrypting it) into an unreadable format that can only be deciphered (or decrypted) by someone who possesses a secret key.<sup>48</sup> Cryptocurrencies such as Bitcoin, are secured via this technique using an ingenious system of public and private digital keys.<sup>49</sup>

Hereinafter we try to give a suitable definition of cryptocurrencies on the basis of a critical analysis of the definitions already developed by various concerned policy makers at European and international level.<sup>50</sup>

### 2.2.2. The policy makers: ECB, IMF, BIS, EBA, ESMA, World Bank and FATF

Since the emergence of Bitcoin in 2009<sup>51</sup>, the subject of cryptocurrencies has been scrutinized by various policy makers, whom have each touched upon the subject in a different way.

#### a. ECB

The European Central Bank (“**ECB**”) has classified cryptocurrencies as a subset of *virtual currencies*. In a report on *Virtual Currency Schemes* of 2012, it defined such currencies as a form of unregulated digital money, usually issued and controlled by its developers, and used and accepted among the members of a specific virtual community.<sup>52</sup>

It further clarified that three types of virtual currencies can be distinguished depending on the interaction with traditional currencies and the real economy:

- i. virtual currencies that can only be used in a closed virtual system, usually in online games (e.g. *World of Warcraft Gold*);
- ii. virtual currencies that are unilaterally linked to the real economy: a conversion rate exists to purchase the currency (with traditional money) and the purchased currency can subsequently be used to buy virtual goods and services (and exceptionally also to buy real goods and services) (e.g. *Facebook Credits*);
- iii. virtual currencies that are bilaterally linked to the real economy: there are conversion rates both for purchasing virtual currency as for selling such currency; the purchased currency can be used to buy both virtual as real goods and services.<sup>53</sup>

<sup>48</sup> See for example: J. Faulkner, *Getting started with Cryptography in .NET*, München BookRix, 2016, 6.

<sup>49</sup> R. HOUBEN, “Bitcoin: there two sides to every coin”, ICCLR, Vol. 26, Issue 5, 2015, 195. Also see above under 2.1.2. How a blockchain works: the basics.

<sup>50</sup> Hence, we do not explore definitions used at national level.

<sup>51</sup> *Inter alia*: <https://bitcoin.org/en/faq#who-created-bitcoin>; G. HILEMAN and M. RAUCHS, “Global Cryptocurrency Benchmarking Study”, Cambridge Centre for Alternative Finance, 2017, [https://www.jbs.cam.ac.uk/fileadmin/user\\_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf](https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf), 15.

<sup>52</sup> ECB, “Virtual Currency Schemes”, October 2012, <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>, 13.

<sup>53</sup> *Ibid.*, 13-19.

Cryptocurrencies, such as Bitcoin, are virtual currencies of the latter type: they can both be bought with traditional money as sold against traditional money, and they can be used to buy both digital and real goods and services.<sup>54</sup>

In a more recent report of 2015 titled *Virtual Currency Schemes – a further analysis*, the ECB put forward a “second”, and largely updated, definition of virtual currencies. It defined virtual currencies as digital representations of value, not issued by a central bank, credit institution or e-money institution, which in some circumstances can be used as an alternative to money.<sup>55</sup> It also clarified that cryptocurrencies, such as Bitcoin, constitute a decentralized bi-directional (i.e. bilateral) virtual currency.<sup>56</sup>

#### b. IMF

Like the ECB, the International Monetary Fund (“*IMF*”) has categorised cryptocurrencies as a subset of *virtual currencies*, which it defines as digital representations of value, issued by private developers and denominated in their own unit of account.<sup>57</sup> According to the IMF, the concept of virtual currencies covers a wider array of ‘currencies’, ranging from simple IOUs (“Informal certificates of debt” or “I owe you’s”) by issuers (such as Internet or mobile coupons and airline miles), virtual currencies backed by assets such as gold, and cryptocurrencies such as Bitcoin.<sup>58</sup>

#### c. BIS

The Committee on Payments and Market Infrastructures (“*CPMI*”), a body of the Bank for International Settlements (“*BIS*”), has qualified cryptocurrencies as *digital currencies* or *digital currency schemes*.<sup>59</sup> These schemes are said to exhibit the following key features:

- i. they are assets, the value of which is determined by supply and demand, similar in concept to commodities such as gold, yet with zero intrinsic value;
- ii. they make use of distributed ledgers to allow remote peer-to-peer exchanges of electronic value in the absence of trust between parties and without the need for intermediaries; and
- iii. they are not operated by any specific individual or institution.<sup>60</sup>

#### d. EBA

The European Banking Authority (“*EBA*”) has suggested to refer to cryptocurrencies as *virtual currencies*, which it defines<sup>61</sup> as digital representations of value that are neither issued by a central

<sup>54</sup> *Inter alia*: BANQUE DE FRANCE, “Les dangers liés au développement des monnaies virtuelles: l'exemple de bitcoin”, in Focus, no. 10, 5 December 2013, [https://www.banque-france.fr/uploads/tx\\_bdfgrandesdates/Focus-10-stabilite-financiere.pdf](https://www.banque-france.fr/uploads/tx_bdfgrandesdates/Focus-10-stabilite-financiere.pdf), 2; R. HOUBEN, “Bitcoin: there two sides to every coin”, ICCLR, Vol. 26, Issue 5, 2015, 194; N. VANDEZANDE, *Virtual currencies: a legal framework*, Antwerp, Intersentia, 2018, 75-76.

<sup>55</sup> ECB, “Virtual Currency Schemes – a further analysis”, February 2015, <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>, 4.

<sup>56</sup> *Ibid.*, 9.

<sup>57</sup> IMF Staff Discussion Note, “Virtual Currencies and Beyond: Initial Considerations”, January 2016, <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>, 7.

<sup>58</sup> *Ibid.*

<sup>59</sup> CPMI, “Digital currencies”, November 2015, <https://www.bis.org/cpmi/publ/d137.pdf>, footnote 2: “this report uses the term “digital currencies”, because, while recognising that the term is not perfect, the term is used widely and reflects the concept that these are assets that are represented in digital form. Previous CPMI reports used the term “virtual currencies”, reflecting their existence in a virtual rather than physical form; virtual currencies in particular are prevalent in certain online environments. Moreover, these schemes are frequently referred to as “cryptocurrencies”, reflecting the use of cryptography in their issuance, and in the validation of transactions”.

<sup>60</sup> *Ibid.*, 4-7.

<sup>61</sup> It should be noted that EBA has indicated that the usage of the term ‘currency’ may be misleading in some cases. It has however opted to use this term due to its common public usage at the time (i.e. 2014). See: EBA, “EBA Opinion on ‘virtual currencies’”, 4 July 2014, <https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf>, 11.

bank or public authority nor necessarily attached to a fiat currency but are used by natural or legal persons as a means of exchange and can be transferred, stored or traded electronically.<sup>62</sup>

#### e. ESMA

The European Securities and Markets Authority ("**ESMA**") has recently also referred to cryptocurrencies as *virtual currencies*, in a pan-European warning issued in cooperation with the European Insurance and Occupational Pensions Authority ("**EIOPA**") and the EBA.<sup>63</sup> Fully in line with the EBA's definition, virtual currencies are defined as digital representations of value that are neither issued nor guaranteed by a central bank or public authority and do not have the legal status of currency or money.<sup>64</sup>

#### f. World Bank

The World Bank has classified cryptocurrencies as a subset of *digital currencies*, which it defines as digital representations of value that are denominated in their own unit of account, distinct from e-money, which is simply a digital payment mechanism, representing and denominated in fiat money.<sup>65</sup>

Contrary to most other policy makers, the World Bank has also defined cryptocurrencies itself as digital currencies that rely on cryptographic techniques to achieve consensus.<sup>66</sup>

#### g. FATF

Like many other policy makers, the Financial Action Task Force ("**FATF**") has approached cryptocurrencies as a subset of *virtual currencies*, which it defines as digital representations of value that can be digitally traded and function as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but do not have legal tender status (i.e., when tendered to a creditor, are a valid and legal offer of payment) in any jurisdiction.<sup>67</sup>

It further suggests that virtual currencies can be divided into two basic types:

- i. convertible virtual currencies that have an equivalent value in real currency and can be exchanged back-and-forth for real currency; these virtual currencies can be of a centralised or a decentralized nature (i.e. they can either have a central administrating authority that controls the system or no central oversight at all); and
- ii. non-convertible virtual currencies that are specific to a particular virtual domain or world (e.g. a Massively Multiplayer Online Role-Playing Game like *World of Warcraft*), and under the rules governing its use, cannot be exchanged for fiat currency.<sup>68</sup>

<sup>62</sup> *Ibid.* See also: Speech by Andrea Enria, Chairperson of EBA, "Designing a Regulatory and Supervisory Roadmap for FinTech", 9 March 2018, <http://www.eba.europa.eu/documents/10180/2151635/Andrea+Enria%27s+speech+on+FinTech+at+Copenhagen+Business+School+090318.pdf>, 5.

<sup>63</sup> See: ESMA, EBA & EIOPA, "Warning on the risks of Virtual Currencies" [https://www.esma.europa.eu/sites/default/files/library/esma50-164-1284\\_joint\\_esas\\_warning\\_on\\_virtual\\_currencies.pdf](https://www.esma.europa.eu/sites/default/files/library/esma50-164-1284_joint_esas_warning_on_virtual_currencies.pdf), 1.

<sup>64</sup> *Ibid.*

<sup>65</sup> See: World Bank Group (H. NATARAJAN, S. KRAUSE, and H. GRADSTEIN), "Distributed Ledger Technology (DLT) and blockchain", 2017, FinTech note, no. 1. Washington, D.C., <http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf>, IV.

<sup>66</sup> *Ibid.*

<sup>67</sup> FATF, "Virtual Currencies – Key Definitions and Potential AML/CFT Risks", June 2014, <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>, 4.

<sup>68</sup> *Ibid.*, 4-5.

Cryptocurrencies like Bitcoin are virtual currencies of the first type, that can, according to the FATF, be defined as math-based, decentralized convertible virtual currencies that are protected by cryptography.<sup>69</sup>

#### h. Summary

The main conclusion that can be drawn from the different perspectives set out above, is that there is no generally accepted definition of the term *cryptocurrencies* available in the regulatory space. Even more, most policy makers have refrained from defining the term altogether. Amongst those cited above, only the World Bank and the FATF have put forward a clear-cut definition. It is clear, however, that most policy makers approach cryptocurrencies as a subset or a form of virtual or digital currencies.

If we try to summarize all the above definitions, a good summary could be that a cryptocurrency is “a digital representation of value that (i) is intended to constitute a peer-to-peer (“P2P”) alternative to government-issued legal tender, (ii) is used as a general-purpose medium of exchange (independent of any central bank), (iii) is secured by a mechanism known as cryptography and (iv) can be converted into legal tender and vice versa”.

Hereinafter we will shed some light on the concept of cryptocurrencies (or coins; we will use both terms interchangeably hereinafter), more in particular the dividing line with other, neighboring concepts, which should nevertheless be distinguished from cryptocurrencies.

### 2.2.3. Cryptocurrencies – Tokens – Cryptosecurities

The term cryptocurrencies is in practice often erroneously used in a very broad sense.<sup>70</sup> As will be shown below, it should be distinguished from both tokens and cryptosecurities.

#### a. Cryptocurrencies – Tokens

Firstly, cryptocurrencies should be distinguished from cryptographic “tokens”, which offer a functionality other than and beyond that of a general-purpose medium of exchange. Tokens are issued in the framework of an Initial Token Offering or “ITO”<sup>71</sup> to raise funds for a given project or enterprise. They constitute a novel class of crypto-assets (i.e. digital assets recorded on a distributed ledger, secured by cryptography<sup>72</sup>) which embody some sort of claim against an entity (or against its cash flows, assets, residual value, future goods or services, ...) that arises from the use of blockchain technology.<sup>73</sup>

Some tokens resemble traditional instruments such as shares or bonds and are commonly referred to as “security tokens” or “investment tokens”.<sup>74</sup> Other tokens grant their holders (future) access to

<sup>69</sup> *Ibid.*, 5.

<sup>70</sup> In some cases, the term “Cryptocurrency” could even be called a misnomer. See: A. ZAINUDDIN, “Differences Between Cryptocurrency Coins and Tokens”, 2017, <https://masterthecrypto.com/differences-between-cryptocurrency-coins-and-tokens/>.

<sup>71</sup> We note that legal literature and popular media commonly refer to these fundraising events as Initial Coin Offerings or ICOs (see for example: J. ROHR and A. WRIGHT, “Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets”, October 2017 (electronically available via <https://ssrn.com/abstract=3048104>); D. ZETZSCHE, R. P. BUCKLEY, D. W. ARNER and L. FÖHR, “The ICO Gold Rush: It’s a scam, it’s a bubble, it’s a super challenge for regulators”, November 2017 (electronically available via <https://ssrn.com/abstract=3072298>); D. FLOYD, “\$6.3 Billion: 2018 ICO Funding Has Passed 2017’s Total”, April 2018, <https://www.coindesk.com/6-3-billion-2018-ico-funding-already-outpaced-2017/>). If we take the position that tokens actually differ from coins, then the term Initial Token Offering or ITO is a more appropriate term for future reference.

<sup>72</sup> EY, “IFRS – Accounting for crypto-assets”, March 2018, <http://eyfinancialservicesthoughtgallery.ie/wp-content/uploads/2018/03/EY-IFRS-Accounting-for-crypto-assets.pdf>, 2.

<sup>73</sup> See: A. SNYERS and K. PAUWELS, “ICOs in Belgium: down the rabbit hole into legal no man’s land? (Part 1)”, ICCLR, 2018, to be published.

<sup>74</sup> *Ibid.*

specific products or services and are commonly referred to as “utility tokens”. They can be used to acquire certain products or services, yet they do not constitute a general-purpose medium of exchange, simply because they can generally only be used on the token platform itself.<sup>75</sup>

## b. Cryptocurrencies – Cryptosecurities

Secondly, cryptocurrencies should also be distinguished from a concept that has recently been referred to as “cryptosecurities”.<sup>76</sup> In short, it has been argued that blockchain technology could also be used to register, issue and transfer regular shares and other corporate securities, so that the capitalisation table of a company is always accurate and up-to-date.<sup>77</sup> Because this technological process would be secured with cryptography, it has been suggested that these securities be defined as cryptosecurities.

The only connection between this newly developed concept “cryptosecurities” and cryptocurrencies, is that they both utilize blockchain technology.

### 2.2.4. Cryptocurrencies – Blockchain

Cryptocurrencies and blockchain have become hot topics in the last couple of years. Whilst the two are often referred to in the same sentence and are clearly linked to each other, one should never mistake one for the other. Blockchain is a type of distributed ledger technology that forms the backbone of the crypto-market. It is the technology behind the large variety of cryptocurrencies currently in circulation. Its scope and field of application are, however, not limited thereto. As set out above, blockchain can be applied in various sectors and can have a wide array of applications. It is important to draw a clear line between these applications and cryptocurrencies, which are but one specific application of blockchain technology. Against this background, regulators need not fear of stifling innovation when tackling the subject of cryptocurrencies.

## 2.3. Who are the players involved?

The cryptocurrency market is a new playing field where different actors each play a particular role. To shed some more light on how the market works, and without attempting to be exhaustive, we will hereinafter further identify the key players.

<sup>75</sup> It should be noted that various studies of the token market have put forward taxonomies of tokens. Not all of these taxonomies coincide, yet the silver thread that appears to run through all of them is that, at the very least, a distinction is to be made between “security” or “investment tokens” on the one hand and “utility tokens” on the other hand. See *inter alia*: D. ZETZSCHE, R. P. BUCKLEY, D. W. ARNER and L. FÖHR, “The ICO Gold Rush: It’s a scam, it’s a bubble, it’s a super challenge for regulators”, November 2017 (electronically available via <https://ssrn.com/abstract=3072298>); J. ROHR and A. WRIGHT, “Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets”, October 2017, (electronically available via <https://ssrn.com/abstract=3048104>); EY, “Research: initial coin offerings (ICOs)”, December 2017, [http://www.ey.com/Publication/vwLUAssets/ey-research-initial-coin-offerings-icos/\\$File/ey-research-initial-coin-offerings-icos.pdf](http://www.ey.com/Publication/vwLUAssets/ey-research-initial-coin-offerings-icos/$File/ey-research-initial-coin-offerings-icos.pdf); Laga, “Initial Coin Offerings - Legal qualification and regulatory challenges”, March 2018, <https://www.slideshare.net/fintechbelgium/fintech-belgium-meetup-on-icos-080318-laurent-godts>; FINMA, “Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)”, February 2018, <https://www.finma.ch/en/~media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=en>; P. HACKER and C. THOMALE, “Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law”, November 2017 (electronically available via <https://ssrn.com/abstract=3075820>); A. SNYERS and K. PAUWELS, “ICOs in Belgium: down the rabbit hole into legal no man’s land? (Part 1)”, ICCLR, 2018, to be published.

<sup>76</sup> M. VAN DE LOOVERBOSCH, “Crypto-effecten: tussen droom en daad”, TRV-RPS 2018, 193-207.

<sup>77</sup> *Ibid.*, 198, n° 22-23. See also: P. PAECH, “Securities, Intermediation and the Blockchain: An Inevitable Choice between Liquidity and Legal Certainty”, LSE Law, Society and Economy Working Paper 20/2015, 26-28. It should be noted that while blockchain technology is currently not yet being widely applied in the context of corporate law, it already has some legal applications (i.e. in the US (Delaware) and France). See for France: Ordonnance n° 2017-1674 du 8 de cembre 2017 relative a l’utilisation d’un dispositif d’enregistrement e lectronique partage pour la repre sentation et la transmission de titres financiers, JORF 9 december 2017, n° 0287, text n° 24, [www.legifrance.gouv.fr/eli/ordonnance/2017/12/8/2017-1674/JO/texte](http://www.legifrance.gouv.fr/eli/ordonnance/2017/12/8/2017-1674/JO/texte); see for Delaware: Delaware General Assembly, Senate Bill 69, <https://legis.delaware.gov/BillDetail?legislationId=25730>; D. LUCKING and C. O’HANLON, “Delaware Passes Law Permitting Companies to Use Blockchain Technology to Issue and Track Shares”, 26 September 2017, <http://www.allenoverly.com/publications/en-gb/Pages/Delaware-Passes-Law-Permitting-Companies-to-Use-Blockchain-Technology-to-Issue-and-Track-Shares.aspx>.



### 2.3.1. Cryptocurrency users

A first, and very important, player is the “**cryptocurrency user**”. A cryptocurrency user is a natural person or legal entity who obtains coins to use them (i) to purchase real or virtual goods or services (from a set of specific merchants<sup>78</sup>), (ii) to make P2P payments, or (iii) to hold them for investment purposes (i.e. in a speculative manner).<sup>79</sup>

Without trying to be exhaustive, a cryptocurrency user can obtain his coins in a number of ways<sup>80</sup>:

- Firstly, he can simply buy his coins on a cryptocurrency exchange using fiat money or another cryptocurrency;
- Secondly, he can buy his coins directly from another cryptocurrency user (i.e. through a trading platform – this form of exchange is often referred to as a “P2P exchange”);
- Thirdly, if a cryptocurrency is based on a PoW consensus mechanism, he can mine a new coin (i.e. participate in the validation of transactions by solving of a “cryptographic puzzle” and be rewarded a new coin<sup>81</sup>);
- Fourthly, in some cases he can obtain his coins directly from the coin offeror, either as part of a free initial offering of coins (e.g. on the Stellar network Lumens (XLM) are being given away for free<sup>82</sup>) or in the framework of a crowd sale set-up by the coin offeror (e.g. a large bulk of ether (cf. Ethereum) was sold in a crowdsale to cover certain development costs<sup>83</sup>);
- Fifthly, if he sells goods or services in exchange for cryptocurrency, he can also receive coins as a payment for those goods or services;
- Sixthly, in case of a “hard fork”<sup>84</sup> of a coin’s blockchain, he will automatically obtain an amount of the newly created coin; and
- Finally, he can receive coins as a gift or donation from another cryptocurrency user.

### 2.3.2. Miners

A second player is the “**miner**” who participates in validating transactions on the blockchain by solving a “cryptographic puzzle”. As explained above, the process of mining relates to cryptocurrencies that are based on a PoW consensus mechanism. A miner supports the network by harnessing computing power to validate transactions and is rewarded with newly mined coins (i.e. through an automatic decentralized new issuance).<sup>85</sup> Miners can be cryptocurrency users, or, more commonly, parties who have made a new business out of mining coins to sell them for fiat currency

<sup>78</sup> At present, only a limited number of (online) merchants accepts payments in Cryptocurrencies. See for example for the Cryptocurrency Litecoin: <https://litecoin.com/services#merchants>.

<sup>79</sup> See *inter alia*: FATF, “Virtual Currencies – Key Definitions and Potential AML/CFT Risks”, June 2014, <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>, 7; ECB, “Virtual Currency Schemes – a further analysis”, February 2015, <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>, 8; COMMISSION STAFF WORKING DOCUMENT Accompanying the document “Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border situations”, COM(2017) 340 final, Annex, Part 2, [https://eur-lex.europa.eu/resource.html?uri=cellar:d4d7d30e-5a5a-11e7-954d-01aa75ed71a1.0001.02/DOC\\_1&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:d4d7d30e-5a5a-11e7-954d-01aa75ed71a1.0001.02/DOC_1&format=PDF), 85.

<sup>80</sup> See also: ECB, “Virtual Currency Schemes – a further analysis”, February 2015, <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>, 8.

<sup>81</sup> Also see above under 2.1.3. The blockchain consensus mechanisms.

<sup>82</sup> See: <https://www.stellar.org/lumens/>. Also see below under 3.2.6. Stellar (XLM).

<sup>83</sup> Also see below under 3.2.2. Ethereum (ETH).

<sup>84</sup> This concept is discussed and explained further below under “Bitcoin Cash”.

<sup>85</sup> ECB, “Virtual Currency Schemes – a further analysis”, February 2015, <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>, 7.

(such as US dollar or Euro) or for other cryptocurrencies.<sup>86</sup> Some miners group in so-called pools of miners to bundle computing power.<sup>87</sup>

At present, the risks associated with so-called “mining businesses” appear to be underestimated. We will further elaborate on this below.<sup>88</sup>

### 2.3.3. Cryptocurrency exchanges

A third group of key players are the so-called “**cryptocurrency exchanges**”. Cryptocurrency exchanges are persons or entities who offer exchange services to cryptocurrency users, usually against payment of a certain fee (i.e. a commission). They allow cryptocurrency users to sell their coins for fiat currency or buy new coins with fiat currency.<sup>89</sup> They usually function both as a bourse and as a form of exchange office.<sup>90</sup> Examples of well-known cryptocurrency exchanges are: Bitfinex<sup>91</sup>, HitBTC<sup>92</sup>, Kraken<sup>93</sup> and Coinbase GDAX<sup>94, 95</sup>.

It is important to note that some exchanges are *pure* cryptocurrency exchanges, which means that they only accept payments in other cryptocurrencies, usually Bitcoin (for example Binance<sup>96</sup>), whilst others also accept payments in fiat currencies such as US dollar or Euro (for example Coinbase). Furthermore, many cryptocurrency exchanges only allow their users to buy a particular selection of coins.

It should also be noted that many cryptocurrency exchanges (i.e. both regular and pure cryptocurrency exchanges) operate as custodian wallet providers<sup>97</sup> (for example Bitfinex).

In general cryptocurrency exchanges offer their users a wide array of payment options, such as wire transfers, PayPal transfers, credit cards and other coins.<sup>98</sup> Some cryptocurrency exchanges also provide statistics on the cryptocurrency market (like trading volumes and volatility of the coins traded<sup>99</sup>) and offer conversion services to merchants who accept payments in cryptocurrencies.

<sup>86</sup> FATF, “Virtual Currencies – Key Definitions and Potential AML/CFT Risks”, June 2014, <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>, 7.

<sup>87</sup> See: COMMISSION STAFF WORKING DOCUMENT Accompanying the document “Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border situations”, COM(2017) 340 final, Annex, Part 2, [https://eur-lex.europa.eu/resource.html?uri=cellar:d4d7d30e-5a5a-11e7-954d-01aa75ed71a1.0001.02/DOC\\_1&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:d4d7d30e-5a5a-11e7-954d-01aa75ed71a1.0001.02/DOC_1&format=PDF), 85.

<sup>88</sup> See 5.3.3 Miners.

<sup>89</sup> FATF, “Virtual Currencies – Key Definitions and Potential AML/CFT Risks”, June 2014, <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>, 7.

<sup>90</sup> *Ibid.*; It should be noted that there is currently also a very limited number of so-called Cryptocurrency ATMs (e.g. Bitcoin ATMs) on the market, which also qualify as cryptocurrency exchanges. See: COMMISSION STAFF WORKING DOCUMENT Accompanying the document “Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border situations”, COM(2017) 340 final, Annex, Part 2, [https://eur-lex.europa.eu/resource.html?uri=cellar:d4d7d30e-5a5a-11e7-954d-01aa75ed71a1.0001.02/DOC\\_1&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:d4d7d30e-5a5a-11e7-954d-01aa75ed71a1.0001.02/DOC_1&format=PDF), 86.

<sup>91</sup> See: <https://www.bitfinex.com>.

<sup>92</sup> See: <https://hitbtc.com>.

<sup>93</sup> See: <https://www.kraken.com>.

<sup>94</sup> See: <https://www.coinbase.com>.

<sup>95</sup> See for other examples: <https://cryptocoincharts.info/markets/info>.

<sup>96</sup> See: <https://www.binance.com>.

<sup>97</sup> See further below: 2.3.5 Wallet providers.

<sup>98</sup> See: ECB, “Virtual Currency Schemes – a further analysis”, February 2015, <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>, 8.

<sup>99</sup> For example, the Bitfinex Cryptocurrency Exchange offers a number of statistics, as well as conversion rates against fiat currency; see: <https://www.bitfinex.com>.

### 2.3.4. Trading platforms

In addition to cryptocurrency exchanges, so-called “**trading platforms**” also play an important role in the exchange of cryptocurrencies (and, most notably, allow cryptocurrency users to buy coins with cash). Trading platforms are market places that bring together different cryptocurrency users that are either looking to buy or sell coins, providing them with a platform on which they can directly trade with each other (i.e. an “eBay” for cryptocurrencies).<sup>100</sup>

Trading platforms are sometimes referred to as “P2P exchanges” or “decentralized exchanges”.<sup>101</sup> They differ from cryptocurrency exchanges in a number of ways. First and foremost, they do not buy or sell coins themselves.<sup>102</sup> Secondly, they are not run by an entity or company that oversees and processes all trades, but they are operated exclusively by software (i.e. there is no central point of authority).<sup>103</sup> Trading platforms simply connect a buyer with a seller, allowing them to conduct a deal, online, or even locally in-person (i.e. a face-to-face trade, often executed in cash). A well-known example of a trading platform for Bitcoins is LocalBitcoins<sup>104</sup>.

### 2.3.5. Wallet providers

Another group of key players are the so-called “**wallet providers**”. Wallet providers are those entities that provide cryptocurrency users digital wallets or e-wallets which are used for holding, storing and transferring coins.<sup>105</sup> Simply put, a wallet holds a cryptocurrency user’s cryptographic keys (see above). A wallet provider typically translates a cryptocurrency user’s transaction history into an easily readable format, which looks much like a regular bank account.<sup>106</sup>

In reality, there are several types of wallet providers<sup>107</sup>:

- *Hardware wallet providers* that provide cryptocurrency users with specific hardware solutions to privately store their cryptographic keys (e.g. Ledger Wallet<sup>108</sup>, ...);
- *Software wallet providers* that provide cryptocurrency users with software applications which allow them to access the network, send and receive coins and locally save their cryptographic keys (e.g. Jaxx<sup>109</sup>);
- *Custodian wallet providers* that take (online) custody of a cryptocurrency user’s cryptographic keys (e.g. Coinbase<sup>110</sup>).

<sup>100</sup> ECB, “Virtual Currency Schemes – a further analysis”, February 2015, <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>, 8.

<sup>101</sup> See: A. MARSHALL, “P2P Cryptocurrency Exchanges, Explained”, April 2017, <https://cointelegraph.com/explained/p2p-cryptocurrency-exchanges-explained>.

<sup>102</sup> ECB, “Virtual Currency Schemes – a further analysis”, February 2015, <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>, 8.

<sup>103</sup> See: A. MARSHALL, “P2P Cryptocurrency Exchanges, Explained”, April 2017, <https://cointelegraph.com/explained/p2p-cryptocurrency-exchanges-explained>.

<sup>104</sup> See: <https://localbitcoins.com>.

<sup>105</sup> FATF, “Virtual Currencies – Key Definitions and Potential AML/CFT Risks”, June 2014, <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>, 8.

<sup>106</sup> See also: ECB, “Virtual Currency Schemes – a further analysis”, February 2015, <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>, 8.

<sup>107</sup> See also: COMMISSION STAFF WORKING DOCUMENT Accompanying the document “Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border situations”, COM(2017) 340 final, Annex, Part 2, [https://eur-lex.europa.eu/resource.html?uri=cellar:d4d7d30e-5a5a-11e7-954d-01aa75ed71a1.0001.02/DOC\\_1&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:d4d7d30e-5a5a-11e7-954d-01aa75ed71a1.0001.02/DOC_1&format=PDF), 85; T. KEATINGE, D. CARLISLE and F. KEEN, “Virtual currencies and terrorist financing: assessing the risks and evaluating responses”, study commissioned by the Directorate General for Internal Policies, Policy Department for Citizens’ Rights and Constitutional Affairs, May 2018, 14 (electronically available via [http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL\\_STU\(2018\)604970\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf)).

<sup>108</sup> See: <https://www.ledgerwallet.com/products>.

<sup>109</sup> See: <https://jaxx.io>.

### 2.3.6. Coin inventors

There are also those players who are referred to as “**coin inventors**”. Coin inventors are individuals or organizations who have developed the technical foundations of a cryptocurrency and set the initial rules for its use.<sup>111</sup> In some cases their identity is known (e.g. Ripple, Litecoin, Cardano), but ever so often they remain unidentified (eg. Bitcoin, Monero). Some remain involved in maintaining and improving the cryptocurrency’s code and underlying algorithm (in principle without administrator’s powers), whilst others simply disappear (e.g. Bitcoin).<sup>112</sup>

### 2.3.7. Coin offerors

A final group of key players to be distinguished are the “**coin offerors**”. Coin offerors are individuals or organizations that offer coins to cryptocurrency users upon the coin’s initial release, either against payment (i.e. through a crowdsale) or at no charge (i.e. in the framework of a specific (sign-up) program (e.g. Stellar – see below)), normally to fund the coin’s further development or boost its initial popularity.

The coins these coin offerors offer to cryptocurrency users are created or pre-mined prior to the coin’s official release / the coin’s inception. Coins that are distributed this way are either partially pre-mined or pre-created (i.e. cryptocurrency users can still generate more coins after the release), or are fully pre-mined or pre-created. In the latter case the coin offeror usually retains a large portion of the coins (e.g. this is the case with Stellar).

It is important to note that not all coins have an identifiable coin offeror, nor are all coins pre-mined or is its full supply pre-created.

A coin offeror can be the same person as the coin inventor, or another individual or organization.

---

<sup>110</sup> See *inter alia*: <https://support.coinbase.com/customer/en/portal/topics/601112-wallet-services/articles>.

<sup>111</sup> ECB, “Virtual Currency Schemes – a further analysis”, February 2015, <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>, 7.

<sup>112</sup> *Ibid.*

### 3. CLASSIFYING CRYPTOCURRENCIES

#### 3.1. Scoping the Crypto-Market

After having known a steady growth over the last couple of years, the market for cryptocurrencies has skyrocketed in 2017, appreciating more than 1,200%.<sup>113</sup> At present, there are several hundreds of coins in circulation (with a total market capitalisation of well over EUR 300 billion)<sup>114</sup>, and more continue to pop up on a regular basis. In order to fully grasp this emerging market and carry out a meaningful study, we have opted to first analyse the key properties of the best-known cryptocurrency Bitcoin and then tackle the main features of a selected number of alternative cryptocurrencies, better known as “**Altcoins**”.

Altcoins are all coins that are an alternative to Bitcoin.<sup>115</sup> In short, there are two types of Altcoins:

- Altcoins that are built using Bitcoin’s original open-source protocol, with a number of changes to its underlying codes<sup>116</sup>, conceiving a new coin with a different set of features.<sup>117</sup> An example of such an Altcoin is Litecoin.<sup>118</sup>
- Altcoins that are not based on Bitcoin’s open-source protocol, but that have their own protocol and distributed ledger. Well-known examples of such Altcoins are Ethereum and Ripple.<sup>119</sup>

This study will focus on the ten Altcoins that currently have the highest market capitalisation (see Table 1).<sup>120</sup> We have made this selection, not only on the basis of the current popularity of these Altcoins within the “crypto-community”, but also because they exhibit a wide range of different features. Some of them are based on Bitcoin’s original open-source protocol, whilst others constitute an entirely new platform and/or eco-system. Some utilise a PoW mechanism, others employ another form of consensus mechanism. Most are characterised as pseudo-anonymous, yet some are said to even be fully anonymous (meaning that the amount of coins their users own, send and receive is not observable, traceable or linkable through the blockchain’s transaction history<sup>121</sup>).

<sup>113</sup> See: C. BOVAIRD, “Why the crypto market has appreciated more than 1,200% this year”, November 2017, <https://www.forbes.com/sites/cbovaire/2017/11/17/why-the-crypto-market-has-appreciated-more-than-1200-this-year/#3906c8d6eed3>. See for some interesting charts on the growth of the market: <https://coinmarketcap.com/charts/>.

<sup>114</sup> According to data available on <https://coinmarketcap.com/coins/views/all/> (data derived on 27 May 2018) the number of Coins in circulation nears 900. If we count both Coins and Tokens, the crypto-market already exceeds a total of 1600 different crypto-assets.

<sup>115</sup> FATF, “Virtual Currencies – Key Definitions and Potential AML/CFT Risks”, June 2014, <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>, 6. See also: D. HELLER, “The implications of digital currencies for monetary policy”, in-depth analysis commissioned by the Directorate General for Internal Policies, Policy Department A: Economic and Scientific Policy, May 2017, 7 (electronically available via [http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/602048/IPOL\\_IDA\(2017\)602048\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/602048/IPOL_IDA(2017)602048_EN.pdf)).

<sup>116</sup> Bitcoin’s original protocol is available via <https://bitcoin.org/bitcoin.pdf>.

<sup>117</sup> ECB, “Virtual Currency Schemes – a further analysis”, February 2015, <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>, 9. See also: A. ZAINUDDIN, “Coins, Tokens & Altcoins: What’s the Difference?”, 2017, <https://masterthecrypto.com/differences-between-cryptocurrency-coins-and-tokens/>.

<sup>118</sup> See *inter alia*: J. MARTINDALE, “What is Litecoin? Here’s everything you need to know”, January 2018, <https://www.digitaltrends.com/computing/what-is-litecoin/>. See also: T. MANDJEE, “Bitcoin, its Legal Classification and its Regulatory Framework”, 15 J. Bus. & Sec. L. 157, 2016, <http://digitalcommons.law.msu.edu/jbsl>, 163.












<sup>119</sup> See: A. ZAINUDDIN, “Coins, Tokens & Altcoins: What’s the Difference?”, 2017, <https://masterthecrypto.com/differences-between-cryptocurrency-coins-and-tokens/>.

<sup>120</sup> This selection was made on 27 May 2018 at 15:00 PM, on the basis of data derived from <https://coinmarketcap.com/coins/views/all/>.

<sup>121</sup> See *inter alia*: A. ZAINUDDIN, “Guide on Privacy Coins: Comparison of Anonymous Cryptocurrencies”, 2017, <https://masterthecrypto.com/privacy-coins-anonymous-cryptocurrencies/>; P. GLAZER, “An Overview of Privacy Coins”, February 2018, <https://hackernoon.com/an-overview-of-privacy-tokens-19f6af8077b7>; L. NEL, “Privacy Coins: Beginner’s Guide to Anonymous Cryptocurrencies”, April 2018, <https://blockonomi.com/privacy-cryptocurrency/>. Also see below under 3.2.10. Monero (XMR) and 3.2.11. Dash (DASH).

The below analysis of the selected cryptocurrencies is based solely on the information available to the public via the internet.

Table 1: Overview of coins

Name	Symbol	Market Cap <sup>122</sup>	Supply limit <sup>123</sup>
Bitcoin	 BTC	\$124.969.093.161	21 million
Ethereum	 ETH	\$57.462.517.858	TBD <sup>124</sup>
Ripple	 XRP	\$23.790.387.789	100 billion
Bitcoin Cash	 BCH	\$17.159.025.225	21 million
Litecoin	 LTC	\$6.704.709.572	84 million
Stellar	 XLM	\$5.128.373.973	100 billion
Cardano	 ADA	\$5.034.129.651	45 billion
IOTA	 MIOTA	\$4.038.240.572	2,779,530,283,277,761
NEO	 NEO	\$3.386.383.000	100 million
Monero	 XMR	\$2.626.586.260	18,4 million
Dash	 DASH	\$2.592.894.544	17.74 – 18.92 million <sup>125</sup>

<sup>122</sup> This data has been derived from <https://coinmarketcap.com/coins/views/all/> on 27 May 2018 at 15:00 PM. It should be noted that this data is very volatile, like the cryptocurrency market itself. For purposes of convenience we have opted to present this data in its original form, i.e. denominated in US dollar.

<sup>123</sup> This data has been derived from different websites set-up and supported by members of each respective cryptocurrency community. See: <https://bitcoin.org> (BTC); <https://www.ethereum.org> (ETH); <https://ripple.com> (XRP); <https://www.bitcoincash.org> (BCH); <https://litecoin.com> (LTC); <https://www.stellar.org> (XLM); <https://www.cardano.org> (ADA); <https://www.iota.org> (MIOTA); <https://neo.org> (NEO); <http://www.monero.cc> (XMR); <https://www.dash.org> (DASH).

<sup>124</sup> We note that Ethereum’s co-inventor Vitalik Buterin recently launched a proposal in the Ethereum community to limit the total supply of ETH to 120,204,432. See: L. K. ABIOLA, ‘Ethereum (ETH) Co-Founder Provides Answer To Long-Lived Supply Limit Question’, April 2018, <https://oracletimes.com/ethereum-eth-co-founder-provides-answer-to-long-lived-supply-limit-question/>; K. SHAH, ‘Ethereum Supply Limit to 120 million – Prank or Reality?’, April 2018, <https://www.cryptoground.com/a/ethereum-supply-limit-to-120-million>.

<sup>125</sup> The total supply limit of Dash depends on the allocation of block rewards, which in turn depends on future voting behaviour within the Dash network. See: <https://docs.dash.org/en/latest/introduction/features.html>.

## 3.2. Bitcoin and beyond: the 10 cryptocurrencies with the highest market capitalisation

### 3.2.1. Bitcoin (BTC)

#### a. What is Bitcoin?

Bitcoin (BTC) is usually described as a virtual, decentralized and (at first glance) anonymous currency that is not government-backed or backed by any other legal entity, and that can not be exchanged into gold or any other commodity.<sup>126</sup>

At the heart of the creation of Bitcoin stands the text "*Bitcoin: a Peer-to-Peer Electronic Cash System*" of Satoshi Nakamoto<sup>127</sup>, published on the internet in 2008. It was on the basis of this text and the ideas conveyed in it that the development of Bitcoin accelerated. Contributory to the mystic nature of Bitcoin is that until now it remains unclear whether Satoshi Nakamoto is a real person, a pseudonym, or perhaps even a group of hackers.<sup>128</sup>

The virtual character of Bitcoin implies that Bitcoins normally do not take a physical form. Therefore, a good representation of a Bitcoin probably is that of a computer file saved on a personal computer or, via an online service, in a digital wallet.<sup>129</sup> The mere virtual character of Bitcoins should, however, be qualified. Reputedly, it is possible to print out the combination of characters that constitute the

<sup>126</sup> R. GRINBERG, "Bitcoin: An Innovative Alternative Digital Currency", *Hastings Science & Technology Law Journal*, 2011, Vol. 4, 160 (electronically available via [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1817857](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1817857)). Also see the similar, yet sometimes gradually differing definitions set forth in: N.M. KAPLANOV, "Nerdy Money: Bitcoin, the private digital currency, and the case against its regulation", *Temple Law Review* 2012, 2 (electronically available via [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2115203](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2115203)); J. BRITO, H. SHADAB and A. CASTILLO, "Bitcoin financial regulation: securities, derivatives, prediction markets & gambling", 24 July 2014, 4 (electronically available via [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2423461](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2423461)); L.J. TRAUTMAN, "Virtual currencies: Bitcoin & what now after Liberty Reserve, Silk Road, and Mt. Gox?", *Richmond Journal of Law and Technology*, Vol. 20, No. 4, 2014, 5 (electronically available via [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2393537](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2393537)); D. BRYANS, "Bitcoin and Money Laundering: Mining for and Effective Solution" *Indiana Law Journal*, 2014, Vol. 89: Iss. 1, Article 13, 443 (electronically available via <https://www.repository.law.indiana.edu/ilj/vol89/iss1/13>); R. BOLLEN, "The Legal Status of Online Currencies: Are Bitcoins the Future?", *Journal of Banking and Finance Law and Practice* 2013, 3 (electronically available via <http://ssrn.com:80/abstract=2285247>); N.A. PLASSARAS, "Regulating Digital Currencies: Bringing Bitcoin Within the Reach of the IMF", *Chicago Journal of International Law*, 2013, 4 (electronically available <http://ssrn.com:80/abstract=2248419>); LAM PAK NIAN, "Bitcoin in Singapore: A Light-Touch Approach to Regulation", 11 April 2014, 9 (electronically available via [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2427626](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2427626)); B.E GUP, "What Is Money? From Commodities to Virtual Currencies/Bitcoin" (14 March 2014), 6 (electronically available via [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2409172](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2409172)). Also see the influential publication of the ECB: ECB, "Virtual Currency Schemes", October 2012, <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>, 21. R. HOUBEN, "Bitcoin: there two sides to every coin", *ICCLR*, Vol. 26, Issue 5, 2015, 193-208.

<sup>127</sup> Which can be found via <https://bitcoin.org/bitcoin.pdf>. Satoshi Nakamoto in turn was inspired by the ideas of W. Dai, as set out in a text of 1998 titled "b-money" (electronically available via: <http://www.weidai.com/bmoney.txt>). See on the history of Bitcoin: R. GRINBERG, "Bitcoin: An Innovative Alternative Digital Currency", *Hastings Science & Technology Law Journal*, 2011, Vol. 4, 162 (electronically available via [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1817857](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1817857)); ECB, "Virtual Currency Schemes", October 2012, <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>, 21; D. BRYANS, "Bitcoin and Money Laundering: Mining for and Effective Solution" *Indiana Law Journal*, 2014, Vol. 89: Iss. 1, Article 13, 444 (electronically available via <https://www.repository.law.indiana.edu/ilj/vol89/iss1/13>); N.A. PLASSARAS, "Regulating Digital Currencies: Bringing Bitcoin Within the Reach of the IMF", *Chicago Journal of International Law*, 2013, 13-14 (electronically available <http://ssrn.com:80/abstract=2248419>).

<sup>128</sup> See the recent speculations made by L. McGRATH GOODMAN, "The Face Behind Bitcoin", in *Newsweek*, 14 March 2014, <http://www.newsweek.com/2014/03/14/face-behind-bitcoin-247957.html>.

<sup>129</sup> *Inter alia*: N.M. KAPLANOV, "Nerdy Money: Bitcoin, the private digital currency, and the case against its regulation", *Temple Law Review* 2012, 4 (electronically available via [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2115203](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2115203)); N.A. PLASSARAS, "Regulating Digital Currencies: Bringing Bitcoin Within the Reach of the IMF", *Chicago Journal of International Law*, 2013, 6 (electronically available <http://ssrn.com:80/abstract=2248419>). We reiterate that such wallets are normally not offered by credit institutions or investment institutions, but by non-regulated entities (i.e. so-called wallet providers). For that reason alone depositors of Bitcoins are not protected by deposit guarantee schemes or investor compensation schemes, as these schemes only apply to deposits at credit institutions and/or investment entities (cf. Directive 94/19/EC of 30 May 1994 on deposit guarantee schemes, *OJ L* 31 May 1994, iss. 135, p. 5 and Article 380 of the Belgian Act of 25 April 2014 on the legal status and supervision of credit institutions and Directive 97/9/EC of 3 March 1997 on investor compensation schemes, *OJ L* 26 March 1997, iss. 84, p. 22).

Bitcoin and, subsequently, to transfer such print as a bearer instrument<sup>130</sup>. However, this is supposed to be a marginal phenomenon and, hence, will not further elaborated here.

Bitcoin is based on a PoW consensus mechanism. The issue of Bitcoins takes place via a process called "mining" (see also above). To reiterate, such process the entire elements of which are publicly available via open-source software – entails that persons voluntarily make their own computers available to the Bitcoin network to solve complex mathematical problems.<sup>131</sup> Computers that are able to solve such problems (and, as a consequence, are able to create so-called transaction "blocks") are rewarded with Bitcoins.<sup>132</sup>

The aggregate number of Bitcoins that can be created through mining is limited: the Bitcoin system is programmed so that the development of blocks in time will be rewarded with increasingly less Bitcoins and that at no point in time will more than 21 million Bitcoins exist.<sup>133</sup> The fact that the creation and the increase of Bitcoins is automated and limited by the system itself implies that there is no need for the intervention of a central entity / authority to issue Bitcoins.<sup>134</sup>

The limited number of Bitcoins, together with the fact that conversion rates for Bitcoins are determined by supply and demand, without a government body being able to intervene (e.g. by printing additional money), results in a high volatility in Bitcoins prices.<sup>135</sup>

#### b. Bitcoin runs on an open, permissionless blockchain

The Bitcoin blockchain is a typical example of an open, permissionless blockchain.<sup>136</sup> Any person can join or leave the public Bitcoin network at will, without having to be (pre-)approved by any (central) entity. All that is needed to join the Bitcoin network and add transactions to the ledger is a computer on which the relevant software has been installed.

<sup>130</sup> EBA, "EBA Opinion on 'virtual currencies'", 4 July 2014, <https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf>, 12.

<sup>131</sup> N.M. KAPLANOV, "Nerdy Money: Bitcoin, the private digital currency, and the case against its regulation", Temple Law Review 2012, 7 (electronically available via [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2115203](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2115203)); ECB, "Virtual Currency Schemes", October 2012, <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>, 21 and 24.

<sup>132</sup> N.M. KAPLANOV, "Nerdy Money: Bitcoin, the private digital currency, and the case against its regulation", Temple Law Review 2012, 7 (electronically available via [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2115203](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2115203)).

<sup>133</sup> N.M. KAPLANOV, "Nerdy Money: Bitcoin, the private digital currency, and the case against its regulation", Temple Law Review 2012, 8 (electronically available via [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2115203](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2115203)); R. BOLLEN, "The Legal Status of Online Currencies: Are Bitcoins the Future?", Journal of Banking and Finance Law and Practice 2013, 6 (electronically available via <http://ssrn.com:80/abstract=2285247>); R. GRINBERG, "Bitcoin: An Innovative Alternative Digital Currency", Hastings Science & Technology Law Journal, 2011, Vol. 4, 163 (electronically available via [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1817857](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1817857)); ECB, "Virtual Currency Schemes", October 2012, <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>, 25; D. BRYANS, "Bitcoin and Money Laundering: Mining for and Effective Solution" Indiana Law Journal, 2014, Vol. 89: Iss. 1, Article 13, 446-447 (electronically available via <https://www.repository.law.indiana.edu/ilj/vol89/iss1/13>); N.A. PLASSARAS, "Regulating Digital Currencies: Bringing Bitcoin Within the Reach of the IMF", Chicago Journal of International Law, 2013, 8 (electronically available <http://ssrn.com:80/abstract=2248419>).

<sup>134</sup> N.M. KAPLANOV, "Nerdy Money: Bitcoin, the private digital currency, and the case against its regulation", Temple Law Review 2012, 8 (electronically available via [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2115203](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2115203)).

<sup>135</sup> Also see the press release of the NBB and the FSMA of 14 January 2014 ([http://www.fsma.be/nl-in-the-picture/Article/press/div/2014/2014-01-14\\_virtueel.aspx](http://www.fsma.be/nl-in-the-picture/Article/press/div/2014/2014-01-14_virtueel.aspx)) and in BANQUE DE FRANCE, "Les dangers liés au développement des monnaies virtuelles: l'exemple de bitcoin", in Focus, no. 10, 5 December 2013, [https://www.banque-france.fr/uploads/tx\\_bdfgrandesdates/Focus-10-stabilite-financiere.pdf](https://www.banque-france.fr/uploads/tx_bdfgrandesdates/Focus-10-stabilite-financiere.pdf), 4; R. BOLLEN, "The Legal Status of Online Currencies: Are Bitcoins the Future?", Journal of Banking and Finance Law and Practice 2013, 4 (electronically available via <http://ssrn.com:80/abstract=2285247>); B.E GUP, "What Is Money? From Commodities to Virtual Currencies/Bitcoin" (14 March 2014), 7 (electronically available via [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2409172](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2409172)); J. BRITO, H. SHADAB and A. CASTILLO, "Bitcoin financial regulation: securities, derivatives, prediction markets & gambling", 24 July 2014, 11-14 (electronically available via [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2423461](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2423461)).

<sup>136</sup> See for example: R. LEWIS, J. MCPARTLAND and R. RANJAN, "Blockchain and financial market innovation", Economic Perspectives, Issue 7, 2017, Federal Reserve Bank of Chicago (electronically available via <https://www.chicagofed.org/publications/economic-perspectives/2017/7>).



### c. Bitcoin is directly convertible into fiat currency

Bitcoin can be bought with and directly converted into fiat currency on a wide array of cryptocurrency exchanges (e.g. Coinbase, Kraken, Anycoin Direct<sup>137</sup>, Lunco<sup>138</sup>, ...). Out of all cryptocurrencies currently in circulation, Bitcoin is one of the easiest coins to convert into fiat currency.

### d. Bitcoin is a medium of exchange

Bitcoin (BTC) is being accepted as a legitimate source of funds by a relatively large number of (online) merchants, among which various large companies (e.g. Microsoft<sup>139</sup>, Expedia<sup>140</sup>, Playboy<sup>141</sup>, Virgin Galactic<sup>142</sup>, LOT Polish Airlines<sup>143</sup>, ...) <sup>144</sup>. As a result it can be qualified as a medium of exchange.

### e. Bitcoin is a pseudo-anonymous coin

Bitcoin is often characterized as an *anonymous* currency: although everyone can verify the chain of transactions on the basis of the public ledger, at first glance nothing in the system connects Bitcoins to individuals.<sup>145</sup> However, this anonymous character is far from absolute. It is technically feasible – though very complex and costly – to identify the parties behind a Bitcoin transaction by bringing together factors that accompany such transaction.<sup>146</sup> In other words, Bitcoin is not a fully anonymous currency, but rather a pseudo-anonymous coin.<sup>147</sup>

## 3.2.2. Ethereum (ETH)

### a. What is Ethereum?

Ethereum, launched in July 2015<sup>148</sup>, is a decentralized platform that runs so-called “smart contracts”. Smart contracts are “self-executing” contracts or applications that run exactly as programmed without any possibility of downtime (i.e. the blockchain is never down, it is always running), censorship, fraud or third-party interference.<sup>149</sup>

<sup>137</sup> See: <https://anycoindirect.eu/>.

<sup>138</sup> See: <https://www.luno.com>.

<sup>139</sup> Microsoft accepts payments with Bitcoin in its Xbox online store for games and movies. See: <https://support.microsoft.com/nl-be/help/13942/microsoft-account-add-money-with-bitcoin>.

<sup>140</sup> See: <https://www.expedia.com/Checkout/BitcoinTermsAndConditions>.

<sup>141</sup> See: <http://fortune.com/2018/03/14/playboy-cryptocurrency-vice-vit-crypto/>.

<sup>142</sup> See: <https://www.virgin.com/richard-branson/bitcoins-space>.

<sup>143</sup> See: <https://www.coindesk.com/lot-polish-airlines-accept-bitcoin/>.

<sup>144</sup> See for more examples: <https://99bitcoins.com/who-accepts-bitcoins-payment-companies-stores-take-bitcoins/>.

<sup>145</sup> R. GRINBERG, "Bitcoin: An Innovative Alternative Digital Currency", Hastings Science & Technology Law Journal, 2011, Vol. 4, 164 (electronically available via [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1817857](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1817857)); ECB, "Virtual Currency Schemes", October 2012, <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>, 23.

<sup>146</sup> M. FLEDER, M.S. KESTER and S. PILAI, "Bitcoin Transaction Graph Analysis", January 2014 (electronically available via <http://people.csail.mit.edu/spillai/data/papers/bitcoin-transaction-graph-analysis.pdf>): "In conclusion, we showed that by leveraging several sources of publicly available information via web-scraped forums and Bitcoin's transaction ledger, the Bitcoin transaction network is shown to be not entirely anonymous.". Also see LAM PAK NIAN, "Bitcoin in Singapore: A Light-Touch Approach to Regulation", 11 April 2014, 14-15 (electronically available via [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2427626](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2427626)).

<sup>147</sup> See: A. VAN WIRDUM, "Is Bitcoin Anonymous? A Complete Beginner's Guide", November 2015, <https://bitcoinmagazine.com/articles/is-bitcoin-anonymous-a-complete-beginner-s-guide-1447875283/>. See also: Q. SHENTU and J. YU, "Research on Anonymization and De-anonymization in the Bitcoin System", October 2015 (electronically available via <https://arxiv.org/pdf/1510.07782.pdf>).

<sup>148</sup> See: <http://ethdocs.org/en/latest/introduction/history-of-ethereum.html>.

<sup>149</sup> See: <https://www.ethereum.org>.

Ethereum has a capability that goes far beyond that of a pure P2P digital cash equivalent like Bitcoin. In simple terms, it is much like a smartphone operating system on top of which software applications can be built.<sup>150</sup>

Technically speaking, the Ethereum platform itself is not a cryptocurrency. However, like other open, permissionless blockchains, Ethereum requires a form of on-chain value to incentivise transaction validation within the network (i.e. a form of payment for the network nodes that execute the operations).<sup>151</sup> This is where Ethereum's native cryptocurrency "ether" (ETH) comes into play. Ether does not only allow smart contracts to be built on the Ethereum platform (i.e. it fuels them<sup>152</sup>), but it also functions as a medium of exchange (specifically in the context of ITOs, as many tokens are bought with ether).

Like Bitcoin, Ethereum currently utilises a PoW consensus mechanism, but it is slowly moving towards the adoption of a PoS consensus mechanism<sup>153</sup>, better known as the Casper Protocol.<sup>154</sup>

Ethereum's development is promoted and supported by the "Ethereum Foundation"<sup>155</sup>, a Swiss non-profit organization, founded by Ethereum's inventors. A large bulk of ether was "pre-mined" (i.e. mined / created before the coin was officially launched to the public<sup>156</sup>) by its inventors and sold in a crowdsale to pay for development costs and fund the Ethereum Foundation.<sup>157</sup>

#### b. Ethereum runs on an open, permissionless blockchain

Just like Bitcoin, Ethereum is a prominent example of an open, permissionless blockchain. Anyone can join or leave the Ethereum network at will, without having to be pre-approved by any entity.

#### c. Ether (ETH) is directly convertible into fiat currency

Ether (ETH) can be bought with and converted into fiat currency on various cryptocurrency exchanges (e.g. Coinbase, Kraken, ...).

#### d. Ether (ETH) is a medium of exchange

Like Bitcoin, ether (ETH) is being accepted as a means of payment by a growing number of merchants (e.g. TapJets<sup>158</sup>, Overstock<sup>159</sup>, ...). It is therefore also a medium of exchange.

#### e. Ether (ETH) is a pseudo-anonymous coin

Just like Bitcoin, ether (ETH) can be categorised as a pseudo-anonymous or pseudonymous coin.<sup>160</sup>

<sup>150</sup> See: EY, "IFRS – Accounting for crypto-assets", March 2018, <http://eyfinancialservicesthoughtgallery.ie/wp-content/uploads/2018/03/EY-IFRS-Accounting-for-crypto-assets.pdf>, 4.

<sup>151</sup> *Ibid.*

<sup>152</sup> Cf. G. HILEMAN and M. RAUCHS, "Global Cryptocurrency Benchmarking Study", Cambridge Centre for Alternative Finance, 2017, [https://www.jbs.cam.ac.uk/fileadmin/user\\_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf](https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf), 17.

<sup>153</sup> That is, if the nodes in the network reach a consensus regarding this change. If they do not, a hard fork of the Ethereum blockchain could arise. See for more information on this concept further below. See also: <https://www.ethereum.org/ether>.

<sup>154</sup> See for example: A. ROSIC, "What is Ethereum Casper Protocol? Crash Course", November 2017, <https://blockgeeks.com/guides/ethereum-casper/>.

<sup>155</sup> See: <https://www.ethereum.org/foundation>.

<sup>156</sup> See: <https://www.investopedia.com/terms/p/premining.asp>.

<sup>157</sup> See: <https://www.ethereum.org/ether>.

<sup>158</sup> See: <https://www.tapjets.com>. See also: A. KAPLAN, "Who accepts Ethereum as payment 2018 (List of companies that accept Ethereum)", May 2018, <https://smartereum.com/2072/accepts-ethereum-payment-2018-list-companies-accept-ethereum-mon-may-28/>.

<sup>159</sup> See: P. RIZZO, "Ether, Litecoin and More: Overstock Now Accepts Cryptocurrencies as Payment", August 2017, <https://www.coindesk.com/ether-litecoin-overstock-now-accepts-cryptocurrencies-payment/>.

### 3.2.3. Ripple (XRP)

#### a. What is Ripple?

Ripple is an open-source, P2P decentralized digital payment platform that allows for near-instantaneous transfers of currency regardless of their form (e.g. US Dollar, Yen, Bitcoin, ...).<sup>161</sup> It was launched in 2012 by the private company Ripple (Labs), Inc.<sup>162</sup> Ripple (Labs), Inc., responsible for the further development of the Ripple protocol, is the first ever company to have received a “BitLicense” for an institutional use case of digital assets from New York’s Department of Financial Services.<sup>163</sup> It is also getting support from a number of big players in the financial services industry, such as Bank of America Merrill Lynch, Santander, etc.<sup>164</sup>

Following Ripple’s establishment, Ripple’s inventors launched the cryptocurrency XRP. XRP was built to become a bridge currency to allow financial institutions to settle cross-border payments a lot faster and cheaper than they can using the global payment networks that are in place today, which can be slow and involve multiple middlemen (i.e. banks).<sup>165</sup> However, in practice, Ripple’s payment platform does not need a bridge currency to actually work.<sup>166</sup>

According to Ripple, XRP can handle more than 1,500 transactions per second.<sup>167</sup> While it was initially developed and intended for enterprise use<sup>168</sup>, it has meanwhile been adopted by a large number of cryptocurrency users. Ripple (XRP) is not based on a PoW or a PoS mechanism to validate transactions, but it makes use of its own specific consensus protocol.<sup>169</sup>

The total supply of XRP has been fully “pre-mined” (or better: created upon the coin’s inception) by its inventors. At present, it is held as follows<sup>170</sup>:

- 8,102,265,714 XRP is held by Ripple (Labs), Inc.;
- 39,189,968,239 XRP has been distributed<sup>171</sup>; and
- 52,700,000,024 XRP has been placed in escrow to create certainty of XRP supply at any given time<sup>172</sup>.

<sup>160</sup> See *inter alia*: C. DANNEN, *Introducing Ethereum and Solidity – Foundations of Cryptocurrency and Blockchain Programming for Beginners*, Apress, 2017, 45; <https://ethereumprice.org/what-is-ethereum/>; A. MADEIRA, “How to make an anonymous ether transaction using WeiMixer”, May 2018, <https://www.cryptocompare.com/coins/guides/how-to-make-an-anonymous-ether-transaction/>.

<sup>161</sup> See: <https://ripple.com/xrp/>.

<sup>162</sup> See: Company Overview of Ripple Labs, Inc., <https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=235707311>.

<sup>163</sup> See: <https://ripple.com/insights/ripple-receives-new-yorks-first-bitlicense-institutional-use-case-digital-assets/>.

<sup>164</sup> See: <https://ripple.com/use-cases/banks/>.

<sup>165</sup> See: M. ORCUTT, “No, Ripple Isn’t the Next Bitcoin”, January 2018, <https://www.technologyreview.com/s/609958/no-ripple-isnt-the-next-bitcoin/>.

<sup>166</sup> *Ibid.*

<sup>167</sup> See: <https://ripple.com/xrp/>.

<sup>168</sup> *Ibid.*

<sup>169</sup> See: <https://ripple.com/build/xrp-ledger-consensus-process/>.

<sup>170</sup> See: <https://ripple.com/xrp/market-performance/>.

<sup>171</sup> It is said that Ripple’s founders still hold 20 billions XRP. See for example: M. ORCUTT, “No, Ripple Isn’t the Next Bitcoin”, January 2018, <https://www.technologyreview.com/s/609958/no-ripple-isnt-the-next-bitcoin/>.

<sup>172</sup> It should be noted that the XRP in this escrow account is indirectly owned by Ripple (Labs), Inc. See: <https://ripple.com/insights/ripple-escrows-55-billion-xrp-for-supply-predictability/>. On its website, Ripple states: “We use Escrow to establish 55 contracts of 1 billion XRP each that will expire on the first day of every month from months 0 to 54. As each contract expires, the XRP will become available for Ripple’s use. You can expect us to continue to use XRP for incentives to market makers who offer tighter spreads for payments and selling XRP to institutional investors. We’ll then return whatever is unused at the end of each month to the back of the escrow rotation. For example, if 500M XRP remain unspent at the end of the first month, those 500M XRP will be placed into a new escrow account set to expire in month 55. For comparison, Ripple has sold on average 300M XRP per month for the past 18 months.”

Unlike Ethereum’s inventors, Ripple’s inventors did not sell a portion of XRP via a crowdsale upon XRP’s creation to fund Ripple (Labs), Inc. The company was privately funded.<sup>173</sup>

At present, it is not fully transparent how XRP (which is mainly held by Ripple (Labs), Inc.) is or will be further distributed in the future.

#### b. Ripple runs on a public permissioned blockchain

Unlike Bitcoin and Ethereum, Ripple runs on a permissioned blockchain.<sup>174</sup> This is because Ripple (Labs) Inc., the company behind Ripple (XRP), determines who may act as a transaction validator on its network. The blockchain itself is considered public, as it can be accessed and viewed by anyone.

#### c. Ripple (XRP) is directly convertible into fiat currency

Like Bitcoin, XRP can be directly converted into fiat currency on various cryptocurrency exchanges (e.g. Kraken, LiteBit<sup>175</sup>, Anycoin Direct, Bitsane<sup>176</sup>, ...).

#### d. Ripple (XRP) is a medium of exchange

Ripple (XRP) is being accepted as a means of payment by a growing number of (online) merchants for various goods and services (e.g. e-cigarettes<sup>177</sup>, honey<sup>178</sup>, coffee<sup>179</sup>, ...) <sup>180</sup>. There is recently even buzz and speculation on the internet that Amazon might be looking to adopt Ripple in the near future.<sup>181</sup>

#### e. Ripple (XRP) is a pseudo-anonymous coin

Like Bitcoin, Ripple (XRP) can be qualified as a pseudo-anonymous coin.<sup>182</sup>

### 3.2.4. Bitcoin Cash (BCH)

#### a. What is Bitcoin Cash?

Bitcoin Cash (BCH) is decentralized P2P digital cash.<sup>183</sup> It was created on the 1<sup>st</sup> of August 2017 and is based on Bitcoin’s original SHA-256 PoW algorithm, yet with some changes to its underlying code. Bitcoin Cash is what is known in the crypto-community as a “hard fork” of the Bitcoin blockchain.<sup>184</sup> It is the result of two very different visions on the future of Bitcoin and the Bitcoin blockchain, whereby

<sup>173</sup> See for example: E. SPAVEN, “Online payment network Ripple Labs receives \$3.5 Million in new funding”, September 2014, <https://www.coindesk.com/online-payment-network-ripple-labs-receives-3-5m-new-funding/>.

<sup>174</sup> See: World Bank Group (H. NATARAJAN, S. KRAUSE and H. GRADSTEIN), “Distributed Ledger Technology (DLT) and blockchain”, 2017, FinTech note, no. 1. Washington, D.C., <http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf>, 12. See also: N. Bauerle, “What is the Difference Between Public and Permissioned Blockchains?”, 2017, <https://www.coindesk.com/information/what-is-the-difference-between-open-and-permissioned-blockchains/>.

<sup>175</sup> See: <https://www.litebit.eu/>.

<sup>176</sup> See: <https://bitsane.com/exchange/xrp-eur>.

<sup>177</sup> See for example: <https://vapourdepot.com/>.

<sup>178</sup> See for example: <http://drapis.com>.

<sup>179</sup> See for example: <https://www.cryptomercado.com>.

<sup>180</sup> See for an overview: <https://www.xrpchat.com/topic/5679-ripple-xrp-merchants-directory/>.

<sup>181</sup> See: J. P. NJUI, “Amazon Partnership Speculation High For Ripple (XRP) As Markets Go Crazy”, May 2018, <https://ethereumworldnews.com/amazon-partnership-speculation-high-for-ripple-xrp-as-markets-go-crazy/>.

<sup>182</sup> See: T. SAMEEH, “What If Ripple’s Transactions Can Be Fully Anonymous?”, May 2017, <http://www.livebitcoinnews.com/ripples-transactions-can-fully-anonymous/>.

<sup>183</sup> See: <https://www.bitcoincash.org/en/>.

<sup>184</sup> See: World Bank Group (H. NATARAJAN, S. KRAUSE, and H. GRADSTEIN), “Distributed Ledger Technology (DLT) and blockchain”, 2017, FinTech note, no. 1. Washington, D.C., <http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf>, 19; EY, “IFRS – Accounting for crypto-assets”, March 2018, <http://eyfinancialservicesthoughtgallery.ie/wp-content/uploads/2018/03/EY-IFRS-Accounting-for-crypto-assets.pdf>, 13.

the Bitcoin blockchain diverged into two potential paths forward.<sup>185</sup> In short, some Bitcoin developers wanted to raise the block size limit from 1MB to 8MB<sup>186</sup>, to reduce transaction fees and improve confirmation times, whilst others had different plans.<sup>187</sup> Because the community could not reach a consensus, the new cryptocurrency Bitcoin Cash was created.<sup>188</sup>

Like Bitcoin, Bitcoin Cash makes use of the PoW mechanism, which means that it can be mined. What is particular about Bitcoin Cash however, and is a direct result of the hard fork, is that anyone who held Bitcoin at the time Bitcoin Cash was created (*i.e.* 1<sup>st</sup> of August 2017 – 13:16 UTC) also became owner of the same amount of Bitcoin Cash.<sup>189</sup> Any Bitcoin acquired after that specific time follows the original path and does not include Bitcoin Cash.

#### b. Bitcoin Cash runs on an open, permissionless blockchain

In principle, a “hard fork” does not change the nature of a coin’s blockchain.<sup>190</sup> In other words, Bitcoin Cash also runs on an open permissionless blockchain, just like Bitcoin.

#### c. Bitcoin Cash is directly convertible into fiat currency

Like Bitcoin, Bitcoin Cash can be easily converted into fiat currency and vice versa through a number of cryptocurrency exchanges (e.g. Coinbase, Kraken, LiteBit, ...).

#### d. Bitcoin Cash is a medium of exchange

Bitcoin Cash can be used to pay for a growing array of goods and services (e.g. jewelry, food, gaming, telecom, ...) on a number of online market places and platforms (e.g. OpenBazaar<sup>191</sup>, the accept Bitcoin Cash initiative<sup>192</sup>). As a result, Bitcoin Cash can be qualified as a medium of exchange.

#### e. Bitcoin Cash is a pseudo-anonymous coin

Although Bitcoin Cash is a hard fork of Bitcoin, it does not differ that much from its original form. It is thus also a pseudo-anonymous coin.<sup>193</sup>

### 3.2.5. Litecoin (LTC)

#### a. What is Litecoin?

Like Bitcoin, Litecoin (LTC) is an open-source decentralized P2P cryptocurrency.<sup>194</sup> It was launched in October 2011 and is based on what is known as the Scrypt PoW algorithm, which utilises Bitcoin’s

<sup>185</sup> *Ibid.*

<sup>186</sup> A larger block size is capable of holding more transactions per block. See: S. BUCHKO, “How Long do Bitcoin Transactions Take?”, December 2017, <https://coincentral.com/how-long-do-bitcoin-transfers-take/>.

<sup>187</sup> *Ibid.*

<sup>188</sup> It is important to note that Bitcoin’s code is open source. It is managed and updated by volunteers who must achieve consensus among nodes for a change to be adopted. If no consensus can be reached the risk of a hard fork exists. See: EY, “IFRS – Accounting for crypto-assets”, March 2018, <http://eyfinancialservicesthoughtgallery.ie/wp-content/uploads/2018/03/EY-IFRS-Accounting-for-crypto-assets.pdf>, 4.

<sup>189</sup> *Ibid.* See also: <https://support.coinbase.com/customer/portal/articles/2911542>.

<sup>190</sup> World Bank Group (H. NATARAJAN, S. KRAUSE, and H. GRADSTEIN), “Distributed Ledger Technology (DLT) and blockchain”, 2017, FinTech note, no. 1. Washington, D.C., <http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf>, 19.

<sup>191</sup> See: <https://www.openbazaar.org>.

<sup>192</sup> See: <https://acceptbitcoin.cash/>.

<sup>193</sup> See *inter alia*: [https://exmo.com/en/news\\_view?id=1912](https://exmo.com/en/news_view?id=1912).

<sup>194</sup> See: <https://litecoin.com>.

original SHA-256 PoW algorithm.<sup>195</sup> Litecoin is often described as the ‘silver’ to Bitcoin’s gold.<sup>196</sup> Apart from the fact that it uses a different algorithm, it is different from Bitcoin in two ways.

Firstly, and this results from the use of the Script PoW algorithm, Litecoin offers a much faster transaction speed than Bitcoin. The time needed to generate a block on the Bitcoin BC is about ten minutes<sup>197</sup>, while the average block creation time on the Litecoin blockchain is approximately 2.5 minutes.<sup>198</sup>

Secondly, the total supply limit of Litecoin is with 84 million coins, much higher than the 21 million supply limit of Bitcoin.<sup>199</sup>

#### b. Litecoin runs on an open, permissionless blockchain

Just like Bitcoin, Litecoin runs on an open, permissionless blockchain. All that is needed to join the network is a download of the open-source software code.

#### c. Litecoin is directly convertible into fiat currency

Litecoin can be bought with fiat currency on a number of cryptocurrency exchanges (e.g. BTCDirect<sup>200</sup>, LiteBit, Coinbase, Anycoin Direct, ...) and can, on those exchanges, just as easily be exchanged for fiat currency.

#### d. Litecoin is a medium of exchange

Litecoin is accepted as a means of payment by a gradually growing number of online merchants.<sup>201</sup> Like Bitcoin, it thus also constitutes a medium of exchange.

#### e. Litecoin is a pseudo-anonymous coin

Just like Bitcoin, Litecoin is a pseudo-anonymous coin. Everyone can verify the chain of LTC transactions on the basis of the public ledger, which would make it technically possible to identify the coins sender and/or receiver.<sup>202</sup>

#### f. Litecoin and the case of “Atomic Swaps”

It should be noted that the Litecoin community recently introduced a new technology into the crypto-world that is being referred to as the “atomic swap”. Simply put, an atomic swap enables a P2P cross-chain exchange or trade of one cryptocurrency for another cryptocurrency, without the need of

<sup>195</sup> A. ROSIC, “What is Litecoin? A Basic Beginners Guide”, December 2017, <https://blockgeeks.com/guides/litecoin/>.

<sup>196</sup> B. PETERSON, “The founder of litecoin, a cryptocurrency that has gained 650% in 7 months, told us he’s worried about all the scams in the nascent market”, January 2018, <http://www.businessinsider.com/litecoin-founder-charlie-lee-on-bitcoin-and-the-cryptocurrency-bubble-2018-1?international=true&r=US&IR=T>; G. HILEMAN and M. RAUCHS, “Global Cryptocurrency Benchmarking Study”, Cambridge Centre for Alternative Finance, 2017, [https://www.jbs.cam.ac.uk/fileadmin/user\\_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf](https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf), 17.

<sup>197</sup> A transaction generally needs six confirmations or ‘blocks’ before its processed. As a result, the time needed to confirm a transaction on the Bitcoin blockchain normally averages around one hour. However, due to Bitcoin’s rise in popularity, congestions have arisen on the Bitcoin network. In some cases, transaction times have been reported to exceed several hours. See for example: S. BUCHKO, “How Long do Bitcoin Transactions Take?”, December 2017, <https://coincentral.com/how-long-do-bitcoin-transfers-take/>.

<sup>198</sup> It has been argued that the enabling of faster transactions might pose a security issue, since less thorough checks of the data are required. See: J. MARTINDALE, “What is Litecoin? Here’s everything you need to know”, January 2018, <https://www.digitaltrends.com/computing/what-is-litecoin/>.

<sup>199</sup> *Ibid.*

<sup>200</sup> See: <https://btcdirect.eu/>.

<sup>201</sup> See for an overview of online merchants that accept payments in Litecoins: <https://litecoin.com/services#merchants>.

<sup>202</sup> Cf. F. ETTO, “Know Your Coins: Public vs. Private Cryptocurrencies”, September 2017, <https://www.nasdaq.com/article/know-your-coins-public-vs-private-cryptocurrencies-cm849588>.

a third-party.<sup>203</sup> For example, if Anna has one Bitcoin and she wants 100 Litecoins in return, she would normally have to go through an exchange (*i.e.* a third-party) and pay certain fees to get this trade done. Suppose that Jeff owns 100 Litecoins and he instead wants one Bitcoin, then with an atomic swap Anna and Jeff could simply trade their Coins with one another.<sup>204</sup> Now, in practice an atomic swap is of course not so easy.

First of all, since it is presently still in its infancy, the implementation of the atomic swap technology requires a lot of IT-knowledge. For example, a link has to be made between the two cryptocurrency blockchains, which requires the implementation of an IT-protocol known in the crypto-community as the “Lightning Protocol”.<sup>205</sup> In addition, both blockchains have to share the same cryptographic function (for example the SHA-256 function) in order for the atomic swap to be possible.<sup>206</sup> While we are not there yet in terms of user friendly cross-chain trading, the emergence of the atomic swap technology brings forth a whole new set of challenges.

### 3.2.6. Stellar (XLM)

#### a. What is Stellar?

Like Ripple, Stellar is an open-source, distributed payments infrastructure. Stellar was created in 2014 by one of Ripple’s founding fathers.<sup>207</sup> Its goal is to connect people to low-cost financial services to fight poverty and develop individual potential.<sup>208</sup> Stellar can also be used to build smart contracts.<sup>209</sup> It is not based on a PoW or PoS consensus mechanism, but has its own specific consensus protocol.

Stellar is home to the cryptocurrency Lumen (XLM). In short, Lumens are used to pay for transactions on the Stellar network; they contribute to the ability to move money around the world and to conduct transactions between different currencies quickly and securely.<sup>210</sup>

Stellar’s development is supported by the non-profit organization Stellar.org (incorporated in 2014 as a non-stock nonprofit corporation in the U.S. State of Delaware), which contributes to the development of tools and social good initiatives around the Stellar network and financial inclusion.<sup>211</sup> Its employees contribute code to the network, but the network itself is said to be completely independent of the organization.<sup>212</sup>

Similar to Ripple’s cryptocurrency XRP, the total supply of Stellar Lumens is “pre-mined”. It is held by Stellar.org who has been given the task to distribute Lumens *for free*, in the following manner<sup>213</sup>:

- 50% is to be given away to individuals (via a direct sign-up program);

<sup>203</sup> See: R. ROSE O’LEARY, “Atomic Action: Will 2018 Be the Year of the Cross-Blockchain Swap?”, January 2018, <https://www.coindesk.com/atomic-action-will-2018-year-cross-blockchain-swap/>.

<sup>204</sup> A recent test case completed by the inventor of Litecoin, Mr Charlie Lee, shows that atomic swaps between Litecoin and Bitcoin are indeed possible. See: J. BUCK, “First BTC-LTC Lightning Network Swap Completed, Huge Potential”, November 2017, <https://cointelegraph.com/news/first-btc-ltc-lightning-network-swap-completed-huge-potential>.

<sup>205</sup> A. ROSIC, “What is Litecoin? A Basic Beginners Guide”, December 2017, <https://blockgeeks.com/guides/litecoin/>.

<sup>206</sup> See: B. ASOLO, “What are Atomic Swaps?”, May 2018, <https://www.cryptocompare.com/coins/guides/what-are-atomic-swaps/>. This means that theoretically, swaps between a number of Cryptocurrencies could be possible.

<sup>207</sup> See *inter alia*: C. ADAMS, “Stellar Lumens Vs Ripple”, March 2018, <https://www.investinblockchain.com/stellar-lumens-vs-ripple/>; S. TOWN, “Introduction to Stellar Lumens (XLM) – The Future of Banking”, April 2018, <https://cryptoslate.com/stellar-lumens/>.

<sup>208</sup> See: <https://www.stellar.org/about/>. It should be noted that Stellar’s primary target audience (*i.e.* the individual) is thus totally different from Ripple’s (*i.e.* financial institutions).

<sup>209</sup> See: <https://www.stellar.org/developers/guides/walkthroughs/stellar-smart-contracts.html>.

<sup>210</sup> See: <https://www.stellar.org/lumens/>.

<sup>211</sup> See: <https://www.stellar.org/about/mandate/>.

<sup>212</sup> See: <https://www.stellar.org/how-it-works/stellar-basics/>.

<sup>213</sup> See: <https://www.stellar.org/about/mandate/>.

- 25% is to be given away to partners (via a specific partnership program);
- 20% is given away to Bitcoin and XRP holders; and
- 5% is reserved for Stellar.org’s operational expenses.

The actual distribution is not conducted at once, but over time in a number of rounds.

#### b. Stellar runs on a permissionless blockchain

Unlike Ripple, Stellar runs on a permissionless blockchain. Anyone can join the network at will and, if certain conditions are met, validate transactions without having to be pre-approved or vetted by any central administrator.<sup>214</sup>

#### c. Lumens (XLM) are directly convertible into fiat currency

Lumens (XLM) can be directly converted into fiat currency through cryptocurrency exchanges such as LiteBit (up to a maximum amount of EUR 500 (per transaction)) or Kraken.

#### d. Lumens (XLM) are NOT a true medium of exchange yet

At present, so it seems, Lumens (XLM) can only be used to pay for promotional Stellar stickers<sup>215</sup>, breakfast at a local breakfast bar in Arkansas<sup>216</sup> and sprouts<sup>217</sup>. While this proves that they are gradually being accepted as a means of payment, they are not a true medium of exchange yet, at least not if you compare them to the coins discussed above.

#### e. Lumens (XLM) are pseudo-anonymous coins

All transactions on the Stellar network are public, but they cannot be linked easily to the identities of their users.<sup>218</sup> As a result, Stellar Lumens (XLM) can be qualified as pseudo-anonymous coins.

### 3.2.7. Cardano (ADA)

#### a. What is Cardano?

Like Ethereum, Cardano is designed and being further developed as a platform on top of which smart contracts and decentralized applications (so-called “Dapps”) can be run.<sup>219</sup> The Cardano project began in 2015<sup>220</sup>, and was officially released to the public in September 2017<sup>221</sup>. It is based on what is known as the Ouroboros PoS algorithm.<sup>222</sup>

<sup>214</sup> See: <https://www.stellar.org/how-it-works/stellar-basics/>.

<sup>215</sup> See: <https://stellar.shop/products>.

<sup>216</sup> See: <https://www.preludebreakfast.com>.

<sup>217</sup> See: <https://www.sproutgrowers.world/product/sprout-grower/>.

<sup>218</sup> See: <https://www.stellar.org/how-it-works/stellar-basics/>.

<sup>219</sup> See: <https://www.cardano.org/en/what-is-cardano/>.

<sup>220</sup> See: <https://www.cardano.org/en/philosophy/>.

<sup>221</sup> E. POSNAK, “On the Origin of Cardano”, December 2017, <https://medium.com/on-the-origin-of-smart-contract-platforms/on-the-origin-of-cardano-a6ce4033985c>.

<sup>222</sup> See: A. KIAYIAS, A. RUSSEL, B. DAVID and R. OLIYNYKOV, “Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol”, August 2017, [https://iohk.io/research/papers/?\\_hstc=64163184.47e0ede3cd3368ac41d33e513fea0c1b.1525905532910.1527544936508.1527699072699.9&\\_hssc=64163184.7.1527699072699&\\_hsfp=2761973715#9BKRHCSI](https://iohk.io/research/papers/?_hstc=64163184.47e0ede3cd3368ac41d33e513fea0c1b.1525905532910.1527544936508.1527699072699.9&_hssc=64163184.7.1527699072699&_hsfp=2761973715#9BKRHCSI).



The Cardano platform is home to the open source decentralized cryptocurrency Ada (ADA).<sup>223</sup> Ada can be used to send and receive digital funds. It fuels the Cardano platform, just like the currency “ether” fuels the Ethereum platform.

In short, Cardano aims to improve scalability, security, governance, and interoperability with traditional financial systems and regulations, by learning from and improving on lessons learned in the Bitcoin and Ethereum communities.<sup>224</sup>

What distinguishes Cardano from Ethereum, and from many other cryptocurrencies, is that it is (one of the first) blockchain projects to be developed and designed from a scientific philosophy by a team of leading academics and engineers.<sup>225</sup> Another notable difference is that, at present, the cryptocurrency Ada (ADA) can only be stored in Cardano’s own digital wallet Daedalus.<sup>226</sup>

The Cardano project currently has three main contributors that each have separate roles:

- the Cardano foundation, based in Switzerland, which aims to standardise, protect and promote the Cardano technology and eco-system;
- IOHK, a blockchain engineering company responsible for building the Cardano blockchain; and
- Emurgo, an entity responsible for the fostering of commercial applications being built upon the Cardano ecosystem.

Similar to Ethereum (*cf.* ether), a good number of Ada was “pre-mined” (i.e. mined / created before the coin was launched to the public) by its inventors and sold in a crowdsale to pay for development costs.<sup>227</sup>

#### b. Cardano runs both permissionless and permissioned blockchains

Cardano’s Ouroboros PoS algorithm allows the platform to run both permissionless and permissioned blockchains.<sup>228</sup>

#### c. Ada (ADA) is directly convertible into fiat currency

The currency Ada (ADA) can be directly converted into fiat currency. However, we found that, at present, only one cryptocurrency exchange offers the option to directly convert Ada (ADA) into Euro, being LiteBit and only up to a maximum amount of EUR 500 (per transaction).

Ada can, on the contrary, easily be exchanged for other cryptocurrencies (for example through an exchange such as Bittrex<sup>229</sup> or Binance). These cryptocurrencies can then be converted into fiat currency.

#### d. Ada (ADA) is NOT a true medium of exchange yet

Our research shows that, at present, Ada can only be used to pay for a very limited number of services (e.g. Hotel Ginebra Barcelona accepts payment in Ada<sup>230</sup>). While this proves that Ada is gradually

<sup>223</sup> See: <https://www.cardano.org/en/what-is-cardano/>.

<sup>224</sup> E. POSNAK, “On the Origin of Cardano”, December 2017, <https://medium.com/on-the-origin-of-smart-contract-platforms/on-the-origin-of-cardano-a6ce4033985c>.

<sup>225</sup> See: <https://www.cardano.org/en/what-is-cardano/>.

<sup>226</sup> See: <https://www.cardano.org/en/the-daedalus-wallet/>.

<sup>227</sup> See: <https://cardanodocs.com/cardano/monetary-policy/>.

<sup>228</sup> See: <https://whycardano.com>. See also: A. Ramesh, “Features of various Blockchains: A Comparison”, February 2018, <https://www.xoken.org/blog/features-of-various-blockchains-a-comparison/>.

<sup>229</sup> See: <https://bittrex.com/home/markets>.

<sup>230</sup> See: <https://www.hotelginebra.com.es/welcome/ada/>.

being accepted as a means of payment, it is not a true medium of exchange yet, at least not if you compare it to the coins discussed above. This could however change fairly quickly.<sup>231</sup>

#### e. Ada (ADA) is a pseudo-anonymous coin

Just like the cryptocurrencies analysed above, Ada can be qualified as a pseudo-anonymous coin.<sup>232</sup> It is interesting to note however – and as far as we could establish, unparalleled – that know your customer (KYC) standards were applied during the initial offering of Ada.<sup>233</sup>

### 3.2.8. IOTA (MIOTA)

#### a. What is IOTA?

IOTA, launched in 2016<sup>234</sup>, is an open-source eco-system where people and machines can transfer value (i.e. money) and/or data without any transaction fees in a trustless, permissionless, and decentralized environment.<sup>235</sup>

In short, IOTA employs specific technology that is said to be more scalable than the technology behind most other coins, and promises faster transaction speeds.<sup>236</sup> Like the cryptocurrencies analysed above, IOTA is based on distributed ledger technology. However, unlike those other cryptocurrencies, IOTA's distributed ledger does not consist of transactions grouped into (transaction) "blocks" and stored into sequential chains (i.e. it is not a "blockchain"), but of a stream of individual transactions entangled together.<sup>237</sup> IOTA is based on what is known as a directed acyclic graph (DAG).<sup>238</sup> Because transactions are entangled together, this technology is also being referred to as the "Tangle".<sup>239</sup>

Instead of requiring miners to perform computational PoW and validate transaction blocks in exchange for newly "mined" coins, IOTA's network participants create a consensus themselves by validating two previous transactions each time they wish to make a new transaction.<sup>240</sup>

At present, IOTA is still very much in its infancy. This is reflected, *inter alia*, by the fact that in order to fully secure the network all transactions have to be digitally signed by a special network node (i.e. the "Coordinator"<sup>241</sup>). Because this affects the network's true decentralized nature, IOTA's development team is working hard on an update to remove this special node by the end of 2018.<sup>242</sup>

The IOTA eco-system is being further developed, supported, promoted and maintained by the "IOTA Foundation"<sup>243</sup>, a German non-profit foundation, founded by IOTA's inventors. The total supply of

<sup>231</sup> Cf. A. ANTONOVICI, "Cardano's Emurgo and SK's Metaps Plus Partner to Accept ADA", May 2018, <https://cryptovest.com/news/cardanos-emurgo-and-sks-metaps-plus-partner-to-accept-ada/>.

<sup>232</sup> See: <https://cardanodocs.com/introduction/#cryptocurrency-basics>.

<sup>233</sup> See: <https://www.cardano.org/en/ada-distribution-audit/>.

<sup>234</sup> X, "An introduction to IOTA", 2017, <https://iotasupport.com/whatisiota.shtml>.

<sup>235</sup> See: <https://www.iota.org/get-started/faqs>.

<sup>236</sup> *Ibid.*

<sup>237</sup> *Ibid.*

<sup>238</sup> S. LEE, "Explaining Directed Acyclic Graph (DAG), The Real Blockchain 3.0", January 2018, <https://www.forbes.com/sites/shermanlee/2018/01/22/explaining-directed-acyclic-graph-dag-the-real-blockchain-3-0/#68781282180b>.

<sup>239</sup> See: <https://www.iota.org/get-started/faqs>.

<sup>240</sup> See: S. POPOV, "The Tangle", October 2017, [http://iotatoken.com/IOTA\\_Whitepaper.pdf](http://iotatoken.com/IOTA_Whitepaper.pdf). See also: L. TENNANT, "Improving the Anonymity of the IOTA Cryptocurrency", October 2017, [https://assets.ctfassets.net/r1dr6vzfxhev/6StLLAy9b26eyUG8SGQqeu/e30c20f91e77e54d88b7644658912c7d/Improving\\_the\\_Anonymity\\_of\\_the\\_IOTA\\_Cryptocurrency.pdf](https://assets.ctfassets.net/r1dr6vzfxhev/6StLLAy9b26eyUG8SGQqeu/e30c20f91e77e54d88b7644658912c7d/Improving_the_Anonymity_of_the_IOTA_Cryptocurrency.pdf), 1.

<sup>241</sup> See: <https://www.iota.org/get-started/faqs>.

<sup>242</sup> *Ibid.*

<sup>243</sup> See: <https://www.ethereum.org/foundation>.

IOTA was created and released to a number of so-called “founder addresses”.<sup>244</sup> The majority of it was sold by IOTA’s inventors in a crowdsale to pay for development costs and fund the IOTA Foundation.<sup>245</sup>

#### b. IOTA runs on a permissionless distributed ledger

IOTA is not based on blockchain technology, but constitutes a different application of distributed ledger technology. It is – to put it in the words of its developers – envisaged to be(come) the *public* and *permissionless* backbone protocol for the internet of things that enables true interoperability between all devices.<sup>246</sup>

#### c. IOTA is directly convertible into fiat currency

The cryptocurrency IOTA (MIOTA) can be directly converted into fiat currency (such as Euro). However, our research shows that, at present, only one cryptocurrency exchange offers the option to directly convert IOTA (MIOTA) into Euro, being CoinFalcon<sup>247</sup>.

IOTA can, on the contrary, easily be exchanged for other cryptocurrencies (for example through an exchange such as Binance). These cryptocurrencies can then be converted into fiat currency.

#### d. IOTA is NOT a medium of exchange

It seems that there are currently no (online) merchants that accept IOTA as a means of payment for certain goods or services. IOTA is thus not a medium of exchange. It cannot be ruled out however, that it may become one in the (near) future.<sup>248</sup>

#### e. IOTA is a pseudo-anonymous coin

Despite IOTA’s unique eco-system, like most cryptocurrencies it has a transparent and publicly available ledger, meaning a IOTA user’s counterparty see that user’s IOTA balance and parts of IOTA’s transaction history.<sup>249</sup> Just like Bitcoin, IOTA can thus be qualified as a pseudo-anonymous coin.

### 3.2.9. NEO (NEO)

#### a. What is NEO?

Similar to Ethereum and Cardano, NEO is an open-source blockchain platform on top of which smart contracts and decentralized applications (so-called “Dapps”) can be run. NEO, sometimes referred to as the “Chinese Ethereum”<sup>250</sup>, was originally launched under the name “Antshares” in February 2014.<sup>251</sup> The project was rebranded “NEO” in June 2017.<sup>252</sup>

<sup>244</sup> See: X, “IOTA Coin Review”, January 2018, <https://hackernoon.com/iota-coin-review-6a1c73c5cfa3>.

<sup>245</sup> X, “An introduction to IOTA”, 2017, <https://iotasupport.com/whatisiota.shtml>.

<sup>246</sup> See: <https://www.iota.org/get-started/faqs>.

<sup>247</sup> See: <https://coinfalcon.com>.

<sup>248</sup> Cf. L. TENNANT, “Improving the Anonymity of the IOTA Cryptocurrency”, October 2017, [https://assets.ctfassets.net/r1dr6vzfxhev/6StLLAy9b26eyUG8SGOqeu/e30c20f91e77e54d88b7644658912c7d/Improving\\_the\\_Anonymity\\_of\\_the\\_IOTA\\_Cryptocurrency.pdf](https://assets.ctfassets.net/r1dr6vzfxhev/6StLLAy9b26eyUG8SGOqeu/e30c20f91e77e54d88b7644658912c7d/Improving_the_Anonymity_of_the_IOTA_Cryptocurrency.pdf), 2.

<sup>249</sup> *Ibid.*

<sup>250</sup> See for example: J. TUWINER, “Introduction to NEO – An Open Network For Smart Economy”, April 2018, <https://cryptoslate.com/introduction-to-neo-an-open-network-for-smart-economy/>.

<sup>251</sup> See: A. MOSKOV, “Cryptocurrency Industry Spotlight: Who is NEO’s Da Hongfei?”, January 2018, <https://coincentral.com/cryptocurrency-industry-spotlight-neos-da-hongfei/>.

<sup>252</sup> See: N. LEVENSON, “NEO versus Ethereum: Why NEO might be 2018’s strongest cryptocurrency”, December 2017, <https://hackernoon.com/neo-versus-ethereum-why-neo-might-be-2018s-strongest-cryptocurrency-79956138bea3>.

In short, the NEO project is aimed at digitising assets and automating the management of digital assets, in order to create a so-called “smart economy” (i.e. an economy where parties can agree on a contract without the need to trust each other).<sup>253</sup>

Just like Ethereum (*cf.* “ether”), NEO itself is technically not a cryptocurrency. NEO’s native currency is called “GAS”. In simple terms, GAS is a fee to be paid to be allowed to utilise NEO’s network. One could in fact say that it “fuels” the platform. What is particular about the NEO platform (and distinguishes it from the Ethereum and Cardano platforms) is that holding the digital value “NEO” (which could best be described as some sort of hybrid crypto-asset) automatically generates an amount of GAS over time.<sup>254</sup>

NEO is based on a consensus mechanism known in the crypto-community as the delegated Byzantine Fault Tolerance (dBFT) algorithm, which could potentially support 10.000 transactions per second.<sup>255</sup>

The total supply of NEO was “pre-mined”<sup>256</sup>; half of it was sold in a crowdsale and the other half is managed by the NEO Council (i.e. group of the project’s founders) to support development and maintenance of the NEO ecosystem.<sup>257</sup>

#### b. NEO runs on a permissioned blockchain

In order to become a transaction validator (i.e. a node) on the NEO network, a validator candidate has to be (i) selected by NEO’s development team and (ii) voted in by the NEO community (i.e. those who hold NEO).<sup>258</sup> These characteristics are typical for a permissioned blockchain.

#### c. NEO is directly convertible into fiat currency, GAS is not

NEO can be directly converted into fiat currency. However, our research shows that, at present, only one cryptocurrency exchange offers the option to directly convert NEO into Euro, being Anycoin Direct<sup>259</sup>.

NEO’s native currency GAS can presently not be directly converted into fiat currency.

Both NEO and GAS can, however, easily be exchanged for other cryptocurrencies (for example through an exchange such as Bittrex). These cryptocurrencies can then be converted into fiat currency.

#### d. NEO’s GAS is NOT a medium of exchange

While NEO is working very closely with big tech companies like Microsoft<sup>260</sup>, its native currency GAS is not a medium of exchange (nor is NEO itself). Contrary to a number of other coins discussed above,

<sup>253</sup> See: <https://neo.org>. See also: M. LERIDER, “What is NEO Smart Economy?”, August 2017, <https://medium.com/@MalcolmLerider/what-is-neo-smart-economy-381a4c6ee286>.

<sup>254</sup> GAS itself can also be individually acquired, for example on the Cryptocurrency Exchange Binance (<https://www.binance.com/>).

<sup>255</sup> See: <http://docs.neo.org/en-us/index.html>.

<sup>256</sup> See *inter alia*: S. KHATWANI, “NEO Cryptocurrency: Everything You Need to Know about China Ethereum”, December 2017, <https://coinsutra.com/neo-cryptocurrency/>; X, “What is NEO, and what is GAS?”, September 2017, <https://hackernoon.com/what-is-neo-and-what-is-gas-5b9828a1aa65>.

<sup>257</sup> X, “What is NEO, and what is GAS?”, September 2017, <https://hackernoon.com/what-is-neo-and-what-is-gas-5b9828a1aa65>.

<sup>258</sup> See *inter alia*: X, “A Definitive Guide To NEO (2nd Edition)”, January 2018, <http://storeofvalueblog.com/posts/a-definitive-guide-to-neo/>; CITY OF ZION, “Coopetition: A New Approach to Decentralization”, December 2017, <https://medium.com/proof-of-working/decentralization-from-coopetition-b10d7ce3b9d>.

<sup>259</sup> It should be noted that “on paper” the cryptocurrency exchange Bitfinex (<https://www.bitfinex.com>) also offers the option to convert NEO into Euro. However, in practise it proves to be very difficult (to impossible) to actually withdraw such funds from the platform.

<sup>260</sup> See for example: H. NASEER, “NEO Launches Dev Competition with \$490,000 Prize Pool, Co-organized by Microsoft”, November 2017, <https://cryptovest.com/news/neo-launches-dev-competition-with-490000-prize-pool-co-organized-by-microsoft/>; W. SUBERG, “NEO

our research did not reveal any online merchants willing to accept NEO's coins as a means of payment. Some argue that GAS is in fact not really intended to be a true medium of exchange.<sup>261</sup> However, the same was also said for Ethereum's currency ether (ETH). With that in mind, it cannot be entirely ruled out that GAS (or even NEO itself) may still become a medium of exchange in the future.

#### e. NEO's GAS is a pseudo-anonymous coin

In essence, NEO's GAS could be qualified as a pseudo-anonymous or pseudonymous coin, just like the coins analysed above. However, NEO's core developers are currently actively working on a concept that would allow coders of smart contracts to tie a so-called "digital identity" to a real world identity.<sup>262</sup> It is not entirely inconceivable – yet at this time still highly unclear – that this technology will also impact GAS's pseudo-anonymous character.<sup>263</sup>

### 3.2.10. Monero (XMR)

#### a. What is Monero?

Monero (XMR) is an open-source P2P cryptocurrency "*with a focus on private and censorship-resistant transactions*".<sup>264</sup> It was launched in April 2014<sup>265</sup> and is based on what is known as the CryptoNote<sup>266</sup> PoW algorithm.

Monero has been specifically developed to allow its users to execute transactions in full anonymity. It is said to be cryptographically private by default.<sup>267</sup> In particular, it uses cryptography to shield both sending and receiving addresses (*i.e.* so-called 'keys'<sup>268</sup>), as well as transacted amounts.

Monero (XMR) is characterized as being fully fungible. This means that two units of XMR can always be mutually substituted and there can be no blacklisting of certain units of XMR by vendors or exchanges due to their association in previous transactions.<sup>269</sup> Non-fungible cryptocurrencies, like Bitcoin and Litecoin, are theoretically susceptible to blacklisting; if they have been used for an illegal purpose in the past, then such history will be contained in the blockchain forever.

Unlike some other Coins, Monero (XMR) has not been pre-mined.

#### b. Monero runs on a permissionless blockchain

Just like Bitcoin, Monero (XMR) runs on a permissionless blockchain.<sup>270</sup> Anyone can join the network at will, without having to be pre-approved or vetted by any central administrator.

---

DevCon Sees Microsoft Judge Network's Potential Uses", November 2017, <https://cointelegraph.com/news/neo-devcon-sees-microsoft-judge-networks-potential-uses>.

<sup>261</sup> See: [https://www.reddit.com/r/NEO/comments/6su31n/here\\_are\\_some\\_things\\_you\\_should\\_know\\_if\\_you\\_are/](https://www.reddit.com/r/NEO/comments/6su31n/here_are_some_things_you_should_know_if_you_are/); M. LERIDER, "Clarification on NEO, GAS and Consensus Nodes", August 2017, <https://medium.com/@MalcolmLerider/clarification-on-neo-gas-and-consensus-nodes-aa94d4f4b09>.

<sup>262</sup> See: <https://neo.org>.

<sup>263</sup> See for a more elaborate analysis and discussion of this technology: K. SOETEMAN, "Werking dBft via Neo in kaart gebracht", February 2018, <https://www.computable.nl/artikel/achtergrond/technologie/6306817/5182002/werking-dbft-via-neo-in-kaart-gebracht.html>.

<sup>264</sup> See: <https://getmonero.org/get-started/what-is-monero/>.

<sup>265</sup> See: <https://getmonero.org/resources/about/>. See also: C. BOVAIRD, "What to know before trading Monero", May 2017, <https://www.coindesk.com/what-to-know-before-trading-monero/>.

<sup>266</sup> See: <https://cryptonote.org/whitepaper.pdf>.

<sup>267</sup> A. ZAINUDDIN, "Guide on Privacy Coins: Comparison of Anonymous Cryptocurrencies", 2017, <https://masterthecrypto.com/privacy-coins-anonymous-cryptocurrencies/>.

<sup>268</sup> Also see above under 2.1.2. How a blockchain works: the basics.

<sup>269</sup> See: <https://getmonero.org/resources/moneropedia/fungibility.html>.

<sup>270</sup> See: <https://getmonero.org/resources/moneropedia/cryptocurrency.html>.

c. **Monero is directly convertible into fiat currency**

Monero (XMR) can be directly converted into fiat currency on a number of cryptocurrency exchanges (e.g. LiteBit, Anycoin Direct, Kraken, ...).

d. **Monero is a medium of exchange**

Monero is accepted as a means of payment by a gradually growing number of online merchants.<sup>271</sup> Like Bitcoin, it thus also constitutes a medium of exchange.

e. **Monero is an anonymous coin**

On a fully transparent blockchain, such as the Bitcoin or Ethereum blockchain, transactions are always openly verifiable and traceable by anyone. In practice – though this will be no easy task – the sending and receiving addresses for such transactions could also be linked to a person's real-life identity.<sup>272</sup> This is where Monero advocates to be different. It positions itself as a secure, private and untraceable cryptocurrency.

This high standard of anonymity is achieved using two different techniques:

- Ring Confidential Transactions (“**RingCT**”); and
- Stealth addresses.

i. *Ring Confidential Transactions*

Firstly, Monero makes use of so-called Ring Confidential Transactions. RingCT combine the technique of ring signatures and what is referred to in the crypto-community as the confidential transactions concept:

- Ring signatures combine or 'mix' a user's account keys with public keys obtained from Monero's blockchain to create, what could be called a 'ring' of possible signers<sup>273</sup>, meaning outside observers cannot link a signature to a specific user.<sup>274</sup> Combined with stealth addresses (see below) they allow to fully obscure the identify of both senders and recipients of XMR;
- Confidential transactions add another layer of privacy to the 'mix' by also concealing the amount of each transaction.<sup>275</sup> Without revealing the actual numbers, they include a cryptographic proof that the sum of the input amounts is the same as the sum of the output amounts.<sup>276</sup>

ii. *Stealth Addresses*

Secondly, and in addition to RingCT, Monero also makes use of stealth addresses. Stealth addresses are randomly generated, one-time addresses created for each transaction made by the sender on behalf of the recipient. All payments sent to the recipient are routed through these addresses, ensuring there are no links on the blockchain between the sender's and the recipient's address.<sup>277</sup> In

<sup>271</sup> See for an overview of online merchants that accept payments in Monero: <https://getmonero.org/community/merchants/>.

<sup>272</sup> N. VANDEZANDE, *Virtual currencies: a legal framework*, Antwerp, Intersentia, 2018, 57. Also see above under 3.2.1. Bitcoin (BTC).

<sup>273</sup> See for more information on this concept: <https://people.csail.mit.edu/rivest/pubs/RST01.pdf>.

<sup>274</sup> C. BOVAIRD, “What to know before trading Monero”, May 2017, <https://www.coindesk.com/what-to-know-before-trading-monero/>.

<sup>275</sup> See for more information on this concept: [https://people.xiph.org/~greg/confidential\\_values.txt](https://people.xiph.org/~greg/confidential_values.txt).

<sup>276</sup> A. ZAINUDDIN, “Guide on Privacy Coins: Comparison of Anonymous Cryptocurrencies”, 2017, <https://masterthecrypto.com/privacy-coins-anonymous-cryptocurrencies/>.

<sup>277</sup> *Ibid.*

---

other words, stealth addresses prevent linkability on the blockchain. However, without the use of RingCT, the original sender of the coins would still be able to trace the coins if they would be moved by the recipient by identifying outputs on the blockchain. RingCT masks these outputs, making the transaction entirely untraceable.<sup>278</sup>

### *iii. The Kovri-Project*

It should be noted that the community of (core) developers and cryptography experts behind Monero is currently working on a project to add yet another layer of privacy to the Monero ecosystem by routing and encrypting XMR transactions via I2P Invisible Internet Project nodes.<sup>279</sup> The use of I2P will obfuscate a transactor's IP address and provide further protection against network monitoring.

This project, of which an alpha version is currently in the works, is better known in the crypto-community as the Kovri-project.

---

<sup>278</sup> See: C. BOVAIRD, "What to know before trading Monero", May 2017, <https://www.coindesk.com/what-to-know-before-trading-monero/>.

<sup>279</sup> "I2P is an anonymous overlay network - a network within a network. It is intended to protect communication from dragnet surveillance and monitoring by third parties such as Internet Service Providers" – see: <https://geti2p.net/en/>.

## Box 1: The Kovri-project

*"Kovri uses (...) encryption and (...) routing to create a private, protected overlay-network across the internet. This overlay-network provides users with the ability **to effectively hide their geographical location and internet IP address**. Essentially, Kovri covers an application's internet traffic to make it anonymous within the network." (own emphasis added)*

Source: <https://getkovri.org>.

## 3.2.11. Dash (DASH)

## a. What is Dash?

Dash (DASH), formerly known as Darkcoin<sup>280</sup>, is an open source P2P privacy-centric cryptocurrency.<sup>281</sup> It was first launched in January 2014 and is based on what is known as the X11 PoW algorithm.<sup>282</sup> What is specific to Dash, and makes it different from most other coins, is that it has a two-tier network. Dash's blockchain is secured via so-called "masternodes" in addition to the PoW done by miners.<sup>283</sup>

In short, a masternode is a server connected to the Dash network which guarantees a certain minimum level of performance and functionality to perform certain tasks related to PrivateSend and InstantSend (Dash's anonymity and instant transaction features).<sup>284</sup>

Transactions with traditional cryptocurrencies can be very time-consuming (i.e. they can take anywhere between a few minutes and more than one hour). This is due to the fact that enough blocks have to pass to ensure that a transaction is irreversible and at the same time not an attempt to double-spend money that has already been spent.<sup>285</sup> Dash tackles this issue utilising its masternode network. Masternodes can be called upon to form voting quorums to check whether or not a submitted transaction is valid and if it is, *"the masternodes 'lock' the inputs for the transaction and broadcast this information to the network, effectively promising that the transaction will be included in subsequently mined blocks and not allowing any other spending of these inputs during the confirmation time period"*.<sup>286</sup> As a result Dash is said to be able to compete with nearly instantaneous transaction systems, such as credit cards.<sup>287</sup>

## b. Dash runs on an open, permissionless blockchain

Like Monero, Dash runs on a permissionless blockchain.<sup>288</sup> Anyone can join the network at will, without having to be pre-approved or vetted by any central administrator.

## c. Dash is directly convertible into fiat currency

Dash (DASH) can be directly converted into fiat currency through various cryptocurrency exchanges (e.g. Anycoin Direct, Kraken, ...).

<sup>280</sup> S. HIGGINS, "How True Anonymity Made Darkcoin King of the Altcoins", May 2014, <https://www.coindesk.com/true-anonymity-darkcoin-king-altcoins/>.

<sup>281</sup> See Dash whitepaper: <https://github.com/dashpay/dash/wiki/Whitepaper>.

<sup>282</sup> See: <https://docs.dash.org/en/latest/introduction/features.html>.

<sup>283</sup> See: <https://docs.dash.org/en/latest/masternodes/understanding.html>.

<sup>284</sup> *Ibid.*

<sup>285</sup> See: <https://docs.dash.org/en/latest/introduction/features.html#instantsend>.

<sup>286</sup> *Ibid.*

<sup>287</sup> *Ibid.*

<sup>288</sup> See: S. GOLDBERG, "Mythbusting: Blockchain and Cryptocurrencies Edition", May 2018, <http://paymentsjournal.com/mythbusting-blockchain-and-cryptocurrencies-edition/>.



#### d. Dash is a medium of exchange

Just like Monero, Dash is being accepted as a means of payment by a steadily growing number of online merchants.<sup>289</sup> As a result Dash also constitutes a medium of exchange.

#### e. Dash is an (optional) anonymous coin

Like Bitcoin's blockchain, Dash's blockchain is transparent by default, which means that generally speaking transactions are always openly verifiable and traceable on the blockchain. To give its users true financial privacy, Dash offers the option to use a feature called PrivateSend. PrivateSend obscures the origins of a user's funds through a process known as "mixing".<sup>290</sup>

#### Box 2: The PrivateSend mixing-process explained

*"1. PrivateSend begins by breaking your transaction inputs down into standard denominations. These denominations are 0.01 Dash, 0.1 DASH, 1 DASH and 10 DASH – much like the paper money you use every day.*

*2. Your wallet then sends requests to specially configured software nodes on the network, called 'masternodes'. These masternodes are informed then that you are interested in mixing a certain denomination. No identifiable information is sent to the masternodes, so they never know 'who' you are.*

*3. When two other people send similar messages, indicating that they wish to mix the same denomination, a mixing session begins. The masternode mixes up the inputs and instructs all three users' wallets to pay the now-transformed input back to themselves. Your wallet pays that denomination directly to itself, but in a different address (called a change address).*

*4. In order to fully obscure your funds, your wallet must repeat this process a number of times with each denomination. Each time the process is completed, it's called a 'round'. Each round of PrivateSend makes it exponentially more difficult to determine where your funds originated. The user may choose between 2-8 rounds of mixing.*

*5. This mixing process happens in the background without any intervention on your part. When you wish to make a transaction, your funds will already be anonymized. No additional waiting is required."*

Source: <https://docs.dash.org/en/latest/introduction/features.html#privatesend>.

### 3.3. Conclusion: a taxonomy and timeline of cryptocurrencies

On the basis of the above overview and the above analysis we come to a taxonomy and timeline of cryptocurrencies, allowing to more precisely conduct the regulatory analysis and to signal the flaws of the regulatory framework hereinafter.

We start with the taxonomy.

What is clear from the overview is that THE cryptocurrency is non existing. Although some are similar to each other, there is a lot of variation as to how they are structured, on which technology they run, the anonymity involved, etc.

The below table intends to illustrate this diversity. The selected cryptocurrencies are compared on the basis of various parameters: whether they run on permissioned or permissionless technology, their decentralized nature, whether they were initially offered by an identifiable person or entity, if they are electronically traded, directly convertible into fiat currency, are a medium of exchange and are pseudo-anonymous or fully anonymous. These parameters are not chosen randomly, but help to

<sup>289</sup> See for an overview of online merchants that accept payments in Dash: <https://www.dash.org/merchants/>.

<sup>290</sup> See: <https://docs.dash.org/en/latest/introduction/features.html#privatesend>.

assess hereinafter to what extent the cryptocurrencies are caught by AMLD5, which crypto players are included in the scope of AMLD5, whether regulation can be attached to relevant players that are not (yet) in scope, etc.

The table reflects our understanding of the selected cryptocurrencies. It should be read mindful of the fact that making clear-cut distinctions between cryptocurrencies is not easy.<sup>291</sup> Complicating factors are *inter alia* the scarcity of the information available and the often highly technical nature thereof. Moreover, cryptocurrencies are a moving target. E.g. a cryptocurrency that is not a medium of exchange now, can be one tomorrow. Therefore, the overview does not pretend to be the only way of portraying or classifying the selected cryptocurrencies.

Arguably, to get an absolutely clear picture of cryptocurrencies and all their different features in view of giving the best possible policy advice, more work needs to be done and further research is required. Nevertheless, for the purposes of this study, we are of the opinion that below table is a workable instrument, allowing to draw some conclusions throughout the regulatory analysis.

---

<sup>291</sup> Sometimes it is even not easy to make a clear-cut distinction between the technology a coin runs on and the coin itself.

Table 2: Coin taxonomy

Name	Permissions / Permitted	Decentralized	Initial offering by an identifiable person or entity?	Electronically traded	Directly convertible into fiat currency	Medium of exchange	Pseudo-anonymous / Anonymous
Bitcoin	 Permissions	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pseudo-anonymous
Ethereum	 Permissions	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pseudo-anonymous
Ripple	 Permitted	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pseudo-anonymous
Bitcoin Cash	 Permissions	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pseudo-anonymous
Litecoin	 Permissions	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pseudo-anonymous
Stellar	 Permissions	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pseudo-anonymous
Cardano	 Permitted / Permissions	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pseudo-anonymous
IOTA	 Permissions	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Pseudo-anonymous
NEO	 Permitted	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Pseudo-anonymous
Monero	 Permissions	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Anonymous
Dash	 Permissions	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Anonymous

Legend:

= Yes



= To a limited extent



= No

Moving on to a timeline of cryptocurrencies, further contributing to a better understanding of these coins for regulatory purposes. We observed the following. Where the first cryptocurrencies were developed as pure P2P digital cash equivalents, the analysis above shows that novel forms of cryptocurrencies have meanwhile been created to serve different and /or additional purposes. In 2014 we saw the emergence of cryptocurrencies advocated to be fully anonymous. In 2015 a crucial tipping point appears to have been the creation of the Ethereum platform, which initiated the development of completely new ecosystems or platforms on top of which so-called smart contracts and/or decentralized applications (“Dapps”) can be run, fueled by a new generation of cryptocurrencies. This ever-growing technological complexity and evolving nature of cryptocurrencies<sup>292</sup>, as illustrated in the timeline included as Figure 2 below, should be taken heed of when further regulating cryptocurrencies in the future.<sup>293</sup>

Figure 2: Coin timeline



<sup>292</sup> See on this evolution also very comprehensive: U. SAIDOV, “Cryptocurrencies: The Rise of Decentralized Money”, April 2018, <https://blogs.cfainstitute.org/investor/2018/04/03/cryptocurrencies-the-rise-of-decentralized-money/>.

<sup>293</sup> It should also be noted that even coins that were originally conceived as pure P2P digital cash equivalents are being further developed by their respective communities and may hold additional features in the future.

## 4. EU REGULATORY FRAMEWORK

### 4.1. Setting the scene: similar regulatory challenges in the fight against money laundering, terrorist financing and tax evasion via cryptocurrencies

#### 4.1.1. Anonymity

The key issue that needs to be addressed in order to adequately capture cryptocurrencies and cryptocurrency players, particularly users, in legislation is to unveil the anonymity, varying from complete anonymity to pseudo-anonymity, that surrounds them.<sup>294</sup> This is the biggest problem for combating money laundering and countering terrorist financing: the anonymity prevents cryptocurrency transactions from being adequately monitored, allowing shady transactions to occur outside of the regulatory perimeter, allowing criminal organisations to use cryptocurrencies to obtain easy access to "clean cash" (both cash in/out). Relating to terrorist financing, the story of Ali Shukri Amin who provided instructions over Twitter on how to use Bitcoin to mask the provision of funds to Daesh is a striking example of the risks brought by the anonymity surrounding cryptocurrencies.<sup>295</sup>

Anonymity is also the major issue when it comes to tax evasion. Entering into taxable cryptocurrency transactions without paying taxes is tax evasion. But, when a tax authority does not know who enters into the taxable transaction, because of the anonymity involved, it cannot detect nor sanction this tax evasion. This makes cryptocurrencies a very attractive means for tax evaders.<sup>296</sup> By some commentators instruments such as Bitcoin were even described as "tomorrow's tax havens".<sup>297</sup>

This being said, and as apparent from our overview of cryptocurrencies above, it should be noted that some cryptocurrencies are pseudo-anonymous, which basically means that if great effort is made<sup>298</sup> and complex techniques are deployed, it is possible for authorities to find out users' identities. Although this can already be a help in the fight against money laundering, terrorist financing and tax evasion in some cases, it does not allow a standardized approach to tackle money laundering, terrorist financing and tax evasion more widely: discovering identities in this way is too complex and costly to become the general answer to tackling this issue - and moreover, it will not certainly lead to any result. New initiatives like the Investigation of Transactions in Underground Markets ("**TITANIUM**") project<sup>299</sup>, may change this at some point, but it is still too early to tell to what extent. In any event, a more structural regulatory approach is desirable.

<sup>294</sup> IMF Staff Discussion Note, "Virtual Currencies and Beyond: Initial Considerations", January 2016, <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>, 27.

<sup>295</sup> FATF, "Report on emerging terrorist financing risks", October 2015, <http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf>, 36.

<sup>296</sup> IMF Staff Discussion Note, "Virtual Currencies and Beyond: Initial Considerations", January 2016, <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>, 27; OECD, "Tax Challenges Arising from Digitalisation – Interim Report", 2018, 206, No. 501; R.M. BRATSPIES, "Cryptocurrencies and the Myth of the Trustless Transaction", March 2018, 43 (electronically available via <https://ssrn.com/abstract=3141605>).

<sup>297</sup> T. MANDJEE, "Bitcoin, its Legal Classification and its Regulatory Framework", 15 J. Bus. & Sec. L. 157, 2016, <https://digitalcommons.law.msu.edu/jbsl/vol15/iss2/>, 188 and the references there.

<sup>298</sup> The emergence of quantum computing, which uses the laws of quantum mechanics to process large volumes of information much more efficiently than traditional computing, may be able to change this. However, this is not something investigators will be able to apply tomorrow. At present, quantum computing still remains at an embryonic stage of theoretical development. See for an introduction to this technology: B. DUPONT, "The cyber security environment to 2022 Trends, drivers and implications", a study prepared for The National Cyber Security Directorate, Public Safety Canada, 2012, 44p. (electronically available via <http://ssrn.com/abstract=2208548>).

<sup>299</sup> See: <https://www.titanium-project.eu>. See also T. KEATINGE, D. CARLISLE and F. KEEN, "Virtual currencies and terrorist financing: assessing the risks and evaluating responses", study commissioned by the Directorate General for Internal Policies, Policy Department for Citizens'

## Box 3: Some thoughts on the TITANIUM project

The TITANIUM project will research, develop, and validate novel data-driven techniques and solutions designed to support law enforcement agencies charged with investigating criminal or terrorist activities involving virtual currencies and/or underground markets in the darknet. The expected result of the project is a set of services and forensic tools, which operate within a privacy and data protection environment that is configurable to local legal requirements, and can be used by investigators for *inter alia* analyzing transactions across different virtual currency ledgers.

It is clear that the TITANIUM project is directly relevant for the fight against money laundering, terrorist financing and tax evasion via cryptocurrencies. If successful, it will add to the toolbox of law enforcement agencies tracking down money laundering, terrorist financing and tax evasion via cryptocurrencies. Interesting will be to see whether the new techniques developed are less complex and costly than the once already available to trace criminals using pseudo-anonymous cryptocurrencies. Probably we can only speak of significant progress if the outcome would be that law enforcement agencies would have at their disposal an easy to use and relatively cheap method to trace criminals using cryptocurrencies. It will also be interesting to find out whether the new techniques can be deployed both to pseudo anonymous and fully anonymous coins.

In any event, and without prejudice to the TITANIUM project being extremely relevant and valuable, it is not something we can suffice with. As we will evidence throughout this research, there is also a need for a more structural, regulatory approach. It goes without saying that such approach and enhancing the toolbox of law enforcement agencies on the basis of the TITANIUM project go hand in hand: to ensure compliance with the regulatory framework, law enforcement agencies must be able to adequately detect infractions (via the newly developed techniques) and subsequently sanction them.

#### 4.1.2. Cross-border nature

In addition to anonymity, the intrinsically cross-border nature of cryptocurrencies, crypto markets and crypto players is a major challenge for regulators.<sup>300</sup> One of the issues is e.g. that crypto markets and crypto players can be located in jurisdictions that do not have effective money laundering and terrorist financing controls in place.<sup>301</sup> The cross-border nature of cryptocurrencies, crypto markets and crypto players probably means that rules will only be adequate when they are taken at a sufficiently international level.

#### 4.1.3. Often no central intermediary

Another factor of importance challenging the fight against money laundering, terrorist financing and tax evasion is that there is often no central intermediary, such as an issuer, that would normally be the focal point of regulation.<sup>302</sup> Therefore, an important question is to which players in the crypto market should regulation be attached, absent a central intermediary.

#### 4.1.4. Cryptocurrencies are falling between the cracks

The existing European legal framework is failing to deal with the aforementioned issues. There are simply no rules unveiling the anonymity associated with crypto-currencies, making the question whether they are taken at the right level or to whom they apply a superfluous one.

Because of the absence of rules unveiling anonymity, more substantive rules that currently could already have cryptocurrencies in scope completely miss effect. This is particularly true for the legal

Rights and Constitutional Affairs, May 2018, 59 (electronically available via [http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL\\_STU\(2018\)604970\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf)).

<sup>300</sup> IMF Staff Discussion Note, "Virtual Currencies and Beyond: Initial Considerations", January 2016, <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>, 25 and 27.

<sup>301</sup> ECB, "Virtual Currency Schemes – a further analysis", February 2015, <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>, 28.

<sup>302</sup> IMF Staff Discussion Note, "Virtual Currencies and Beyond: Initial Considerations", January 2016, <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>, 25.

framework on exchange of information in the field of taxation.<sup>303</sup> The framework simply cannot be activated: to exchange information, authorities must have it in the first place. For the same reasons, the current EU framework on tax avoidance<sup>304</sup>, relating *inter alia* to exit taxes in the context of assets transfers by corporates, miss effect when it comes to cryptocurrencies, because of their anonymous and easy-to-hide nature. To be able to tax, the tax administration should know of the taxable basis and when it comes to cryptocurrencies this is just extremely difficult.

Another example relates to the freezing and confiscation of property. Substantively, it is arguable that cryptocurrencies are already in scope of the relevant European rules.<sup>305</sup> Property within these rules refers to property of any description, whether corporeal or incorporeal, movable or immovable, and legal documents or instruments evidencing title or interest in such property. Well, it is acceptable that cryptocurrencies are within the remit of this definition: they could be seen as incorporeal moveable property. Yet, leaving a few examples of success stories aside, the rules largely miss effect. The reason, again, is the same: to be able to freeze and confiscate cryptocurrencies it is necessary to know that a criminal has them, and this is what the anonymity surrounding cryptocurrencies prevents.

So, the crux of the matter is how we can unveil the anonymity related to cryptocurrency transactions so as to be able to track the illegal transactions.

#### 4.1.5. A difficult dividing line with cybersecurity, data protection and privacy

It is accepted that encryption, which is basically what happens in the context of cryptocurrencies, is an effective way for citizens and businesses to defend themselves against the abuse of IT technologies, such as hacking, identity and personal data theft, fraud and the improper disclosure of confidential information. However, encryption can also be used by criminals, e.g. the use of cryptocurrencies for money laundering or terrorist financing, complicating law enforcement authorities' criminal investigations. Therefore, it is a thin line between preserving strong encryption for the protection of cybersecurity, data protection and privacy on the one hand, while offering opportunities for legitimate law enforcement access to information for the purpose of criminal investigations with appropriate safeguards on the other hand, as was recognized by the European Commission.<sup>306</sup> We raise this issue, but will not elaborate on cybersecurity, data protection and privacy aspects in this research. That would exceed the scope.<sup>307</sup>

<sup>303</sup> Council Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC, as amended from time to time, as regards mandatory automatic exchange of information in the field of taxation; this Directive was very recently, on 25 May 2018, amended again with rules relating to the mandatory automatic exchange of information in the field of taxation for reportable cross-border arrangements and reporting duties of intermediaries (see a first analysis: <https://www.tiberghien.com/en/1282/new-reporting-obligation-for-cross-border-arrangements-council-directive-approved-25-may-2018>).

<sup>304</sup> Council Directive (EU) 2016/1164 of 12 July 2016 laying down rules against tax avoidance practices that directly affect the functioning of the internal market, OJ L 193, 19 July 2016 (electronically available via <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1164&from=EN>).

<sup>305</sup> The current EU legal framework on the freezing and confiscation of proceeds of crime consists of four Council Framework Decisions (FD) and one Council Decision: Framework Decision 2001/500/JHA13, Framework Decision 2005/212/JHA15, Framework Decision 2003/577/JHA17, Framework Decision 2006/783/JHA18 and Council Decision 2007/845/JHA19. Also see the proposal for a directive on the freezing and confiscation of proceeds of crime in the European Union of 12 March 2012, COM(2012) 85 final and the proposal for a regulation on the mutual recognition of freezing and confiscation orders, COM/2016/0819 final.

Besides, without going into detail on the scope of the whole European substantial framework relating to financial crimes, generally speaking that framework has a broad reach. Therefore, the conclusion we made for freezing and confiscation of property (its scope being large enough already to capture cryptocurrencies), could very well also apply to the larger framework.

<sup>306</sup> See: [https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/encryption\\_en](https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/encryption_en).

<sup>307</sup> On the interaction between blockchain and the GDPR, see *inter alia* M. FINCK, "Blockchains and Data Protection in the European Union", Max Planck Institute for Innovation & Competition Research Paper No. 18-01, 30 November 2017, 32p. (electronically available via <https://ssrn.com/abstract=3080322>); W. MAXWELL and J. SALMON, "A guide to blockchain and data protection", Hogan Lovells, September 2017, 22p., [https://www.hlengage.com/uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf?\\_sm\\_au=iVV6bs5Z45DMRVfr](https://www.hlengage.com/uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf?_sm_au=iVV6bs5Z45DMRVfr); A. VAN HUMBEECK, "The Blockchain-GDPR Paradox", November 2017, <https://medium.com/wearethelidger/the-blockchain-gdpr-paradox->

#### 4.1.6. Don't throw the baby out with the bathwater: the technology

Cryptocurrencies run on ingenious technology. From a law enforcement perspective, introducing mechanisms of accountability of crypto players should prevent this technology from being used largely for nefarious purposes, but at the same time not prevent technological innovation from happening<sup>308</sup>. Therefore, legislative action should always be proportionate so that it addresses the illicit behaviour while at the same time not strangling technological innovation at birth. This is an aspect of particular relevance for this research. Cryptocurrencies run on blockchain or other technology. This technology is perfectly legitimate and offers many advantages for innovation in multiple legitimate sectors, including the business and public sector. It has for instance been suggested that blockchain technology could be an adequate defense mechanism against digital ransomware<sup>309</sup>. The idea is that through blockchain technology sensitive information can be kept in a decentralized manner instead of centralized (as it is now). Keeping information in a decentralized manner makes it harder to link the information to the person it relates to. It is then also harder to know who to address for the ransom. Moreover, there would be numerous copies of the info, making it extremely difficult for criminals to hold them all to ransom. Another deterring factor could be that attacking a decentralized system of information would be easily visible to its participants.<sup>310</sup> Another example of a legitimate use case of blockchain technology for the greater good can be found in China<sup>311</sup>, where blockchain is being used to combat tax fraud in the context of a partnership between Tencent and the Shenzhen national taxation bureau.<sup>312</sup>

If cryptocurrencies are used for criminal purposes, it is therefore not the technology that needs to be addressed. On the contrary, it is the illicit use that should be targeted. Exceptionally, however, an exception can be made in well-defined cases, such as the mixing technique used in the context of Dash and Monero's RingCT<sup>313</sup>, stealth addresses and Kovri-project.<sup>314</sup>

---

[fc51e663d047](https://www.techzine.nl/blogs/404986/blockchain-en-gdpr-een-moeilijk-huwelijk.html?redirect=1); X, "Blockchain en GDPR: een moeilijk huwelijk", May 2018, <https://www.techzine.nl/blogs/404986/blockchain-en-gdpr-een-moeilijk-huwelijk.html?redirect=1>; S. MARTINET, "GDPR and Blockchain: Is the New EU Data Protection Regulation a Threat or an Incentive?", May 2018, <https://cointelegraph.com/news/gdpr-and-blockchain-is-the-new-eu-data-protection-regulation-a-threat-or-an-incentive>.

<sup>308</sup> U.W., CHOCHAN, "International Law Enforcement Responses to Cryptocurrency Accountability: Interpol Working Group", Discussion Paper, 3 April 2018, 3.

<sup>309</sup> Ransomware is the illegal act of restricting access to computer files until a ransom is paid. See: X, "True scale of Bitcoin ransomware extortion revealed", MIT Technology Review, April 2018, <https://www.technologyreview.com/s/610803/true-scale-of-bitcoin-ransomware-extortion-revealed/>. See also more elaborate: T. KEATINGE, D. CARLISLE and F. KEEN, "Virtual currencies and terrorist financing: assessing the risks and evaluating responses", study commissioned by the Directorate General for Internal Policies, Policy Department for Citizens' Rights and Constitutional Affairs, May 2018, 17 *et seq.* (electronically available via [http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL\\_STU\(2018\)604970\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf)).

<sup>310</sup> See e.g. T. SERRES, "2017's Ransomware Attacks: Could Blockchain Technology Have Prevented Them?", May 2017, <https://medium.com/animal-media/2017s-ransomware-attacks-could-blockchain-technology-have-prevented-them-ed9ca6bf348b>.

<sup>311</sup> It should be noted that China's approach towards blockchain technology stands in contrast with its strict approach towards cryptocurrency exchanges. China recently introduced a ban on cryptocurrency exchanges to stop all (domestic) cryptocurrency trading. See: S. SETH, "Is Bitcoin Banned in China?", February 2018, <https://www.investopedia.com/news/bitcoin-banned-china/>; R. PERPER, "China is moving to eliminate all cryptocurrency trading with a ban on foreign exchanges", February 2018, [https://www.businessinsider.nl/china-eliminates-all-cryptocurrency-trading-2018-2/?international=true&r=US&sm\\_au=iVV6bs5Z45DMRVfr](https://www.businessinsider.nl/china-eliminates-all-cryptocurrency-trading-2018-2/?international=true&r=US&sm_au=iVV6bs5Z45DMRVfr); W. SUBERG, "Ban Complete: China Blocks Foreign Crypto Exchanges To Counter 'Financial Risks'", February 2018, <https://cointelegraph.com/news/ban-complete-china-blocks-foreign-crypto-exchanges-to-counter-financial-risks>; S. LENG, "Beijing bans bitcoin, but when did it all go wrong for cryptocurrencies in China?", February 2018, <http://www.scmp.com/news/china/economy/article/2132119/beijing-bans-bitcoin-when-did-it-all-go-wrong-cryptocurrencies>.

<sup>312</sup> See e.g. S. SUNDARARAJAN, "Chinese City to Use Blockchain In Fight Against Tax Evasion", May 2018, <https://www.coindesk.com/tencent-partners-with-city-authority-to-combat-tax-evasion-with-blockchain/>; J. SHAWDAGOR, "Blockchain Against Tax Fraud As Tencent Partners Up With Shenzhen National Taxation Bureau", May 2018, <https://bitrazzi.com/blockchain-against-tax-fraud-as-tencent-partners-up-with-shenzhen-national-taxation-bureau/>.

<sup>313</sup> This technique is also being applied to other coins. See: T. KEATINGE, D. CARLISLE and F. KEEN, "Virtual currencies and terrorist financing: assessing the risks and evaluating responses", study commissioned by the Directorate General for Internal Policies, Policy Department for Citizens' Rights and Constitutional Affairs, May 2018, 32 (electronically available via [http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL\\_STU\(2018\)604970\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf)).

<sup>314</sup> See above and below.



This approach is recognized by the European Commission in the build-up to its proposal to amend AMLD<sup>315</sup>, as will be discussed hereinafter. In that context, the Commission stressed that the proposed measures have no negative effects on the benefits and technological advances presented by the distributed ledger technology underlying virtual currencies, including innovative ways for governments to reduce fraud, corruption, error and the cost of paper-intensive processes, set in place new, modern ways in which governments and citizens interact, in terms of data sharing, transparency and trust, and provide novel insights into establishing ownership and provenance for goods and intellectual property.

#### 4.1.7. The tide is changing: AMLD5

As we will analyse further in this research, the European tide is changing. At the time of writing of this research new European rules on money laundering and terrorist financing are in the final phase of being adopted. These rules include measures to pull cryptocurrencies and (some) crypto players out of the regulatory dark. Hence, the regulatory approach taken by the EU is to address cryptocurrencies and crypto players via the rules on money laundering and terrorist financing.

As a final introductory side note, from a conceptual perspective, the EU could have also done this via other types of legislation, such as financial services legislation. That would have also pulled cryptocurrencies and crypto players out of the dark and into the light, and even more, e.g. relevant crypto players would have needed a license.<sup>316</sup> As we will see further on, this option, from a policy perspective, was not preferred at this stage.

Hereinafter we will elaborate on the new European framework on cryptocurrencies and crypto players in the context of combating money laundering and terrorist financing. We will start the analysis by highlighting the background of the legislative framework. After that, we will briefly discuss the current framework. Subsequently, the legislative road to the upcoming framework and the upcoming framework itself will be scrutinized. Lastly, two add-ons to the framework of combating money laundering and terrorist financing will be briefly touched upon, the Funds Transfer Regulation and the Cash Control Regulation, to verify whether cryptocurrencies are in scope of these regulations.

<sup>315</sup> COM/2016/0450, "Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC", 6 July 2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016PC0450&qid=1523358551244&from=EN>.

<sup>316</sup> At present it is generally speaking very difficult, if not impossible, to include cryptocurrencies and players within the existing scope of financial services legislation. A number of examples to illustrate this can be given. First, the scope of various rules is connected to the concept financial instruments, such as market abuse rules or MiFID rules. When we look at the definition of "financial instruments", it is very difficult to include cryptocurrencies within that definition. Therefore, cryptocurrencies will probably not be financial instruments. This means that MiFID licensing rules and behavioural rules for that reason alone cannot be attached to cryptocurrency players, such as cryptocurrency exchange platforms or wallet providers. A second example is that of the prospectus regulation. This uses as connecting factor "securities". Taking a close look at the definition of "securities", it seems that cryptocurrencies do not fit easily within this definition. But more importantly, prospectus requirements are connected to an issuer. In the context of cryptocurrencies, there will not be an issuer (yet, sometimes, there is an offeror, to which theoretically rules could be attached; see *infra*). A third example is that of payment services. In view of the various components of the definition of payment services it seems difficult to include service providers in relation to cryptocurrencies within that definition. Moreover, it can be expected that the provision of services related to payments by a service provider in the framework of cryptocurrency transactions will not constitute his ordinary profession or business, exempting him anyway from the scope of PSD2. Dependent on the circumstances, also the limited network exception could serve as a safe harbour for the offered services. A last example is that of the e-money rules. It is very clear that cryptocurrencies do not fit within the definition of e-money, exempting them from the scope of these rules. See for a regulatory analysis e.g. R. HOUBEN, "Bitcoin: there two sides to every coin", ICCLR, Vol. 26, Issue 5, 2015, 193-208; P. VALCKE, N. VANDEZANDE and N. VAN DE VELDE, "The evolution of third party payment providers and cryptocurrencies under the EU's upcoming PSD2 and AMLD4", 2015, Swift Institute Working Paper No. 2015-001, 77p.; N. VANDEZANDE, *Virtual currencies: a legal framework*, Antwerp, Intersentia, 2018, 165 *et seq.*

## 4.2. Money laundering and terrorist financing

### 4.2.1. Background

The fight against money laundering and terrorism financing is a key priority of the international community, including the EU. It has long been established that money laundering activities are usually carried out in an international context and therefore national measures are not sufficient. The Recommendations of the Financial Action Task Force ("**FATF**") – drawn up in 1990 and revised from time to time – are the cornerstone of the international framework for combating money laundering and terrorist financing. They have been endorsed by over 180 countries, and are universally recognised as setting out the international standards.<sup>317</sup>

The European Union adopted its first Anti-Money Laundering Directive on 10 June 1991 ("**AMLD1**").<sup>318</sup> An anti-money laundering framework at the level of the European Union was needed to coordinate measures across the different Member States and safeguard the stability of the financial system as a whole. This first Anti-Money Laundering Directive was later amended by the second Anti-Money Laundering Directive ("**AMLD2**")<sup>319</sup>, before being repealed and replaced by the third Anti-money Laundering Directive ("**AMLD3**").<sup>320</sup> The latter introduced the fight against terrorist financing and included the revised 2003 FATF Recommendations.<sup>321</sup> In February 2012, the FATF published a revised set of its Recommendations.<sup>322</sup> In parallel, the Commission undertook a review of the third Anti-Money Laundering Directive, which needed to be updated and aligned with the 2012 FATF Recommendations. On 20 May 2015 a revised anti-money laundering and counter-terrorism financing framework was adopted which substantially changed the EU's existing legal framework designed to protect the financial system against money laundering and terrorist financing. The revised rules consist of the fourth Anti-Money Laundering Directive ("**AMLD4**")<sup>323</sup> and the EU Funds Transfer Regulation ("**FTR**")<sup>324</sup> and provide for a more targeted and focused risk-based approach.<sup>325</sup> AMLD4 intends to strengthen the existing rules and to make the fight against money laundering and

<sup>317</sup> FATF, "International standards on combating money laundering and the financing of terrorism & proliferation. The FATF Recommendations", February 2012, 7

[http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF\\_Recommendations.pdf](http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf)

<sup>318</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, *OJ L 166*, 28 June 1991, 77 (electronically available via

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31991L0308&from=EN>).

<sup>319</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, *OJ L 344*, 28 December 2001, 76, (electronically available via

[https://eur-lex.europa.eu/resource.html?uri=cellar:57ce32a4-2d5b-48f6-adb0-c1c4c7f7a192.0004.02/DOC\\_1&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:57ce32a4-2d5b-48f6-adb0-c1c4c7f7a192.0004.02/DOC_1&format=PDF)).

<sup>320</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 purposes of money laundering and terrorist financing, *OJ L 309*, 25 November 2005, 15 (electronically available via <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005L0060&from=EN>).

<sup>321</sup> FATF, "The Forty Recommendations", 20 June 2003,

<http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202003.pdf>.

<sup>322</sup> FATF, "International standards on combating money laundering and the financing of terrorism & proliferation. The FATF Recommendations", February 2012,

[http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF\\_Recommendations.pdf](http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf).

<sup>323</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, *OJ L 141*, 5 juni 2015, 73 (electronically available via

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L0849&from=En>).

<sup>324</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, *OJ L 141*, 5 juni 2015, 1 (electronically available via <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015R0847>).

<sup>325</sup> On this approach, see e.g. E. HERLIN-KARNELL and N. RYDER, "The robustness of EU Financial Crimes Legislation: A Critical review of the EU and UK Anti-Fraud and Money Laundering Scheme", 2017, *European Business Law Review*, 1-39.

terrorism financing more effective. AMLD4 should have been transposed by Member States on 26 June 2017 at the latest. As of the same date, also the FTR became applicable.

#### 4.2.2. AMLD4

The core principle of AMLD4 is the prohibition of money laundering and terrorist financing.<sup>326</sup>

What is money laundering? Technically, the following conduct is money laundering, when committed intentionally:

- a) the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action;
- b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity;
- c) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity;
- d) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in points a, b and c<sup>327</sup>.

In more simple terms money laundering can be explained as the process by which proceeds of criminal activity are "cleaned" and brought into the lawful economy so that their illegal origins are concealed or disguised.<sup>328</sup>

In the application of the definition of money laundering, "*property*" means assets of any kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such assets.<sup>329</sup>

Money laundering shall be regarded as such even where the activities which generated the property to be laundered were carried out in the territory of a third country.<sup>330</sup>

What is terrorist financing? This is defined as the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA on combating terrorism.<sup>331</sup> The offenses referred to are intentional acts which given their nature or context, may seriously damage a country or an international organisation where committed with the aim of seriously intimidating a population, or unduly compelling a government or international organisation to perform or abstain from performing any act, or seriously destabilising or destroying the fundamental political, constitutional,

<sup>326</sup> Article 1, 1 and 2 AMLD4.

<sup>327</sup> Article 1, 3 AMLD4.

<sup>328</sup> E.g. I. BANTEKAS and S. NASH, *International Criminal Law*, Routledge-Cavendish, 2007, 247; S. ROYER, "Bitcoins in het Belgische strafrecht en strafprocesrecht", *RW* 2016-17, No. 13, 491. Generally, there are three steps: the placement phase where the profits generated by the criminal activity must be separated from the criminal activity itself (e.g. dirty money is placed with other legitimate money in the system), the layering phase during which steps are taken to disguise the route which the money takes during the laundering process and the integration phase where the money must become available for use by the criminal organisation.

<sup>329</sup> Article 3, (3) AMLD4.

<sup>330</sup> Article 1, 4 AMLD4.

<sup>331</sup> Article 1, 5 AMLD4.

economic or social structures of a country or an international organisation. Are deemed to be terrorist offences: attacks upon a person's life which may cause death, attacks upon the physical integrity of a person, kidnapping or hostage taking, causing extensive destruction to a government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major economic loss, etc.

A difference between terrorist financing and money laundering is that in the event of terrorist financing, the origin of the funds can be legitimate. It is the destination of the funds, i.e. financing terrorists, that makes the whole deal illegitimate.<sup>332</sup> Money laundering on the contrary is by definition based on another crime which gives rise to the laundering in question.<sup>333</sup>

There is no definition of "*funds*" included in AMLD4. Legal doctrine opines that it should have the same meaning as "*property*" under AMLD4, especially given that such approach would be consistent with the FATF recommendations.<sup>334</sup>

*Ratione personae* AMLD4 applies to so-called obliged entities. Because these obliged entities are the entry-point for money laundering and terrorist financing requirements, they are sometimes also referred to as the "gatekeepers".<sup>335</sup>

The obliged entities include: credit institutions, financial institutions, a well defined list of natural or legal persons acting in the exercise of their professional activities (under which auditors, external accountants, tax advisors, notaries and other independent legal professionals), trust or company service providers, estate agents, 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 and providers of gambling services.<sup>336</sup>

In addition, Member States are required to extend the scope of AMLD4 in whole or in part to professions and categories of undertakings, other than the obliged entities referred to above, which engage in activities which are particularly likely to be used for the purposes of money laundering or terrorist financing.<sup>337</sup> This implies a continuous monitoring by Member States of money laundering and terrorist financing risks within their territory and taking action when they discover vulnerabilities.

When an entity is an obliged entity and thus falls within the remit of AMLD4, it is subject to various requirements, which ultimately aim at tracing financial information and having a deterrent effect on money laundering and terrorist financing.<sup>338</sup>

An important requirement is that obliged entities have to perform customer due diligence when establishing a business relationship, when carrying out an occasional transaction that amounts to EUR 15.000 or more, when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold, when there are doubts about the veracity or adequacy of previously obtained customer identification data, etc.<sup>339</sup> Customer due diligence measures comprise among others identifying the customer and verifying his/her identity, identifying beneficial owners

---

<sup>332</sup> E.g. N. VANDEZANDE, *Virtual currencies: a legal framework*, Antwerp, Intersentia, 2018, 278.

<sup>333</sup> E. HERLIN-KARNELL and N. RYDER, "The robustness of EU Financial Crimes Legislation: A Critical review of the EU and UK Anti-Fraud and Money Laundering Scheme", *European Business Law Review*, 2017, No. 4, 1-39.

<sup>334</sup> N. VANDEZANDE, *Virtual currencies: a legal framework*, Antwerp, Intersentia, 2018, 295.

<sup>335</sup> See: [https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/money-laundering\\_en](https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/money-laundering_en).

<sup>336</sup> Article 2, 1 AMLD4.

<sup>337</sup> Article 4 AMLD4.

<sup>338</sup> See: [https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/criminal-justice/financial-crime\\_en](https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/criminal-justice/financial-crime_en).

<sup>339</sup> Article 11 AMLD4.

and taking reasonable measures to verify these persons' identities, conducting ongoing monitoring of the business relationship, the business and risk profile.<sup>340</sup>

Another important requirement is that when obliged entities know, suspect or have reasonable grounds to suspect that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to terrorist financing, they have to inform the competent financial intelligence unit ("**FIU**"), which every Member State must establish in order to prevent, detect and effectively combat money laundering and terrorist financing, and provide it with all necessary information. All suspicious transactions, including attempted transactions, must be reported.<sup>341</sup> The FIU in turn analyses the suspicious transactions. It disseminates the results of its analyses to the competent authorities where there are grounds to suspect money laundering, associated predicate offences or terrorist financing.<sup>342</sup> Because money-laundering and terrorist financing is not bound by borders, it is evident that FIUs have to cooperate and exchange information with each other to the greatest extent possible, regardless of their organisational status.<sup>343</sup>

When obliged entities fail their duties under AMLD4, they can be sanctioned. AMLD4 demands that any such sanction must be effective, proportionate and dissuasive. Furthermore, and more in general, competent authorities should have at their disposal an adequate sanctioning toolbox, as further detailed under AMLD4, enabling them to adequately sanction breaches of the national provisions transposing AMLD4.<sup>344</sup>

An important innovation of AMLD4 is the so-called beneficial ownership register. This relates to the mandatory set-up of a central register<sup>345</sup> comprising info on the beneficial ownership of corporate and other legal entities. When obliged entities are taking customer due diligence measures, the information on beneficial ownership must be provided to them. Also should the information be accessible by competent authorities and FIUs. Other persons than competent authorities and FIUs who are able to demonstrate a legitimate interest with respect to money laundering, terrorist financing, and the associated predicate offences, such as corruption, tax crimes and fraud, will also be granted access to beneficial ownership information, in accordance with data protection rules.<sup>346</sup>

AMLD4 contains various provisions relating to the relation with high-risk third countries. Firstly, obliged entities must apply an enhanced level of customer due diligence when dealing with natural persons or legal entities established in high-risk third countries identified by the Commission.<sup>347</sup> Furthermore, reliance on third parties established in high-risk third countries is prohibited.<sup>348</sup> AMLD4 is also conscious of the fact that money laundering and terrorist financing are international problems and the effort to combat them should be global. One of the illustrations is that Member States should ensure that their FIUs exchange information freely, spontaneously or upon request, with third-country FIUs, having regard to Union law and to the principles relating to information exchange

---

<sup>340</sup> Article 13 AMLD4.

<sup>341</sup> Article 33 AMLD4.

<sup>342</sup> Article 32 AMLD4.

<sup>343</sup> Article 52 AMLD4.

<sup>344</sup> Article 58 AMLD4.

<sup>345</sup> Article 30 AMLD4.

<sup>346</sup> Preamble 14 AMLD4.

<sup>347</sup> Article 18 AMLD4.

<sup>348</sup> Article 26, 2 AMLD4.

developed by the Egmont Group, *i.e.* an informal network of FIUs for the stimulation of international co-operation.<sup>349</sup>

#### 4.2.3. Cryptocurrencies under AMLD4

Are transactions in cryptocurrencies included in the scope of AMLD4? Although there is some scholarly debate on this<sup>350</sup>, it is fair to say that it is very difficult, if not impossible, to stretch the scope of AMLD4 so far as to include cryptocurrency transactions.<sup>351</sup>

A surmountable hurdle for cryptocurrencies to be included in the scope of AMLD4 is the connecting factor "*property*" or "*funds*". As aforementioned, property – and arguably, funds – is defined as assets of any kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such assets. Although not written for cryptocurrencies, at first glance, this definition is broad enough to also include cryptocurrencies, as they could be seen as incorporeal immovable assets for the purposes of AMLD4.<sup>352</sup>

An insurmountable hurdle, however, is that of the list of obliged entities. None of the players in the cryptocurrency scheme, regardless of which cryptocurrency is concerned, is directly or indirectly included in the list of obliged entities, not even crypto exchanges. Therefore, the AMLD4 framework simply cannot be attached to the crypto scheme, exempting it fully from the AMLD4 scope.

This also came to the attention of the European Commission in 2016, which initiated legislative action to bring virtual currency exchange platforms and custodian wallet providers under the scope of the AMLD in the future.<sup>353</sup> The coming of age of this inclusion into the AMLD framework will be elaborated hereinafter. It is not the intention to discuss all steps that were taken, but only to highlight the important steps, ultimately with the aim to create a better understanding of where the final results and policy choices came from.

#### 4.2.4. The coming of age of the inclusion of cryptocurrencies into AMLD5<sup>354</sup>

##### a. Preliminary remark: the terminology

Prior to deep diving into the coming of age of the inclusion of cryptocurrencies into AMLD5, we note that most of the policy documentation uses the term "virtual currencies" instead of cryptocurrencies. Important for this research is that cryptocurrencies are a subcategory of virtual currencies, more particularly that kind of virtual currencies that have a bi-directional link to the real economy. Therefore, when throughout this analysis of the regulatory framework we refer to virtual currencies, this includes cryptocurrencies. Moreover, when we look at the exact scope of the definitions included in the various policy documentation, there is a clear tendency towards targeting cryptocurrencies

<sup>349</sup> AMLD5 provides for additional measures, such as a requirement for Member States to refuse the establishment of subsidiaries or branches or representative offices of obliged entities from a high risk third country or prohibit obliged entities from establishing branches or representative offices in such a country (new Article 18a).

<sup>350</sup> It has e.g. been argued that crypto-exchanges and platforms that exchange 'virtual currency' into fiat money could fall within the definition of 'financial institutions' as set out in article 3(2)(a) of AMLD4, as this definition also includes the activities of "currency exchange offices" (see: C. HAUBEN, "Bitcoin en EU-recht: de virtuele vreemde eend in de bijt" in M. E. STORME and F. HELSEN (eds.), *Innovatie en disruptie in het economisch recht*, Antwerpen, Intersentia, 2017, 87), though this reasoning is not generally accepted.

<sup>351</sup> Very clearly: N. VANDEZANDE, *Virtual currencies: a legal framework*, Antwerp, Intersentia, 2018, 286, 298-303 and 309.

<sup>352</sup> N. VANDEZANDE, *Virtual currencies: a legal framework*, Antwerp, Intersentia, 2018, 295.

<sup>353</sup> See hereinafter: the road to AMLD5 for cryptocurrencies.

<sup>354</sup> See very informative [http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-revision-of-the-anti-money-laundering-directive-\(aml\)](http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-revision-of-the-anti-money-laundering-directive-(aml)).

with these definitions and not or only to a lesser extent other kinds of virtual currencies that have only a one directional or no link to the real economy.

#### b. The 2014 EBA opinion on virtual currencies

A first important step towards including the cryptocurrency scheme into the AMLD framework, is an opinion of the European Banking Authority in 2014 on virtual currencies.<sup>355</sup>

In this report the EBA advocates a comprehensive regulatory approach towards virtual currencies over time.<sup>356</sup> Preferably this is done through designing a tailored regulatory regime along the lines of the following characteristics: creating a virtual currency scheme governance authority that is accountable to the regulator, customer due diligence requirements, fitness and probity standards for individuals performing specified functions in a scheme governance body, exchange or other relevant market participants, mandatory incorporation in an EU Member State, transparent price formation and requirements against market abuse, authorisation and corporate governance requirements, capital requirements, evidence of secure IT systems, payment guarantee and refunds requirements, separation of virtual currency schemes from conventional payment systems and a global regulatory approach.

As a more immediate response, the EBA recommends to include market participants at the direct interface between conventional and virtual currencies, such as virtual currency exchanges, in the scope of the AMLD as 'obliged entities' and thus subject these to anti-money laundering and counter-terrorist financing requirements.

According to the EBA, this immediate response will 'shield' regulated financial services from virtual currency schemes, and will mitigate those risks that arise from the interaction between virtual currency schemes and regulated financial services. Other things being equal, this immediate response, according to the EBA, will allow virtual currency schemes to innovate and develop outside of the financial services sector, including the development of solutions that would satisfy regulatory demands on the longer term.

None of these options were eventually retained by the European legislator: no tailored framework was developed for virtual currencies, nor were the EBA's suggestions to expand the scope of the AMLD followed in the course of the - then ongoing - revision that led to the AMLD4.

#### c. The Council Invite

The momentum changed after the terrorist attacks in France. In meetings held in December 2015, the European Council concluded that rapid further action against terrorist finance was required. Following up on this, the Council on 12 February 2016 underlined the importance of achieving rapid progress on legislative actions identified by the Commission, including in the field of virtual currencies.<sup>357</sup> Therefore, it called upon the Commission to submit targeted amendments to AMLD4 and if necessary to the revised Directive on Payment Services ("**PSD2**") and to the Cash Control Regulation.

<sup>355</sup> EBA, "EBA Opinion on 'virtual currencies'", 4 July 2014, <https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf>.

<sup>356</sup> See below.

<sup>357</sup> Council conclusions on the fight against the financing of terrorism, 12 February 2016, <http://www.consilium.europa.eu/en/press/press-releases/2016/02/12/conclusions-terrorism-financing/>.

#### d. The Commission's Supranational Risk Assessment

On 26 June 2017, the European Commission released its report on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities (also referred to as the "**Supranational Risk Assessment**").<sup>358</sup> In its report the Commission identified virtual currencies as potentially vulnerable to money laundering and terrorist financing risks affecting the internal market. More in general, the Commission rightly identifies anonymity in financial transactions as a vulnerability common to all sectors, including the anonymity related to virtual currencies. Their anonymity features place an intrinsic limitation on identification and monitoring possibilities. The Commission goes as far as recommending Member States to extend already the list of obliged entities in the application of Article 4 of the AMLD4 and to consider including at least virtual currency exchange platforms and wallet providers in AMLD4's scope.

#### e. The Commission's Impact Assessment accompanying the AMLD5 proposal

In the build-up to a legislative proposal to amend the AMLD4, the Commission conducted an extensive impact assessment ("**Impact Assessment**")<sup>359</sup>. The Impact Assessment acknowledges the problem that suspicious transactions made through virtual currencies are not sufficiently monitored by the authorities, which are unable to link identities and transactions, mainly because of the anonymity surrounding virtual currencies and because of virtual currency schemes and their participants (users (traders, suppliers, customers), 'miners', currency exchange platforms, wallet providers, ...) not being regulated.

Particularly interesting are the potential regulatory answers to address this problem. According to the Impact Assessment, these are the following.

##### *i. First option: target users, including consumers and retailers using virtual currencies as an investment product or as a means of exchange for buying/selling products or services.*

The Impact Assessment sees two ways to lift the anonymity of users. The first one is through the mandatory registration of users (option A). The second one is softer and reduces virtual currencies' anonymity through the voluntary self-registration of users (option B). This option would not eradicate anonymity, but would allow authorities combating financial crime to rapidly verify identities of registered users.

##### *ii. Second option: target virtual currency exchange platforms*

Again, the Impact Assessment suggests two ways forward. The first one is to make exchange platforms obliged entities under AMLD4 (option C), submitting them *inter alia* to customer due diligence requirements. The second way forward is to bring virtual currency exchange platforms under the scope of PSD2 (option D). PSD2 goes further than AMLD4. On top of the anti-money laundering and counter-terrorist financing requirements which it automatically imposes by reference

<sup>358</sup> ECOM(2017) 340 final. The Supranational Risk Assessment ("SNRA") was the final product of a review by the Commission of anti-money laundering and terrorist financing risks at Union level in the application of Article 6 of AMLD4. The SNRA was accompanied by an elaborate Commission Staff Working Document in which among others the money laundering and terrorist financing risks relating to virtual currencies are detailed (SWD(2017) 241 final). On the one hand, the risk levels relating to virtual currencies in the context of money laundering and terrorist financing are estimated moderately significant, which is a level 2 risk on a scale of 1 (low) to 4 (high risk): while terrorists or other criminals may have a high intent to use virtual currencies' due to their characteristics (anonymity in particular), the level of capability is lower due to high technology required. On the other hand, virtual currency schemes are assessed to be highly vulnerable for terrorist financing and money laundering, because they are not regulated in the EU.

<sup>359</sup> COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document "Proposal for a Directive of the European Parliament and the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC", SWD/2016/0223 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0223&from=EN>.



to AMLD4, PSD2 also establishes a licensing obligation for regulated entities, minimum capital requirements, safeguarding requirements, and consumer protection rules. This way forward is, hence, more burdensome for exchanges.

### *iii. Third option: target custodian wallet providers*

As for the first and second option, the Impact Assessment suggests two possible actions, which are similar to the approaches suggested for exchange providers, hence: respectively bringing them under the scope of AMLD4 (option E) or under the scope of PSD2 (option F).

Why are only custodian wallet providers targeted? The *rationale* of the Impact Assessment is that software wallet providers only provide applications or programs running on users' hardware to access public information from a distributed ledger and access the network. Therefore, they are only a technical service provider. Custodian wallet providers on the contrary have custody over the user's public and private key, making them from a conceptual perspective quite similar to financial institutions holding bank or payment accounts. Therefore, they warrant more regulatory attention.

### *iv. Evaluation of the options*

Having consulted relevant stakeholders, the Impact Assessment evaluates that there is a need to have gatekeepers that manage the control of users' identities when needed. In that respect, an overwhelming majority of Member States favoured option C over D, hence make virtual currency exchange platforms obliged entities under AMLD4 instead of including them in the scope of PSD2.<sup>360</sup> The options envisaging custodian wallet providers were apparently not in scope of the debate with the stakeholders, although some Member States nevertheless expressed a preference to include these in the scope of AMLD4, instead of in the scope of PSD2. Generally, any option involving PSD2 was thus not welcomed by most Member States. They believed that this would give too much legitimacy to virtual currencies and drive consumers to believe virtual currencies are safe and sound products, which they are not, according to the various warnings financial supervisors all across the globe have issued.

The virtual currency industry itself appeared to be generally favourable to legislation for two reasons: it would give them more legitimacy and it would help to differentiate between bona-fide users and criminals.

The options involving registration of users were apparently only tested with some relevant stakeholders (i.e. consumers/users, experts), resulting in a preference for non-mandatory registration.

## **f. The Commission's AMLD5 Proposal**

In its proposed fifth revision of the AMLD ("**Commission Proposal**")<sup>361</sup>, launched on 5 July 2016, the Commission eventually takes the approach of including both virtual currency exchanges (defined as "*providers engaged primarily and professionally in exchange services between virtual currencies and fiat currencies*") and custodian wallet providers (defined as "*wallet providers offering custodian services of credentials necessary to access virtual currencies*") in the scope of the AMLD and to label these as obliged entities. Consequently, going forward these entities will have to apply customer due

<sup>360</sup> All Member States were consulted and 27 supported option C with one exception having a preference for option D. Option E was also envisaged by some Member States even though not presented in the questionnaire.

<sup>361</sup> COM/2016/0450, "Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC", 6 July 2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016PC0450&qid=1523358551244&from=EN>.

diligence controls when exchanging virtual for fiat currencies, ending the anonymity associated with such exchanges and such wallet providers, and report suspicious transactions to the competent FIU. In addition, virtual currency exchanges and custodian wallet providers will need to be licensed or registered; apparently the Commission leaves the option between licensing and registration open.

For legal certainty reasons, the Commission also proposes a definition of the term "*virtual currency*": "*a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically*".

As regards user registration, the Commission takes no immediate action. Instead, it commits itself to including in its next supranational risk assessment, which is due by 26 June 2019, if necessary, appropriate proposals, including, where appropriate, with respect to virtual currencies, empowerments to set-up and maintain a central database registering users' identities and wallet addresses accessible to FIUs, as well as self-declaration forms for the use of virtual currency users.

This does, however, not mean that users remain completely out of scope of the Commission Proposal. More in particular, users are targeted indirectly insofar they hold their virtual currencies via a custodian wallet provider or enter into virtual currency transactions via a virtual currency exchange platform. These users can no longer be anonymous, because of the customer due diligence requirements vested upon the custodian wallet providers and virtual currency exchange platforms.<sup>362</sup> All other users remain out of scope (for now).

#### g. The updated EBA Opinion

Following the Commission Proposal, the EBA published an update of its 2014 opinion on virtual currencies. The EBA welcomes this proposal as an important step to mitigate some of the financial crime risks arising from the use of virtual currencies. The EBA furthermore endorses the Commission's approach not to include virtual currency transactions in the scope of PSD2 for the time being, given the short time frame within which the Commission was asked to develop its proposals. Including such transactions within the scope of PSD2 requires further legal and business model analysis, the EBA opines. Moreover, the EBA seems to still favour a separate and tailored regulatory regime, the elements of which it proposed in its 2014 Opinion. To that end, the EBA invites the Commission to initiate as soon as possible the comprehensive analysis that is needed for assessing which, if any, regulatory regime would be most suitable for virtual currency transactions.

#### h. The 2016 ECB opinion on the Commission's proposal

In addition to the EBA, also the ECB, on 12 October 2016, released a report on the Commission Proposal.<sup>363</sup> In that report the ECB strongly supports including virtual currency exchange platforms and custodian wallet providers into the list of obliged entities, as well requiring them to be licensed or registered. The ECB, however, also expresses some concerns, under which that, while it is appropriate to regulate virtual currencies for combating money laundering and terrorist financing, regulation should not seek to promote a wider use of virtual currencies. Furthermore, the ECB makes technical comments relating to the definition of virtual currencies, that were later picked up in the compromise text, discussed hereinafter<sup>364</sup>.

<sup>362</sup> N. VANDEZANDE, *Virtual currencies: a legal framework*, Antwerp, Intersentia, 2018, 304.

<sup>363</sup> Opinion of the ECB of 12 October 2016 on a proposal for a directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC, [https://www.ecb.europa.eu/ecb/legal/pdf/con\\_2016\\_49\\_with\\_technical\\_working\\_document\\_.pdf](https://www.ecb.europa.eu/ecb/legal/pdf/con_2016_49_with_technical_working_document_.pdf).

<sup>364</sup> See below.

### i. Discussion in in Parliament

The Commission Proposal was thoroughly studied by members of the European Parliament throughout 2016 and 2017. An extensive report was adopted suggesting several amendments.<sup>365</sup> Particularly interesting are the suggestions made by the Committee on Legal Affairs of 18 January 2017. The Committee proposes to expand the scope of AMLD significantly as regards virtual currencies, so as to include virtual currency exchange platforms, custodian wallet providers, issuers, administrators, intermediaries and distributors of virtual currencies, and administrators and providers of systems for online payments. This is very broad and potentially brings all virtual currency service providers under the AMLD's scope. This has been criticized by some legal doctrine to the extent the scope also includes purely technical service providers, such as miners of cryptocurrencies, or is simply not realistic, because there is no central issuer – as is the case for many cryptocurrencies.<sup>366</sup>

Furthermore, the Committee on Legal Affairs is of the opinion that to combat the risks related to anonymity, national FIUs should be able to associate virtual currency addresses to the identity of the owner of virtual currencies.

The scope extensions were not picked up in the Compromise Text, which is analyzed hereinafter.

### j. The Compromise Text

On 13 December 2017, and following the technical work thereafter, a provisional agreement was reached between the Parliament and the Council on AMLD5, which resulted in a final compromise.<sup>367</sup> This was formally adopted by the European Parliament in plenary on 19 April 2018.<sup>368</sup> On 14 May 2018, the Council approved the European Parliament's position at first reading.<sup>369</sup> AMLD5 will enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.<sup>370</sup> Member States will have to bring into force laws, regulations and administrative provisions necessary to comply with AMLD5 by 10 January 2020.

Overall, the adopted Compromise Text is in line with the Commission Proposal. Nevertheless, there are some differences.

Firstly, the Compromise Text uses different wording to include virtual currency exchange services and custodian wallet providers in the list of obliged entities (the changes compared to the Commission Proposal are marked hereinafter: "providers engaged<sup>371</sup> in exchange services between virtual currencies and fiat currencies and custodian wallet providers"<sup>372</sup>).

<sup>365</sup> EP Report on the proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC, 9 March 2017, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0056+0+DOC+XML+V0//EN#title1>.

<sup>366</sup> N. VANDEZANDE, *Virtual currencies: a legal framework*, Antwerp, Intersentia, 2018, 293.

<sup>367</sup> See: <http://data.consilium.europa.eu/doc/document/ST-15849-2017-INIT/en/pdf>.

<sup>368</sup> European Parliament legislative resolution of 19 April 2018 on the proposal for a directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC (COM(2016)0450 – C8-0265/2016 – 2016/0208(COD)), <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2018-0178+0+DOC+PDF+V0//EN>.

<sup>369</sup> See: [https://eur-lex.europa.eu/procedure/EN/2016\\_208](https://eur-lex.europa.eu/procedure/EN/2016_208).

<sup>370</sup> AMLD5 was published in the Official Journal of the European Union on 19 June 2018. See: 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, OJ L 156, 19 June 2018, 43 (electronically available via: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843&from=EN>).

<sup>371</sup> Hence, the qualifier of "primarily and professionally" was dropped, meaning that also those providing these services occasionally would be caught under the scope. Vandezande raises the question of whether a virtual currency user, who on a non-commercial basis – for instance as a gesture to a friend – exchanges some units of virtual currency for legal tender or similar instruments, could become an

Secondly, the Compromise Text uses a slightly different definition of virtual currencies. More in particular, it defines virtual currencies 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*" (the changes compared to the Commission Proposal are marked hereinafter: "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").

Thirdly, a definition of "custodian wallet provider" ("an entity that provides services to safeguard private cryptographic keys on behalf of their customers, to hold, store and transfer virtual currencies") is included. Such a definition was not included in the Commission Proposal.

Fourthly, the Compromise Text is more precise on whether exchange platforms and custodian wallet providers should be licensed or registered: they should be registered (the changes compared to the Commission Proposal are marked hereinafter: "ensure that providers of exchange services between virtual currencies and fiat currencies, and custodian wallet providers, are registered").

The obligation for the Commission to assess the desirability of a (voluntary) registration of users in the course of its next supranational risk assessment, due by 26 June 2019, is unchanged.

#### 4.2.5. Funds Transfer Regulation

As aforementioned, the anti-money laundering framework as introduced in 2015 also includes the Funds Transfer Regulation or FTR. It is interesting to see whether this regulation somehow is a useful instrument to combat the illicit use of cryptocurrencies.

The FTR lays down rules on the information on payers<sup>373</sup> and payees<sup>374</sup> accompanying transfers of funds, in any currency, for the purposes of preventing, detecting and investigating money laundering and terrorist financing (as defined under AMLD4), where at least one of the payment service providers<sup>375</sup> involved in the transfer of funds is established in the Union. Particularly, the FTR requires the payment service provider of the payer to ensure that transfers of funds are accompanied by the name of the payer, the payer's payment account number, the payer's address, official personal document number, customer identification number or date and place of birth, the name of the payee and the payee's payment account number<sup>376</sup>, absent which he cannot execute any transfer of funds.<sup>377</sup> The payment service provider of the payee is required to detect missing information on the

---

obliged entity under the anti-money laundering framework: N. VANDEZANDE, *Virtual currencies: a legal framework*, Antwerp, Intersentia, 2018, 292.

<sup>372</sup> The proposed Preamble 7a elaborates on the difference with e-money: virtual currencies should not to be confused with electronic money as defined in the e-money Directive nor with the larger concept of "funds" as defined in point (25) of Article 4 of PSD2 nor with monetary value stored on instruments exempted as specified in Article 3(k) and 3(l) of PSD2, nor with in-games currencies, that can be used exclusively within the specific game environment. Whilst they could frequently be used as a means of payment, they may also be used for other different purposes and find broader applications such as means of exchange, investment purposes, store-of-value products or uses in online casinos. The objective of AMLD5, the Preamble continues, is to cover all the potential uses of virtual currencies. The exact added value of this Preamble is not very clear.

<sup>373</sup> "Payer" means a person that holds a payment account and allows a transfer of funds from that payment account, or, where there is no payment account, that gives a transfer of funds order (Article 3, (3) FTR).

<sup>374</sup> "Payee" means a person that is the intended recipient of the transfer of funds (Article 3, (3) FTR).

<sup>375</sup> "Payment service provider" means *inter alia* the categories of payment service providers referred to in Article 1(1) of the former Payment Services Directive (Article 3, (5) FTR).

<sup>376</sup> Article 4, 1 and 2 FTR.

<sup>377</sup> Article 4(6) FTR.

payer or the payee.<sup>378</sup> Where the payment service provider of the payee becomes aware of missing or incomplete information, he must reject the transfer or ask for additional information.<sup>379</sup> Furthermore, he is required to take into account missing or incomplete information on the payer or the payee as a factor when assessing whether a transfer of funds, or any related transaction, is suspicious and whether it is to be reported to the competent FIU in accordance with AMLD4.

With some exceptions, the FTR applies to transfers of funds<sup>380</sup>, in any currency, which are sent or received by a payment service provider or an intermediary payment service provider established in the EU.<sup>381</sup> "Funds" means banknotes and coins, scriptural money and electronic money.<sup>382</sup>

Here's the rub: cryptocurrencies are none of those, and, hence out of scope. Moreover, crypto intermediaries as a rule will not be payment service providers or intermediate payment service providers in the meaning of the FTR<sup>383</sup>. This is a second reason why the FTR is not equipped to fight the illicit use of cryptocurrencies, apart from it not being designed with cryptocurrencies in mind, which is apparent from the information to be provided, especially the reference to account numbers.

#### 4.2.6. Cash Control Regulation

As an add-on to its money laundering and terrorist financing framework, the EU enacted already in 2005 rules on the control of cash entering or leaving the Union.<sup>384</sup> These rules intend to address cash movements for illicit purposes. They apply to significant movements of cash crossing the borders of the Union, i.e. cash movements equal to or above EUR 10.000 by any natural person entering or leaving the Union. Such a person must declare the cash movement, enabling customs authorities to gather information on the movements and, where appropriate, transmit that information to other authorities.

In the context of the Cash Control Regulation, "cash" means: (a) bearer-negotiable instruments including monetary instruments in bearer form such as travellers cheques, negotiable instruments (including cheques, promissory notes and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery and incomplete instruments (including cheques, promissory notes and money orders) signed, but with the payee's name omitted; and (b) currency (banknotes and coins that are in circulation as a medium of exchange).<sup>385</sup>

Can cryptocurrencies be included in this definition? Remarkably, theoretically, there is an opening. Coins that are in circulation as a medium of exchange are in scope. Cryptocurrencies can be seen as such coins, which is also evidenced by the AMLD5 definition of virtual currencies.

<sup>378</sup> Article 7 FTR.

<sup>379</sup> Article 8 FTR.

<sup>380</sup> "Transfer of funds" means any transaction at least partially carried out by electronic means on behalf of a payer through a payment service provider, with a view to making funds available to a payee through a payment service provider, irrespective of whether the payer and the payee are the same person and irrespective of whether the payment service provider of the payer and that of the payee are one and the same (Article 3, (9) FTR).

<sup>381</sup> Article 2 FTR. Please note that the regulation also has EEA relevance.

<sup>382</sup> Article 3, (8) FTR.

<sup>383</sup> Also see the similar reasoning why crypto intermediaries are thought not to be in scope of the PSD2.

<sup>384</sup> Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community, *OJ L* 309, 25 November 2005, 9 (electronically available via: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005R1889&from=EN>).

<sup>385</sup> The current 2005 framework is currently under revision and will be replaced by a new one, taking into account the development of new best practices in the implementation within the EU of international standards on combating money laundering and terrorism financing developed by the FATF ([https://ec.europa.eu/taxation\\_customs/sites/taxation/files/com\\_2016\\_825\\_en.pdf](https://ec.europa.eu/taxation_customs/sites/taxation/files/com_2016_825_en.pdf)). The proposed new framework extends the definition of cash to some instruments or methods of payment other than currency, such as cheques, traveller's cheques, gold and prepaid cards.

Nonetheless, it is clear that the Cash Control Regulation is not written with movements of cryptocurrencies in mind. It is written with physical movements of cash in mind, explaining *inter alia* the requirement to declare and the involvement of customs authorities. Cryptocurrencies are normally not moved physically: when they move, they move digitally. This makes the cash control framework intrinsically unfit to track movements of cryptocurrencies. From a practical perspective, a scholarly debate on the inclusion of cryptocurrencies into the scope of the Cash Control Regulation, therefore, is not very useful. The one event wherein it could be of any use is when cryptocurrencies would be stored onto a portable carrier, such as a USB-stick, making that stick some sort of a bearer instrument, and this stick would be moved across the EU border. But even for this event, it does not help a lot to include it into the scope of the Cash Control Regulation. After all, even leaving aside issues of proportionality and data protection, it seems not very practical – and desirable – to verify the content of every USB-stick or the like moving across Union borders.

### 4.3. Tax evasion

The second part of this research's analysis of the regulatory framework relates to tax evasion.

As was already explained above<sup>386</sup>, the EU framework that is in place on the exchange of information in tax matters, specifically aiming at combating tax evasion, is not very well equipped to address the use of virtual currencies for tax evasion, because to be able to share information on this, authorities must have the information in the first place, which is being complicated, if not made impossible, by the anonymity surrounding cryptocurrencies.

Salvation could lie in the anti-money laundering and counter-terrorist financing framework. To the extent this framework unveils anonymity, the relevant information is registered into a central database *and* the tax authorities are able to consult and use this information, the fight against tax evasion through cryptocurrency transactions could become more effective.

Is this something that can be done already under the current AMLD framework?

Firstly, it can be noted that the definition of "criminal activity" under AMLD4 includes tax crimes relating to direct taxes and indirect taxes, which are punishable by deprivation of liberty or a detention order for a maximum of more than one year.<sup>387</sup> Hence, the use of illegal proceeds of tax crimes is in scope of AMLD4 and can constitute money laundering. Therefore, obliged entities who know, suspect or have reasonable grounds to suspect that proceeds stem from tax evasion must inform the competent FIU. The FIU will analyse the file and disseminate the results of its analysis to the competent authorities where there are grounds to suspect money laundering, associated predicate offences or terrorist financing. When it relates to a cross-border file the FIUs concerned have to cooperate and exchange the obtained information with each other to the greatest extent possible. In this respect, the AMLD4 imposes that differences between national law definitions of tax crimes can be no impediment to the ability of FIUs to exchange information or provide assistance to another FIU, to the greatest extent possible under their national law.<sup>388</sup>

In the context of all this, FIUs and competent authorities should have access to the beneficial ownership register, allowing them to verify beneficial ownership of corporate and other legal entities.

---

<sup>386</sup> See: setting the scene.

<sup>387</sup> Article 3, (4)(f) AMLD4 and Preamble 11 AMLD4.

<sup>388</sup> Article 57 AMLD4. In addition, according to Preamble 56 of the AMLD4, the exchange of information on cases identified by FIUs as possibly involving tax crimes should be without prejudice to the exchange of information in the field of taxation in accordance with Directive 2011/16 or in accordance with international standards on the exchange of information and administrative cooperation in tax matters. As aforementioned, the latter directive does not help out a lot currently as regards fighting tax evasion via the use of cryptocurrencies.

This can be very helpful when these corporates or other legal entities are in fact set-up to mask their beneficial owners for purposes of tax evasion. Other persons than competent authorities and FIUs who are able to demonstrate a legitimate interest with respect to money laundering, terrorist financing, and the associated predicate offences, such as tax crimes, will also be granted access to beneficial ownership information, in accordance with data protection rules, as already aforementioned.<sup>389</sup>

Is the tax administration a competent authority who can get access to the beneficial ownership register? There is no definition of what constitutes a "*competent authority*" under AMLD4, basically leaving it open for Member States to decide who the competent authorities within their respective territories are. At least theoretically, this could mean that the tax administration is not a competent authority. What is clear, however, is that within each Member State a competent authority should be able to initiate administrative or criminal proceedings against launderers of proceeds of tax crimes. If not, that would probably be in breach of Article 58, 2 of AMLD4, requiring Member States to have in place and make available to competent authorities a sanctioning toolbox allowing them to adequately sanction breaches of the national provisions transposing AMLD4.

However it may be, the fifth revision of the Directive on administrative cooperation in taxation in 2016 ("**DAC5**") took away all doubt: as of 1 January 2018 tax authorities must have access to the information gathered in the context of combating money laundering and terrorist financing, including the beneficial ownership register.<sup>390</sup>

AML5 acknowledges this established right.<sup>391</sup> It explicitly lists tax authorities in the list of competent authorities that must be granted access to the beneficial ownership register.<sup>392</sup> The tax administration is also explicitly recognized in Article 49 of the revised AMLD framework, requiring Member States to ensure that tax authorities when acting within the scope of the AMLD, have effective mechanisms to enable them to cooperate and coordinate domestically concerning the development and implementation of policies and activities to combat money laundering and terrorist financing. In this context, it is furthermore made clear that a request for assistance between competent authorities cannot be refused on the grounds that the request is also considered to involve tax matters.<sup>393</sup>

All these innovations brought by DAC5 and AML5 strengthen the tax authorities' toolbox to pick up the gauntlet against tax evasion, in addition to other competent authorities that may also have sanctioning powers in this field, such as public prosecutors.

The above analysis is a general one. What does all of it mean for tax evasion through the use of cryptocurrencies? Well, under AMLD4 cryptocurrencies are not in scope because none of the crypto

<sup>389</sup> Preamble 14 AMLD4.

<sup>390</sup> Council Directive (EU) 2016/2258 of 6 December 2016 amending Directive 2011/16/EU as regards access to anti-money-laundering information by tax authorities, *OJ L* 342, 16 December 2016, 1 (electronically available via <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L2258&from=EN>).

<sup>391</sup> As a side note, we mention that a similar clarification of the right to access information by tax authorities is recently also envisaged in a pending proposal for a directive laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences (COM (2018) 213), which is perceived as an add-on to the AMLD framework. This directive relates to financial information and bank account information contained in the centralised bank account registries. "Financial information" is defined rather broadly as any type of information or data which is held by FIUs to prevent, detect and effectively combat money laundering and terrorist financing, or any type of information or data which is held by public authorities or by obliged entities for those purposes and which is available to FIU without the taking of coercive measures under national law. This could be information relating to cryptocurrencies, so it seems. What is remarkable, however, is that nonetheless the proposed Preamble 9 is clear about the tax authorities' rights to information, the proposed text of the directive itself, particularly Article 3, is a lot less clear about this.

<sup>392</sup> Amended Articles 30 and 31 AMLD.

<sup>393</sup> Article 50a of the revised AMLD.

players are obliged entities, as analysed already above. So, there is no information available within the AMLD framework to be accessed by the tax administration. Thus, this is not much of a help.

Under AMLD5, virtual currency exchange platforms and custodian wallet providers become obliged entities and cryptocurrencies - via the concept "*virtual currencies*" - are brought in scope. So, insofar cryptocurrency is held through a custodian wallet provider or transactions occur via a virtual currency exchange platform, there will be information available for the tax administration, as the case may be brought to the attention of the tax administration by an FIU reporting a suspicious transaction linked to tax evasion.



## 5. ADEQUACY OF THE REGULATORY FRAMEWORK

### 5.1. Introduction

Now that we have a clear picture of the current and upcoming regulatory framework for combating money laundering, terrorist financing and tax evasion via cryptocurrencies, it is high time to analyse whether that framework is adequate to address the many challenges cryptocurrencies bring.

The existing framework is not adequate. This we have already analysed above.

How does the upcoming AMLD5 score and what would be a good way forward?

We will hereinafter try to answer that question on the basis of a number of more technical sub-questions<sup>394</sup>. The questions are the following.

- Is the definition of virtual currencies sufficient to capture the cryptocurrencies that can be used to launder money, finance terrorists or evade taxes?
- Is it enough to include only custodian wallet providers and virtual currency exchanges in the list of obliged entities?
- Does the AMLD5 framework allow to pull enough cryptocurrency users into the light?
- Would it make sense to extend the scope of the Funds Transfer Regulation and/or the Cash Control Regulation as to include cryptocurrency transactions?
- Is there a need for a more comprehensive approach, introducing license requirements for cryptocurrency players?
- Is it not best to outright ban some activities or aspects linked to cryptocurrencies?
- Is the European level the appropriate level to tackle money laundering, terrorist financing and tax evasion via cryptocurrency transactions?

It is not our intention to give the definitive answer to all the questions raised. What we do intend is to give our analysis and to fuel the further debate.

### 5.2. Is the definition of virtual currencies under AMLD5 sufficient?

As a recall, the definition of virtual currencies under AMLD5 is the following: "*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*".

#### 5.2.1. Conclusions on the basis of the taxonomy

Referring back to our taxonomy of cryptocurrencies, we can conclude that almost all of the cryptocurrencies scrutinized fit within this definition. All of the cryptocurrencies are:

- a digital representation of value;
- decentralized, *i.e.* not issued or guaranteed by a central bank or a public authority;
- not attached to a legally established currency;

<sup>394</sup> It is not our intention to give a comprehensive list of all the relevant sub-questions instrumental to assessing the framework's adequacy. The selected questions allow to draw some preliminary conclusions though.

- not possessing the legal status of currency or money;
- electronically transferable, storable and tradeable.

The one element that could give rise to discussion is that of the cryptocurrencies having to be a means of exchange. The AMLD5 does not provide further guidance of what this means, but an acceptable interpretation is that the cryptocurrencies should be able to be used to facilitate the sale, purchase or trade of goods between parties and represent a standard of value that is accepted between the parties.<sup>395</sup>

Two questions arise.

Firstly, what if a cryptocurrency is not accepted as a means of exchange now, but there is no intrinsic limitation preventing it from becoming a means of exchange in the future? This is for instance relevant for cryptocurrencies that are apparently not used as a means of exchange now, such as IOTA and NEO. But that may change. All depends on the willingness of parties to accept the cryptocurrency as a standard of value in their mutual dealings. As soon as that happens, they become a means of exchange and tumble into the scope of the definition of "virtual currencies" under AMLD5. Therefore, from the perspective of combating money laundering, terrorist financing and tax evasion, there is no big issue: normally, committing one of these offences via cryptocurrencies implies having done an exchange, implying the cryptocurrency used is a means of exchange and is included in the scope of AMLD5.

Secondly, what if a cryptocurrency is a medium of exchange, but also and foremost an investment instrument? This is an extremely relevant question, as it is very clear from high volatility and various warnings from financial supervisors that some cryptocurrencies are considered an investment instrument by users, not in the least Bitcoin, which still has the highest market capitalisation of all cryptocurrencies. If the answer to this question would be that these cryptocurrencies are out of scope, this would mean that AMLD5's fruits all in all are very little. We argue against such an interpretation. AMLD5's definition requires cryptocurrencies to be accepted as a means of exchange. It does not say that this should be the only or predominant function of the cryptocurrency. Therefore, it does not matter if the cryptocurrency is also or predominantly an investment instrument. Also in that event, the cryptocurrency is included in the scope of AMLD5. Furthermore, an argument can be derived from the fiat currency framework: a fiat currency can also be acquired and held for investment (speculation) purposes; this does not change the fiat currency's primary status of being a fiat currency.

Therefore, we conclude that AMLD5's definition of virtual currencies is sufficient to combat money laundering, terrorist financing and tax evasion via the cryptocurrencies included in our taxonomy. Of course, that taxonomy is not exhaustive. Nevertheless, we believe that it is fairly representative for the cryptocurrencies that are out there, both from the perspective of market capitalisation and from the perspective of distinctive features. Therefore, we believe that our conclusion here, and the conclusions that follow below, should also be representative, although it cannot be ruled out that some conclusions may not or not to the same extent apply to cryptocurrencies that were not in scope of this research.

### 5.2.2. Other virtual currencies than cryptocurrencies

Virtual currencies within the scope of AMLD5 are those that can be transferred, stored and traded electronically. There is no requirement that virtual currencies are bi-directionally transferable or

---

<sup>395</sup> See: <https://www.investopedia.com/terms/m/mediumofexchange.asp>.

tradeable against fiat currencies. This means, for instance, that virtual currencies that can be acquired with fiat money and then used only in the virtual world to buy goods or services and/or that are transferable or tradeable only against other virtual currencies, are also included in the scope of the AMLD5 definition of virtual currencies.

However, legal doctrine rightly analysed that this inclusion in the scope of AMLD5's definition of virtual currencies does not help a lot looking at the list of obliged entities.<sup>396</sup> The analysis is that the list of obliged entities, and especially the reference to virtual currency exchanges as defined by AMLD5, shows that the scope of the anti-money laundering regulation of virtual currencies is limited to certain bi-directional scheme virtual currencies only. Other virtual currency schemes are not in scope, including virtual currency to virtual currency exchanges and virtual currencies used to attain goods and services without requiring exchange into legal tender or similar instruments, or the use of a custodian wallet provider<sup>397</sup>. This leaves a blind spot, allowing such activities to still result in money laundering or terrorist financing activities outside of the scope of AMLD5.

Is it a problem? Well, yes and no.

No, because it is arguable that some types of virtual currencies are of minor to no importance for money laundering or terrorist financing, for instance virtual currencies that can only be obtained and used in the virtual world and have no interaction with the real economy. This makes them not very useful for money laundering or terrorist financing purposes. Schemes allowing to acquire virtual currencies with fiat currency, but where the acquired virtual currency can only be used in the virtual environment suffer the same defect for purposes of money laundering or terrorist financing, given that no money can flow out of the system. Of course, it is possible that in such a scheme the acquired virtual currency can be used as a means of payment (e.g. when a person consents to receiving payment in virtual currency). Nevertheless, it is assessed that such a method is fairly unsuited for larger scale money laundering operations.<sup>398</sup> Therefore, arguably predominantly the schemes allowing to acquire virtual currency against fiat money and allowing to sell virtual currency against fiat money pose the biggest threat, as they can be linked to cash both at the entry into and the exit from the virtual sphere.

Yes, because the world of cryptocurrencies is a fast moving one and the network of acceptance of virtual currencies can grow, the Impact Assessment rightfully points out. If virtual currencies effectively become widely accepted and used, there might come a point in time when there will no longer be a need to convert virtual currencies back into fiat currencies. In other words, with a growing network of acceptance, the need to "cash-out" of virtual currencies and exchange them for fiat currencies might decrease over time. This trend would, according to the Impact Assessment, increase further if virtual currencies would become less volatile.

Therefore, it is important to closely follow-up and monitor the use cases of virtual currencies, and especially whether the use of virtual currencies within a virtual setting and without having to cash-out again becomes increasingly important.<sup>399</sup> When that would actually happen, the regulatory framework should follow and include these cases into its scope. Or, as the IMF points out more

---

<sup>396</sup> N. VANDEZANDE, *Virtual currencies: a legal framework*, Antwerp, Intersentia, 2018, 303.

<sup>397</sup> *Ibid.*

<sup>398</sup> N. VANDEZANDE, *Virtual currencies: a legal framework*, Antwerp, Intersentia, 2018, 278-279.

<sup>399</sup> Also see the IMF's advice: IMF Staff Discussion Note, "Virtual Currencies and Beyond: Initial Considerations", January 2016, <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>, 37.

broadly, the changing nature of the technology requires that regulation be flexible and can be adapted to evolving circumstances.<sup>400</sup>

### 5.3. Is it enough to include only custodian wallet providers and virtual currency exchanges in the list of obliged entities?

#### 5.3.1. State of play

We recall AMLD5's definitions of custodian wallet providers and virtual currency exchanges. These are respectively: "*an entity that provides services to safeguard private cryptographic keys on behalf of their customers, to hold, store and transfer virtual currencies*" and "*providers engaged in exchange services between virtual currencies and fiat currencies*".

Above we have identified the key players in the cryptocurrency market: users, miners, cryptocurrency exchanges, trading platforms, wallet providers, coin inventors and offerors.

Clearly, a number of these key players are not obliged entities under AMLD5.

#### 5.3.2. Users

Firstly, users are not obliged entities under AMLD5. Making them obliged entities would not make a lot of sense, as the AMLD framework for a large part focuses on intermediaries<sup>401</sup>. In any event, it would not be proportionate<sup>402</sup>. So, this is fine.

#### 5.3.3. Miners

Secondly, miners are also not obliged entities. And, as for users and for the same reasons, at first glance making them obliged entities would probably make little sense. According to the Impact Assessment, there are mainly two reasons for not considering miners as obliged entities. Firstly, miners are considered to be more a sort of technical service providers than gatekeepers between the virtual sphere and the real world. Secondly, miners are mostly located in China which would make any initiative largely impossible to enforce.

Nevertheless, two critical observations can be made here. Firstly, miners can be cryptocurrency users too, or, more commonly, parties who have made a new business out of mining cryptocurrencies to sell them for fiat currency or for other cryptocurrencies.<sup>403</sup> Along the same lines it is not inconceivable that criminals start mining cryptocurrencies to do the same - if they are not already doing this.<sup>404</sup> Mining Bitcoins is probably hard to do for criminals, given that it requires massive server power and substantial knowhow, but the same is not necessarily true for other cryptocurrencies, which can be easier to mine and still from the own living room so to speak.<sup>405</sup> Once mined, the cryptocurrencies can be linked to the real world. Secondly, we are not sure that mining is done from China predominantly. This is true for Bitcoins and probably also for other major coins requiring a certain level of

<sup>400</sup> IMF Staff Discussion Note, "Virtual Currencies and Beyond: Initial Considerations", January 2016, <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>, 26-27.

<sup>401</sup> It of course also includes rules on the beneficial ownership register. This can include info on cryptocurrency users to the extent these users are corporate or other legal entities.

<sup>402</sup> Also see on the US approach not to target users via regulation: T. MANDJEE, "Bitcoin, its Legal Classification and its Regulatory Framework", 15 J. Bus. & Sec. L. 157, 2016, <http://digitalcommons.law.msu.edu/jbsl>, 182.

<sup>403</sup> At which time they become offerors; see hereinafter.

<sup>404</sup> See with respect to cryptocurrencies running on permissionless, public blockchains: J. BLUMBERG, "We Need To Shut Bitcoin And All Other Cryptocurrencies Down. Here's Why.", March 2018, <https://www.forbes.com/sites/jasonbloomberg/2018/03/10/we-need-to-shut-bitcoin-and-all-other-cryptocurrencies-down-heres-why/#1dbed32b1bca>.

<sup>405</sup> See e.g. <https://cryptocurrencyfacts.com/asic-mining-basics/>; <https://www.coinwarz.com/cryptocurrency>.

sophistication to mine, but is it also true for the cryptocurrencies that are easier to mine? Because criminals may be attracted to the mining business, some commentators even advocate a "know your miner" policy, at least with respect to the cryptocurrencies that run on permissioned blockchain technology (because for those that run on permissionless blockchain technology, it is hard to find out their identities)<sup>406</sup>.

At present, the fact that the mining business is susceptible for illegitimate use, appears to be underestimated. Going forward, increasing attention should be devoted to the risks that accompany it, especially in light of the number of cryptocurrencies that is minable (i.e. based on a PoW consensus mechanism). The exclusion of miners from AMLD5's scope, currently leaves a blind spot in the EU's fight against money laundering, terrorist financing and tax evasion.

#### 5.3.4. Cryptocurrency exchanges

Thirdly, we have identified cryptocurrency exchanges as relevant players. Most of these allow users to sell their cryptocurrency for fiat currency or buy new cryptocurrency with fiat currency. It is clear from the definition of virtual currency exchanges in AMLD5 that cryptocurrency exchanges of this nature are obliged entities.

However, there also pure cryptocurrency exchanges, only accepting payments in other cryptocurrencies, usually Bitcoin. Insofar as these exchanges do not also qualify as custodian wallet providers, they remain out of AMLD5's scope because they have no dealings with fiat currency. This is a blind spot in the fight against money laundering, terrorist financing and tax evasion, because it can add an extra layer of disguise of the origin of the cryptocurrencies (when they later pass through an obliged entity) or simply allow that cryptocurrencies are used completely outside of the monitored system.

The atomic swap, which in its essence is a pure cryptocurrency exchange 2.0, because it can function without the need of a third party, deserves special emphasis. As other pure cryptocurrency exchanges it is outside of the scope of the AMLD 5 and, thus, a blind spot. Contrary to other exchanges, it is also hard to bring it into the scope, because of the absence of a middleman. Therefore, if this over time would become a successful platform through which criminals operate, it will be hard to find the right regulatory answer.

#### 5.3.5. Trading platforms

As a fourth player, we identified trading platforms, which function as a market place bringing together different cryptocurrency users that are either looking to buy or sell cryptocurrencies and allow them to interact directly. Such trading platforms are so-called "P2P exchanges" or "decentralised exchanges" and differ from cryptocurrency exchanges in a number of ways, as elaborated above. For the purposes of attaching regulation to these trading platforms it is important that they are not run by an entity or company that oversees and processes all trades, but they are operated exclusively by software (i.e. there is no central point of authority). This simply makes it very hard to regulate them and *a fortiori* to include them in the list of obliged entities. Again, this is a blind spot in the fight against money laundering, terrorist financing and tax evasion, for the same reasons as aforementioned with respect to pure cryptocurrency exchanges.

---

<sup>406</sup> J. BLUMBERG, "We Need To Shut Bitcoin And All Other Cryptocurrencies Down. Here's Why.", March 2018, <https://www.forbes.com/sites/jasonbloomberg/2018/03/10/we-need-to-shut-bitcoin-and-all-other-cryptocurrencies-down-heres-why/#1dbed32b1bca>.

### 5.3.6. Wallet providers

Next, we identified wallet providers as key players. We made a distinction between three types:

- hardware wallet providers that provide cryptocurrency users with specific hardware solutions to privately store their cryptographic keys;
- software wallet providers that provide cryptocurrency users with software applications allowing them to access the network, send and receive cryptocurrencies and locally save their cryptographic keys; and
- custodian wallet providers that take (online) custody of a cryptocurrency user's cryptographic keys.

As aforementioned, only custodian wallet providers, defined as entities that provide services to safeguard private cryptographic keys on behalf of their customers, to hold, store and transfer virtual currencies, are obliged entities under AMLD5. Hardware wallet providers and software wallet providers are not custodian wallet providers, as they do not safeguard keys on behalf of their customers, but merely provide the tools to customers to safeguard their cryptocurrencies themselves. So, again there is a blind spot in the fight against money laundering, terrorist financing and tax evasion. Users using software or hardware wallets escape AMLD5, as long as they also stay away from exchanges exchanging cryptocurrencies into fiat money.

### 5.3.7. Coin inventors

Sixthly, we identified coin inventors as key players. These were the individuals or organisations who have developed the technical foundations of a cryptocurrency and set the initial rules for its use. Often they remain unidentified, making them a hard category to target. On the other hand, it does not seem necessary to target them. As coin inventors, they are only the founding fathers of cryptocurrency schemes. They only provide the technological tools for others to work with. However, if and when they would take-up a different role, the situation might change. Depending on which role they take-up concretely they can then fall into one of the above categories or the below category.

### 5.3.8. Offerors

That brings us to the last category we identified: the offerors of cryptocurrencies, of course to the extent an offeror can be identified; some coins do not have an identifiable offeror. Coin offerors are individuals or organizations that offer coins to cryptocurrency users upon the coin's initial release, either against payment (i.e. through a crowd sale) or at no charge (i.e. in the framework of a specific (sign-up) program (e.g. Stellar)). When coins are offered this way, we speak of an initial coin offering in the true meaning of the word.<sup>407</sup>

Offerors are clearly not obliged entities under AMLD5. Moreover, they will most likely also not be caught by financial services laws, because it is difficult to include cryptocurrencies into the scope of these laws.<sup>408</sup> So, again, there is a blind spot in the fight against money laundering, terrorist financing and tax evasion.

<sup>407</sup> The terminology initial coin offering is often used as an umbrella term referring to all kinds of offerings, mostly of tokens. Here, it is used in its pure meaning: that of an offering of coins.

<sup>408</sup> See supra footnote 316. Going forward these offerors could be a useful connecting factor for financial services laws, if it would be decided to subject cryptocurrencies to financial services laws.

### 5.3.9. The initial question

Moving over to the initial question: is it enough to include only virtual currency exchanges and custodian wallet providers in the list of obliged entities under AMLD5?

What is certain is that there are relevant crypto players that are not caught by AMLD5<sup>409</sup>, sometimes because the legislator chose not to (this is true for software wallet providers and pure cryptocurrency exchanges that are not custodian wallet providers), but, so it seems, sometimes also because he did not pay a lot of attention to their existence and the potential risks involved (this is e.g. true for the trading platforms, that, admittedly, escape regulation anyway because there is no one to attach it to; for miners, hardware wallet providers and coin offerors). This leads to blind spots in the fight against money laundering, terrorist financing and tax evasion.<sup>410</sup>

Does it matter?

Maybe. It all depends on whether these blind spots are actually going to be exploited by criminals. Our estimation is that it would not be so surprising if persons with malicious intent would actually look up these blind spots in the shadow of AMLD5. If that would happen and it would appear to have a (material) adverse effect on the fight against money laundering, terrorist financing and tax evasion, there is definitely something to say for expanding the list of obliged entities with those players that were identified the weak spots or have great potential of being weak spots.<sup>411</sup> It is therefore important to closely follow-up on this and to intervene when required.

Meanwhile, an interesting thing to watch is the emergence of self-regulation.<sup>412</sup> There have been reports of crypto players voluntarily applying customer due diligence to maintain a leading commercial edge over others.<sup>413</sup> If that would become a more general trend, it could very well influence the assessment of whether or not a hard law approach, via an amendment of the list of obliged entities, is necessary.

## 5.4. Does the AMLD5 framework allow to pull enough cryptocurrency users into the light?

This brings us to the next question in need for an answer: does the AMLD5 framework allow to pull enough cryptocurrency users into the light? This question boils down to finding out how anonymous their actions can still be on the crypto market after AMLD5.

First, and as already mentioned before, under AMLD5 users that hold their virtual currencies via a custodian wallet provider or enter into virtual currency transactions via a virtual exchange platform can no longer be anonymous, because of the customer due diligence requirements vested upon the custodian wallet providers and virtual currency exchange platforms.

<sup>409</sup> Also see N. VANDEZANDE, *Virtual currencies: a legal framework*, Antwerp, Intersentia, 2018, 308.

<sup>410</sup> It is interesting to note that in the legislative process, as elaborated above, the suggestions made by the Committee on Legal Affairs of 18 January 2017 broadened the scope of the AMLD5, thus further limiting the blind spots. These suggestions were not picked up later on.

<sup>411</sup> A different perspective is that of unfair competition. It has been argued that bringing some virtual currency service providers under the scope of the AMLD5, whereas others, who provide similar services, escape, fosters unfair competition: N. VANDEZANDE, *Virtual currencies: a legal framework*, Antwerp, Intersentia, 2018, 309.

<sup>412</sup> See also: T. KEATINGE, D. CARLISLE and F. KEEN, "Virtual currencies and terrorist financing: assessing the risks and evaluating responses", study commissioned by the Directorate General for Internal Policies, Policy Department for Citizens' Rights and Constitutional Affairs, May 2018, 55-56 (electronically available via [http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL\\_STU\(2018\)604970\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf)).

<sup>413</sup> See for the US: T. MANDJEE, "Bitcoin, its Legal Classification and its Regulatory Framework", 15 J. Bus. & Sec. L. 157, 2016, <http://digitalcommons.law.msu.edu/jbsl>, 215.

However, users using hardware or software wallets and for instance trade via a P2P network or via any other way than through a virtual currency exchange platform, can still operate anonymously.<sup>414</sup>

For those crypto players deliberately left out of the scope of AMLD5, the legislator is of course aware of this risk.<sup>415</sup> The solution proposed to address it is that national FIUs should be able to associate virtual currency addresses to the identity of the owner of virtual currencies and that the possibility for users to self-declare to designated authorities on a voluntary basis should be further assessed.

Concretely, however, as aforementioned, no immediate action is taken. The only achievement is a requirement for the Commission to include in its next supranational risk assessment, which is due by 26 June 2019, if necessary, appropriate proposals, including, where appropriate, with respect to virtual currencies, empowerments to set-up and maintain a central database registering users' identities and wallet addresses accessible to FIUs, as well as self-declaration forms for the use of virtual currency users. This seems to point in the direction of a system of voluntary registration, instead of mandatory registration (which was also an option brought forward by the Impact Assessment), if at all any system will be retained following the next supranational risk assessment. Bearing in mind the timing of that assessment and that of potential subsequent AMLD amendments coming into force, it is clear that nothing is to be expected from Europe very soon.

This is a very soft approach towards unveiling anonymity of users and linking them to cryptocurrencies and cryptocurrency transactions. First, it is not sure that a system of registration will be introduced. Secondly, if ever a system would be put in place, it would be a voluntary one. It can very much be doubted if the category that should be targeted the most, users of cryptocurrencies for illicit purposes, would voluntarily register as a user. That would be like trusting the thief to come to the police station voluntarily after committing a theft. All in all, the approach taken is therefore not very convincing if the legislator is truly serious about unveiling anonymity of cryptocurrency users to make the combat against money laundering, terrorist financing and tax evasion more effective. A mandatory registration and a pre-set date as of which it applies, is to that end a much better approach, albeit of course more intrusive.

In this respect we also note that some cryptocurrencies that are now on the market, such as Dash and Monero, are fully anonymous, whereas others, such as Bitcoin and the like are pseudo-anonymous, basically meaning that if great effort is made and complex techniques are deployed, it is possible for authorities to find out users' identities. These fully anonymous cryptocurrencies are designed to stay in the dark and outside of the scope of authorities. After AMLD5 this will no longer be possible to the fullest extent: the cryptocurrency users that want to convert their cryptocurrency into fiat currency via a virtual currency exchange or hold their portfolio via a custodian wallet provider, will be subject to customer due diligence. But, as aforementioned, there is still a whole world outside of these new obliged entities under AMLD5. It goes without saying that this may sound particularly interesting for criminals seeking for new ways to launder money, finance terrorists or evade taxes. If a legislator does not want to outright ban these cryptocurrencies - and for not imposing such a ban a good argument is that cash is also fully anonymous and lawful - the only way to find out who uses them is to require users to register mandatorily. For reasons of proportionality it could then be considered to make the registration subject to a materiality threshold.

---

<sup>414</sup> See also: T. KEATINGE, D. CARLISLE and F. KEEN, "Virtual currencies and terrorist financing: assessing the risks and evaluating responses", study commissioned by the Directorate General for Internal Policies, Policy Department for Citizens' Rights and Constitutional Affairs, May 2018, 38-42 (electronically available via [http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL\\_STU\(2018\)604970\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf)).

<sup>415</sup> The legislator admits this explicitly in the Commission Proposal and the proposed Preamble 7 of the Compromise Text.



Of course, naivety is not in its place here. The adequacy of a mandatory registration of users, whether or not of fully anonymous or pseudo-anonymous cryptocurrencies, depends on the users' compliance with the registration requirement. Such compliance will partly depend on an adequate sanctioning toolbox in the event of breach, which is a necessity. But how do we detect a breach? Is this at all possible outside of the context of randomly bumping into it, at least when fully anonymous cryptocurrencies are concerned? This remains a loose end, even in a system of mandatory registration, and even when a ban would be imposed on technology fully anonymising cryptocurrencies, which will be elaborated below.

An interesting line of thought here is again self-regulation: crypto intermediaries could decide for themselves not to accept fully anonymous cryptocurrencies in the course of their business. That could give them a reputational advantage over others, possibly also leading to a commercial advantage. If that would become a more general trend, it could have an influence on the assessment of whether or not a hard law approach, via registration of users, is necessary.

### **5.5. Would it make sense to extend the scope of the Funds Transfer Regulation and/or the Cash Control Regulation as to include cryptocurrency transactions?**

Another question is whether it would make sense to extend the scope of the Funds Transfer Regulation and/or the Cash Control Regulation as to include cryptocurrency transactions.

The answer relating to the Cash Control Regulation can be short: it doesn't. Cryptocurrencies are normally not moved physically, making the Cash Control Regulation not such a good instrument to target cryptocurrency movements.

The answer relating to the Funds Transfer Regulation is more nuanced. This regulation basically aims at making sure that all relevant information accompanying fund transfers is there, allowing an adequate money laundering and terrorist financing check. It seems conceivable to develop and roll-out a similar system for cryptocurrency transactions. The entities that would have to fulfil the requirements could be the intermediaries through which the transactions run. Going forward, this could be a valuable add-on to the existing framework.

### **5.6. Is there a need for a more comprehensive approach, introducing license requirements for cryptocurrencies?**

A difficult question is whether a more intrusive approach towards regulating the crypto market is warranted. As we have seen throughout this research, the EBA is a strong advocate of developing a tailored and more comprehensive framework for cryptocurrencies in time, including license requirements for cryptocurrency service providers. Part of such framework would be to create a virtual currency scheme governance authority that is accountable to the regulator.<sup>416</sup> An interesting line of thought for future regulation could indeed be to create or impose a "middleman", where the use of blockchain or other distributed ledger technology has cut out such middleman, as this will allow the regulator to attach regulation to an identifiable person, thus contributing to enhanced compliance and effective enforcement.

---

<sup>416</sup> See 4.2.4 The coming of age of the inclusion of cryptocurrencies into AMLD5.

Examples of tailored regimes for inspirational purposes can also be found abroad, e.g. the New York State Virtual Currency Business Activity license<sup>417</sup> or the proposed Maltese Virtual Currency Act and Framework for the Certification of Distributed Ledger Technology Platforms and Related Service Providers<sup>418</sup>.

The IMF also invited regulators to consider a more comprehensive approach.<sup>419</sup>

A similar call can be found in very recent PhD research.<sup>420</sup> Along the same lines, some legal doctrine suggested to revise the e-money framework and include cryptocurrencies into that revised framework.<sup>421</sup> Other legal doctrine, however, is more reluctant and advocates that a hard-touch regulatory approach can hinder the potential welfare-enhancing innovations coming from the ecosystem of cryptocurrencies<sup>422</sup>. In line herewith, it was raised that the benefits of regulation should be weighed with the costs associated therewith, and the potential deterrent effect on emerging businesses.<sup>423</sup>

A more comprehensive approach would include in any event the anti-money laundering and counter terrorist financing framework, because it would refer to AMLD5. Because of that, for the purposes of this research, the question is very interesting, but out of scope. Therefore, we will not elaborate it further.

## 5.7. Is it not best to introduce an outright ban for some aspects linked to some cryptocurrencies?

The question arises whether some aspects relating to some cryptocurrencies should not just be banned and criminally sanctioned. To mind come the mixing process attached to Dash's feature PrivateSend and Monero's RingCT, stealth addresses and Kovri-project. In essence, these features are designed to make cryptocurrency users untraceable. But why is such degree of anonymity truly necessary? Would allowing this not veer too far towards criminals? Imposing a ban for such aspects surrounding cryptocurrencies that are aimed at making it impossible to verify their users and criminally sanctioning these aspects seems to be in line with the Council's conclusions of April 2018

<sup>417</sup> The regulatory framework can be accessed via: <https://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf>. A concise analysis can be found in P. VALCKE, N. VANDEZANDE and N. VAN DE VELDE, "The evolution of third party payment providers and cryptocurrencies under the EU's upcoming PSD2 and AMLD4", 2015, Swift Institute Working Paper No. 2015-001, 64-65.

<sup>418</sup> Malta positions itself as a leader in distributed ledger technology regulation. In February 2018 the Parliamentary Secretary for Financial Services, Digital Economy and Innovation within the Office of the Prime Minister, issued a consultation document on the establishment of a Malta Digital Innovation Authority, a Framework for the Certification of Distributed Ledger Technology Platforms and Related Service Providers, and a Virtual Currency Act. The consultation was recently closed on 9 March 2018, but the results have yet to be made public. It will be interesting to follow-up on this and assess the future framework for potential inspiration of future EU legislation. See: Consultation Document on "The establishment of the Malta Digital Innovation Authority; the Framework for the Certification of Distributed Ledger Technology Platforms and Related Service Providers; and a Virtual Currency Act", February 2018, [https://meae.gov.mt/en/Public\\_Consultations/OPM/Documents/PS%20FSDEI%20-%20DLT%20Regulation%20Document%20OUTPUT.PDF](https://meae.gov.mt/en/Public_Consultations/OPM/Documents/PS%20FSDEI%20-%20DLT%20Regulation%20Document%20OUTPUT.PDF); also see S. OZELLI, "Malta Emerges as World's Cryptocurrency Hub Despite EU's TAX3 Investigation: Expert Take", June 2018, <https://cointelegraph.com/news/malta-emerges-as-world-s-cryptocurrency-hub-despite-eu-s-tax3-investigation-expert-take>.

<sup>419</sup> IMF Staff Discussion Note, "Virtual Currencies and Beyond: Initial Considerations", January 2016, <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>, 36.

<sup>420</sup> N. VANDEZANDE, *Virtual currencies: a legal framework*, Antwerp, Intersentia, 2018, 310.

<sup>421</sup> P. VALCKE, N. VANDEZANDE and N. VAN DE VELDE, "The evolution of third party payment providers and cryptocurrencies under the EU's upcoming PSD2 and AMLD4", 2015, Swift Institute Working Paper No. 2015-001, 59.

<sup>422</sup> See H. NABILOU and A. PRÜM, "Ignorance, debt and cryptocurrencies: the old and the new in the law and economics of concurrent currencies", May 2018, 40p. (electronically available via <https://ssrn.com/abstract=3121918>).

<sup>423</sup> T. MANDJEE, "Bitcoin, its Legal Classification and its Regulatory Framework", 15 J. Bus. & Sec. L. 157, 2016, <http://digitalcommons.law.msu.edu/jbsl>, 213.

on how to respond to malicious cyber activities, under which that the use of ICT for malicious purposes is unacceptable.<sup>424</sup>

Whatever the answer may be, we must again avoid being naive: even if a ban would be imposed, how do we detect a breach, given that the purpose of the object of the ban just is to obscure identities?<sup>425</sup> Nevertheless, it would be worthwhile to consider introducing a ban. If authorities then bump into the prohibited activities, they have a legal basis for prosecution, insofar not yet available. Possibly, imposing a ban could also have a deterrent effect. Of course, again there is the tension with data protection, but arguably in the balance of things the interest of authorities and society to more effectively combat money laundering, terrorist financing and tax evasion via well-defined specific bans outweighs the interest of persons desiring to hide their identities completely.

In any event, imposing a ban should always be focused on specific aspects facilitating the illicit use of cryptocurrency too much. We are not in favour of general bans on cryptocurrencies or barring the interaction between cryptocurrency business and the formal financial sector as a whole, such as is the case in China for example.<sup>426</sup> That would go too far in our opinion. As long as good safeguards are in place protecting the formal financial sector and more in general society as a whole, such as rules combating money laundering, terrorist financing, tax evasion and maybe a more comprehensive set of rules aiming at protecting legitimate users (such as ordinary consumers and investors), that should be sufficient.

## 5.8. Is the European level the appropriate one to tackle money laundering, terrorist financing and tax evasion via cryptocurrency transactions?

Cryptocurrency transactions and crypto players are not bound by borders. Therefore, it is certain that the national level is not the right level to address money laundering, terrorist financing and tax evasion via cryptocurrencies. The European level is more appropriate. Even more appropriate, however, is the international level, as crypto activity is also not limited by the European border. Therefore, international collaboration, e.g. in the context of the UN Office on Drugs and Crime, the FATF and the Egmont Group, is crucial to successfully impose and enforce rules on combating money laundering, terrorist financing and tax evasion.<sup>427</sup>

From a regulatory perspective, a G20 initiative on a global framework for regulating and overseeing cryptocurrencies, to the extent necessary, would be welcome.<sup>428</sup> As it stands now, a first step toward a unified regulation of cryptocurrencies is expected to be taken at this level<sup>429</sup> in July 2018.<sup>430</sup> It will be

<sup>424</sup> See: <http://www.consilium.europa.eu/en/press/press-releases/2018/04/16/malicious-cyber-activities-council-adopts-conclusions/>.

<sup>425</sup> With respect to Dash's PrivateSend, a line of thought here could be to assess to what extent the masternodes could be targeted. If that would be possible, sanctioning would arguably be easier: if you shut the masternodes down who facilitate the mixing process, the process in itself may not be available any longer.

<sup>426</sup> See e.g. IMF Staff Discussion Note, "Virtual Currencies and Beyond: Initial Considerations", January 2016, <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>, 28 and 35.

<sup>427</sup> And probably, more work needs to be done here: see IMF Staff Discussion Note, "Virtual Currencies and Beyond: Initial Considerations", January 2016, <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>, 36; also see P. VALCKE, N. VANDEZANDE and N. VAN DE VELDE, "The evolution of third party payment providers and cryptocurrencies under the EU's upcoming PSD2 and AMLD4", 2015, Swift Institute Working Paper No. 2015-001, 74 and 76.

<sup>428</sup> T. MANDJEE, "Bitcoin, its Legal Classification and its Regulatory Framework", 15 J. Bus. & Sec. L. 157, 2016, <http://digitalcommons.law.msu.edu/jbsl>, 216; S. TEAGUE, "G20 ministers wrestle with cryptocurrency oversight", 29 March 2018, [https://www.euromoney.com/article/b17jt5vnb3fn3m/g20-ministers-wrestle-with-cryptocurrency-oversight?utm\\_source=FX%20this%20week%20v2&utm\\_medium=email%20editorial&utm\\_content=Editorial&utm\\_campaign=636579242347129780&utm\\_term=G20%20ministers%20wrestle%20with%20cryptocurrency%20oversight](https://www.euromoney.com/article/b17jt5vnb3fn3m/g20-ministers-wrestle-with-cryptocurrency-oversight?utm_source=FX%20this%20week%20v2&utm_medium=email%20editorial&utm_content=Editorial&utm_campaign=636579242347129780&utm_term=G20%20ministers%20wrestle%20with%20cryptocurrency%20oversight).

<sup>429</sup> In a communiqué issued in preparation of the last G20 meeting in March 2018, the Financial Stability Board ("**FSB**") pointed out that its initial assessment is that crypto-assets do not pose risks to global financial stability at this time, though this could change in the future. At the same time the FSB stressed that crypto-assets raise a host of issues around consumer and investor protection, as well as their use

interesting to see which regulatory proposals make it to the regulatory drawing board. In any event, it would be good to see the EU take a leading role in this context and, to the extent feasible, lead by example through already adopting EU standards for cryptocurrencies.

---

to shield illicit activity and for money laundering and terrorist financing, which need to be addressed. See: FSB, "Communiqué to G20 Finance Ministers and Central Bank Governors", 13 March 2018, <http://www.fsb.org/wp-content/uploads/P180318.pdf>.

<sup>430</sup> The G20 asked the FSB, in consultation with other international standard-setting bodies, including CPMI and IOSCO, and FATF to report in July 2018 on their work on crypto-assets (see: G20, Communiqué, 19-20 March 2018, [https://g20.org/sites/default/files/media/communique\\_-\\_fmcdbg\\_march\\_2018.pdf](https://g20.org/sites/default/files/media/communique_-_fmcdbg_march_2018.pdf)). See also: N. DE, "G20 Calls for Crypto Regulation Recommendations By July", March 2018, <https://www.coindesk.com/g20-calls-crypto-regulation-recommendations-july/>; D. POLLOCK, "G20 and Cryptocurrencies: Baby Steps Towards Regulatory Recommendations", March 2018, <https://cointelegraph.com/news/g20-and-cryptocurrencies-baby-steps-towards-regulatory-recommendations>; C. GEORGACOPOULOS, "Banks And Cryptocurrencies Global Evaluation: Europe", April 2018, <https://cointelegraph.com/news/banks-and-cryptocurrencies-global-evaluation-europe>.

## 6. WHAT ABOUT BLOCKCHAIN?

The reader will have noticed that our overview and assessment of the regulatory framework almost entirely relates to cryptocurrencies. This has been done deliberately so.

As aforementioned and evidenced throughout this research, blockchain is technology on which a cryptocurrency can run. The scope of blockchain is, however, much wider than that of cryptocurrencies. It can be applied in a large variety of sectors (e.g. trade and commerce, healthcare, governance, ...), has numerous potential promising applications, e.g. relating to pledging of collateral, the registration of shares, bonds and other assets<sup>431</sup>, the operation of land registers, etc.

Therefore, it would be too blunt to associate blockchain with money laundering, terrorist financing or tax evasion. It is just technology, which is not designed to launder money, facilitate terrorist financing or evade taxes, and has numerous applications throughout the whole lawful economy. It would not be wise to discourage future innovations in this respect by submitting blockchain and fintechs exploring its use cases to burdensome requirements, simply because of one of the applications using blockchain technology, cryptocurrencies, is used illicitly by some<sup>432</sup>. Admittedly, cryptocurrencies are the first well known application putting blockchain technology into the spotlight, but nowadays blockchain has clearly outgrown the context of cryptocurrencies.

Therefore, we suggest to leave blockchain be from a money laundering, terrorist financing and tax evasion perspective and focus on the illicit use cases of cryptocurrencies.

---

<sup>431</sup> CPMI, "Digital currencies", November 2015, <https://www.bis.org/cpmi/publ/d137.pdf>, 15.

<sup>432</sup> Also see P. VALCKE, N. VANDEZANDE and N. VAN DE VELDE, "The evolution of third party payment providers and cryptocurrencies under the EU's upcoming PSD2 and AMLD4", 2015, Swift Institute Working Paper No. 2015-001, 76 and 77; G. LILIENTHAL and N. AHMAD, "Bitcoin: is it really coinage?", 2018, Computer and Telecommunications Law Review, 24(3), 49-56.

## REFERENCES

- ABIOLA, L. K., 'Ethereum (ETH) Co-Founder Provides Answer To Long-Lived Supply Limit Question', April 2018, <https://oracletimes.com/ethereum-eth-co-founder-provides-answer-to-long-lived-supply-limit-question/>.
- ADAMS, C., "Stellar Lumens Vs Ripple", March 2018, <https://www.investinblockchain.com/stellar-lumens-vs-ripple/>.
- ANTONOVICI, A., "Cardano's Emurgo and SK's Metaps Plus Partner to Accept ADA", May 2018, <https://cryptovest.com/news/cardanos-emurgo-and-sks-metaps-plus-partner-to-accept-ada/>.
- ASOLO, B., "What are Atomic Swaps?", May 2018, <https://www.cryptocompare.com/coins/guides/what-are-atomic-swaps/>.
- BANQUE DE FRANCE, "Les dangers liés au développement des monnaies virtuelles: l'exemple de bitcoin", in Focus, no. 10, 5 December 2013, [https://www.banque-france.fr/uploads/tx\\_bdfgrandesdates/Focus-10-stabilite-financiere.pdf](https://www.banque-france.fr/uploads/tx_bdfgrandesdates/Focus-10-stabilite-financiere.pdf), 6p.
- BANTEKAS, I. and S. NASH, S., *International Criminal Law*, Routledge-Cavendish, 2007, 640p.
- BLUMBERG, J., "We Need To Shut Bitcoin And All Other Cryptocurrencies Down. Here's Why.", March 2018, <https://www.forbes.com/sites/jasonbloomberg/2018/03/10/we-need-to-shut-bitcoin-and-all-other-cryptocurrencies-down-heres-why/#1dbed32b1bca>.
- BOLLEN, R., "The Legal Status of Online Currencies: Are Bitcoins the Future?", *Journal of Banking and Finance Law and Practice* 2013, 38p. (electronically available via <http://ssrn.com:80/abstract=2285247>).
- BOVAIRD, C., "What to know before trading Monero", May 2017, <https://www.coindesk.com/what-to-know-before-trading-monero/>.
- BOVAIRD, C., "Why the crypto market has appreciated more than 1,200% this year", November 2017, <https://www.forbes.com/sites/cbovaire/2017/11/17/why-the-crypto-market-has-appreciated-more-than-1200-this-year/#3906c8d6eed3>.
- BRATSPIES, R.M., "Cryptocurrencies and the Myth of the Trustless Transaction", March 2018, 49p. (electronically available via <https://ssrn.com/abstract=3141605>).
- BRITO, J., SHADAB, H., and CASTILLO, A., "Bitcoin financial regulation: securities, derivatives, prediction markets & gambling", 24 July 2014, 78p. (electronically available via [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2423461](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2423461)).
- BRYANS, D., "Bitcoin and Money Laundering: Mining for and Effective Solution" *Indiana Law Journal*, 2014, Vol. 89: Iss. 1, Article 13, 32p. (electronically available via <https://www.repository.law.indiana.edu/ilj/vol89/iss1/13>).
- BUCHKO, S., "How Long do Bitcoin Transactions Take?", December 2017, <https://coincentral.com/how-long-do-bitcoin-transfers-take/>.
- BUCK, J., "First BTC-LTC Lightning Network Swap Completed, Huge Potential", November 2017, <https://cointelegraph.com/news/first-btc-ltc-lightning-network-swap-completed-huge-potential>.
- CHOHAN, U.W., "International Law Enforcement Responses to Cryptocurrency Accountability: Interpol Working Group", Discussion Paper, 3 April 2018, 8p.

- CITY OF ZION, "Coopetition: A New Approach to Decentralization", December 2017, <https://medium.com/proof-of-working/decentralization-from-coopetition-b10d7ce3b9d>.
- COM/2016/0450, "Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC", 6 July 2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016PC0450&qid=1523358551244&from=EN>.
- COMMISSION STAFF WORKING DOCUMENT Accompanying the document "Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border situations", COM(2017) 340 final, Annex, Part 2, [https://eur-lex.europa.eu/resource.html?uri=cellar:d4d7d30e-5a5a-11e7-954d-01aa75ed71a1.0001.02/DOC\\_1&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:d4d7d30e-5a5a-11e7-954d-01aa75ed71a1.0001.02/DOC_1&format=PDF), 85.
- COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document "Proposal for a Directive of the European Parliament and the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC", SWD/2016/0223 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0223&from=EN>.
- Consultation Document on "The establishment of the Malta Digital Innovation Authority; the Framework for the Certification of Distributed Ledger Technology Platforms and Related Service Providers; and a Virtual Currency Act", February 2018, [https://meae.gov.mt/en/Public\\_Consultations/OPM/Documents/PS%20FSDEI%20-%20DLT%20Regulation%20Document%20OUTPUT.PDF](https://meae.gov.mt/en/Public_Consultations/OPM/Documents/PS%20FSDEI%20-%20DLT%20Regulation%20Document%20OUTPUT.PDF).
- Council conclusions on the fight against the financing of terrorism, 12 February 2016, <http://www.consilium.europa.eu/en/press/press-releases/2016/02/12/conclusions-terrorism-financing/>.
- Council Directive (EU) 2016/1164 of 12 July 2016 laying down rules against tax avoidance practices that directly affect the functioning of the internal market, *OJ L* 193, 19 July 2016 (electronically available via <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1164&from=EN>).
- Council Directive (EU) 2016/2258 of 6 December 2016 amending Directive 2011/16/EU as regards access to anti-money-laundering information by tax authorities, *OJ L* 342, 16 December 2016, 1 (electronically available via <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L2258&from=EN>).
- Council Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC, as amended from time to time, as regards mandatory automatic exchange of information in the field of taxation; this Directive was very recently, on 25 May 2018, amended again with rules relating to the mandatory automatic exchange of information in the field of taxation for reportable cross-border arrangements and reporting duties of intermediaries (see a first analysis: <https://www.tiberghien.com/en/1282/new-reporting-obligation-for-cross-border-arrangements-council-directive-approved-25-may-2018>).
- Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering, *OJ L* 166, 28 June 1991, 77 (electronically available via <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31991L0308&from=EN>).

- CPMI, “Digital currencies”, November 2015, <https://www.bis.org/cpmi/publ/d137.pdf>, 21p.
- CPMI, “Distributed ledger technology in payment, clearing and settlement – An analytical framework”, February 2017, <https://www.bis.org/cpmi/publ/d157.pdf>, 23p.
- DANNEN, C., *Introducing Ethereum and Solidity – Foundations of Cryptocurrency and Blockchain Programming for Beginners*, Apress, 2017, 185p.
- DE, N., “G20 Calls for Crypto Regulation Recommendations By July”, March 2018, <https://www.coindesk.com/g20-calls-crypto-regulation-recommendations-july/>.
- Delaware General Assembly, Senate Bill 69, <https://legis.delaware.gov/BillDetail?legislationId=25730>;
- 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, *OJ L* 141, 5 juni 2015, 73 (electronically available via <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L0849&from=En>).
- Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering, *OJ L* 344, 28 December 2001, 76, (electronically available via [https://eur-lex.europa.eu/resource.html?uri=cellar:57ce32a4-2d5b-48f6-adb0-c1c4c7f7a192.0004.02/DOC\\_1&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:57ce32a4-2d5b-48f6-adb0-c1c4c7f7a192.0004.02/DOC_1&format=PDF)).
- 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, *OJ L* 309, 25 November 2005, 15 (electronically available via <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005L0060&from=EN>).
- DUPONT, B., “The cyber security environment to 2022 Trends, drivers and implications”, a study prepared for The National Cyber Security Directorate, Public Safety Canada, 2012, 44p. (electronically available via <http://ssrn.com/abstract=2208548>).
- EBA, “EBA Opinion on ‘virtual currencies’”, 4 July 2014, <https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf>, 46p.
- ECB, “Virtual Currency Schemes”, October 2012, <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>, 53p.
- ECB, “Virtual Currency Schemes – a further analysis”, February 2015, <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>, 37p.
- Enria, A., Chairperson of EBA, “Designing a Regulatory and Supervisory Roadmap for FinTech”, 9 March 2018, <http://www.eba.europa.eu/documents/10180/2151635/Andrea+Enria%27s+speech+on+FinTech+at+Copenhagen+Business+School+090318.pdf>, 11p.
- EP Report on the proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC, 9



- March 2017, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0056+0+DOC+XML+V0//EN#title1>.
- ESMA, EBA & EIOPA, "Warning on the risks of Virtual Currencies" [https://www.esma.europa.eu/sites/default/files/library/esma50-164-1284\\_joint\\_esas\\_warning\\_on\\_virtual\\_currenciesl.pdf](https://www.esma.europa.eu/sites/default/files/library/esma50-164-1284_joint_esas_warning_on_virtual_currenciesl.pdf), 3p.
  - ETTO, F., "Know Your Coins: Public vs. Private Cryptocurrencies", September 2017, <https://www.nasdaq.com/article/know-your-coins-public-vs-private-cryptocurrencies-cm849588>.
  - European Parliament legislative resolution of 19 April 2018 on the proposal for a directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC (COM(2016)0450 – C8-0265/2016 – 2016/0208(COD)), <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2018-0178+0+DOC+PDF+V0//EN>.
  - EY, "IFRS – Accounting for crypto-assets", March 2018, <http://eyfinancialservicesthoughtgallery.ie/wp-content/uploads/2018/03/EY-IFRS-Accounting-for-crypto-assets.pdf>, 21p.
  - EY, "Research: initial coin offerings (ICOs)", December 2017, [http://www.ey.com/Publication/vwLUAssets/ey-research-initial-coin-offerings-icos/\\$File/ey-research-initial-coin-offerings-icos.pdf](http://www.ey.com/Publication/vwLUAssets/ey-research-initial-coin-offerings-icos/$File/ey-research-initial-coin-offerings-icos.pdf), 43p.
  - FATF, "International standards on combating money laundering and the financing of terrorism & proliferation. The FATF Recommendations", February 2012, [http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF\\_Recommendations.pdf](http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf), 132p.
  - FATF, "Report on emerging terrorist financing risks", October 2015, <http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf>, 47p.
  - FATF, "The Forty Recommendations", 20 June 2003, <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202003.pdf>, 7p.
  - FATF, "Virtual Currencies – Key Definitions and Potential AML/CFT Risks", June 2014, <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>, 15p.
  - Faulkner, J., *Getting started with Cryptography in .NET*, München BookRix, 2016, 121p.
  - FINCK, M., "Blockchains and Data Protection in the European Union", Max Planck Institute for Innovation & Competition Research Paper No. 18-01, 30 November 2017, 32p. (electronically available via <https://ssrn.com/abstract=3080322>).
  - FINMA, "Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)", February 2018, [https://www.finma.ch/en/~/\\_media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=en](https://www.finma.ch/en/~/_media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=en), 11p.
  - FLEDER, M., KESTER, M.S., and PILAI, S., "Bitcoin Transaction Graph Analysis", January 2014, 8p. (electronically available via <http://people.csail.mit.edu/spillai/data/papers/bitcoin-transaction-graph-analysis.pdf>).

- FLOYD, D., “\$6.3 Billion: 2018 ICO Funding Has Passed 2017’s Total”, April 2018, <https://www.coindesk.com/6-3-billion-2018-ico-funding-already-outpaced-2017/>).
- FSB, “Communiqué to G20 Finance Ministers and Central Bank Governors”, 13 March 2018, <http://www.fsb.org/wp-content/uploads/P180318.pdf>.
- G20, Communiqué, 19-20 March 2018, [https://g20.org/sites/default/files/media/communique\\_-\\_fmcbg\\_march\\_2018.pdf](https://g20.org/sites/default/files/media/communique_-_fmcbg_march_2018.pdf).
- GEORGACOPOULOS, C., “Banks And Cryptocurrencies Global Evaluation: Europe”, April 2018, <https://cointelegraph.com/news/banks-and-cryptocurrencies-global-evaluation-europe>.
- GLAZER, P., “An Overview of Privacy Coins”, February 2018, <https://hackernoon.com/an-overview-of-privacy-tokens-19f6af8077b7>.
- GOLDBERG, S., “Mythbusting: Blockchain and Cryptocurrencies Edition”, May 2018, <http://paymentsjournal.com/mythbusting-blockchain-and-cryptocurrencies-edition/>.
- GRINBERG, R., "Bitcoin: An Innovative Alternative Digital Currency", Hastings Science & Technology Law Journal, 2011, Vol. 4, 50p. (electronically available via [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1817857](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1817857)).
- GUP, B.E, "What Is Money? From Commodities to Virtual Currencies/Bitcoin" (14 March 2014), 12p. (electronically available via [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2409172](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2409172)).
- HACKER, P. and THOMALE, C., “Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law”, November 2017, 45p. (electronically available via <https://ssrn.com/abstract=3075820>).
- HAUBEN, C., “Bitcoin en EU-recht: de virtuele vreemde eend in de bijt” in M. E. STORME and F. HELSEN (eds.), *Innovatie en disruptie in het economisch recht*, Antwerpen, Intersentia , 2017, 79-104.
- HELLER, D., “The implications of digital currencies for monetary policy”, in-depth analysis commissioned by the Directorate General for Internal Policies, Policy Department A: Economic and Scientific Policy, May 2017, 12p. (electronically available via [http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/602048/IPOL\\_IDA\(2017\)602048\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/602048/IPOL_IDA(2017)602048_EN.pdf)).
- HERLIN-KARNELL, E., and RYDER, N., “The robustness of EU Financial Crimes Legislation: A Critical review of the EU and UK Anti-Fraud and Money Laundering Scheme”, 2017, European Business Law Review, No. 4, 1-39.
- HIGGINS, S., “How True Anonymity Made Darkcoin King of the Altcoins”, May 2014, <https://www.coindesk.com/true-anonymity-darkcoin-king-altcoins/>.
- HILEMAN, G. and RAUCHS, M., “Global Cryptocurrency Benchmarking Study”, Cambridge Centre for Alternative Finance, 2017, [https://www.jbs.cam.ac.uk/fileadmin/user\\_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf](https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf), 115p.
- HOLDEN, W., “Bringing Blockchain to Land Registry”, January 2018, <https://www.blockchain-expo.com/2018/01/blockchain/bringing-blockchain-land-registry/>.
- HOUBEN, R., "Bitcoin: there two sides to every coin", ICCLR, Vol. 26, Issue 5, 2015, 193-208.

- IMF Staff Discussion Note, "Virtual Currencies and Beyond: Initial Considerations", January 2016, <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>, 42p.
- JAGATI, S., "Ethereum's Proof of Stake Protocol Under Review", April 2018, <https://cryptoslate.com/ethereums-proof-of-stake-protocol-in-review/>.
- JAYACHANDRAN, P. "The difference between public and private blockchain", May 2017, <https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/>.
- KAPLAN, A., "Who accepts Ethereum as payment 2018 (List of companies that accept Ethereum)", May 2018, <https://smartereum.com/2072/accepts-ethereum-payment-2018-list-companies-accept-ethereum-mon-may-28/>.
- KAPLANOV, N.M., "Nerdy Money: Bitcoin, the private digital currency, and the case against its regulation", Temple Law Review 2012, 46p. (electronically available via [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2115203](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2115203)).
- KEATINGE, T., CARLISLE, D., and KEEN, F., "Virtual currencies and terrorist financing: assessing the risks and evaluating responses", study commissioned by the Directorate General for Internal Policies, Policy Department for Citizens' Rights and Constitutional Affairs, May 2018, 87p. (electronically available via [http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL\\_STU\(2018\)604970\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf)).
- KHATWANI, S., "NEO Cryptocurrency: Everything You Need to Know about China Ethereum", December 2017, <https://coinsutra.com/neo-cryptocurrency/>.
- KIAYIAS, A., RUSSEL, A., DAVID, B. and OLIYNYKOV, R., "Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol", August 2017, [https://iohk.io/research/papers/?\\_hstc=64163184.47e0ede3cd3368ac41d33e513fea0c1b.1525905532910.1527544936508.1527699072699.9&\\_hssc=64163184.7.1527699072699&\\_hsfp=2761973715#9BKRHCSI](https://iohk.io/research/papers/?_hstc=64163184.47e0ede3cd3368ac41d33e513fea0c1b.1525905532910.1527544936508.1527699072699.9&_hssc=64163184.7.1527699072699&_hsfp=2761973715#9BKRHCSI).
- Laga, "Initial Coin Offerings - Legal qualification and regulatory challenges", March 2018, <https://www.slideshare.net/fintechbelgium/fintech-belgium-meetup-on-icos-080318-laurent-godts>, 9p.
- LEE, S., "Bitcoin's Energy Consumption Can Power An Entire Country -- But EOS Is Trying To Fix That", April 2018, <https://www.forbes.com/sites/shermanlee/2018/04/19/bitcoins-energy-consumption-can-power-an-entire-country-but-eos-is-trying-to-fix-that/>.
- LEE, S., "Explaining Directed Acyclic Graph (DAG), The Real Blockchain 3.0", January 2018, <https://www.forbes.com/sites/shermanlee/2018/01/22/explaining-directed-acyclic-graph-dag-the-real-blockchain-3-0/#68781282180b>.
- LENG, S., "Beijing bans bitcoin, but when did it all go wrong for cryptocurrencies in China?", February 2018, <http://www.scmp.com/news/china/economy/article/2132119/beijing-bans-bitcoin-when-did-it-all-go-wrong-cryptocurrencies>.
- LERIDER, M., "Clarification on NEO, GAS and Consensus Nodes", August 2017, <https://medium.com/@MalcolmLerider/clarification-on-neo-gas-and-consensus-nodes-aa94d4f4b09>.

- LERIDER, M., "What is NEO Smart Economy?", August 2017, <https://medium.com/@MalcolmLerider/what-is-neo-smart-economy-381a4c6ee286>.
- LEVENSON, N., "NEO versus Ethereum: Why NEO might be 2018's strongest cryptocurrency", December 2017, <https://hackernoon.com/neo-versus-ethereum-why-neo-might-be-2018s-strongest-cryptocurrency-79956138bea3>.
- LEWIS, R., MCPARTLAND, J. and RANJAN, R., "Blockchain and financial market innovation", Economic Perspectives, Issue 7, 2017, Federal Reserve Bank of Chicago, 13p. (electronically available via <https://www.chicagofed.org/publications/economic-perspectives/2017/7>).
- LILIENTHAL, G. and AHMAD, N., "Bitcoin: is it really coinage?", 2018, Computer and Telecommunications Law Review, 24(3), 49-56.
- LUCKING, D., and O'HANLON, C., "Delaware Passes Law Permitting Companies to Use Blockchain Technology to Issue and Track Shares", 26 September 2017, <http://www.allenvery.com/publications/en-gb/Pages/Delaware-Passes-Law-Permitting-Companies-to-Use-Blockchain-Technology-to-Issue-and-Track-Shares.aspx>.
- MADEIRA, A., "How to make an anonymous ether transaction using WeiMixer", May 2018, <https://www.cryptocompare.com/coins/guides/how-to-make-an-anonymous-ether-transaction/>.
- MANDJEE, T., "Bitcoin, its Legal Classification and its Regulatory Framework", 15 J. Bus. & Sec. L. 157, 2016, <http://digitalcommons.law.msu.edu/jbsl>, 62p.
- MARSHALL, A., "P2P Cryptocurrency Exchanges, Explained", April 2017, <https://cointelegraph.com/explained/p2p-cryptocurrency-exchanges-explained>.
- MARTINDALE, J., "What is Litecoin? Here's everything you need to know", January 2018, <https://www.digitaltrends.com/computing/what-is-litecoin/>.
- MARTINET, S., "GDPR and Blockchain: Is the New EU Data Protection Regulation a Threat or an Incentive?", May 2018, <https://cointelegraph.com/news/gdpr-and-blockchain-is-the-new-eu-data-protection-regulation-a-threat-or-an-incentive>.
- MAXWELL, W., and SALMON, J., "A guide to blockchain and data protection", Hogan Lovells, September 2017, 22p. [https://www.hलगage.com/uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf?\\_sm\\_au=iVV6bs5Z45DMRVfr](https://www.hलगage.com/uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf?_sm_au=iVV6bs5Z45DMRVfr).
- MCGRATH GOODMAN, L., "The Face Behind Bitcoin", in Newsweek, 14 March 2014, <http://www.newsweek.com/2014/03/14/face-behind-bitcoin-247957.html>.
- MOSKOV, A., "Cryptocurrency Industry Spotlight: Who is NEO's Da Hongfei?", January 2018, <https://coincentral.com/cryptocurrency-industry-spotlight-neos-da-hongfei/>.
- NABILOU, H. and PRÜM, A., "Ignorance, debt and cryptocurrencies: the old and the new in the law and economics of concurrent currencies", May 2018, 40p. (electronically available via <https://ssrn.com/abstract=3121918>).
- NASEER, H., "NEO Launches Dev Competition with \$490,000 Prize Pool, Co-organized by Microsoft", November 2017, <https://cryptovest.com/news/neo-launches-dev-competition-with-490000-prize-pool-co-organized-by-microsoft/>.
- NEL, L., "Privacy Coins: Beginner's Guide to Anonymous Cryptocurrencies", April 2018, <https://blockonomi.com/privacy-cryptocurrency/>.

- NIAN, LAM PAK, "Bitcoin in Singapore: A Light-Touch Approach to Regulation", 11 April 2014, 72p. (electronically available via [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2427626](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2427626)).
- NJUI, J. P., "Amazon Partnership Speculation High For Ripple (XRP) As Markets Go Crazy", May 2018, <https://ethereumworldnews.com/amazon-partnership-speculation-high-for-ripple-xrp-as-markets-go-crazy/>.
- OECD, "Tax Challenges Arising from Digitalisation – Interim Report", 2018, 206, No. 501.
- Opinion of the ECB of 12 October 2016 on a proposal for a directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC, [https://www.ecb.europa.eu/ecb/legal/pdf/con\\_2016\\_49\\_with\\_technical\\_working\\_document\\_.pdf](https://www.ecb.europa.eu/ecb/legal/pdf/con_2016_49_with_technical_working_document_.pdf).
- ORCUTT, M., "No, Ripple Isn't the Next Bitcoin", January 2018, <https://www.technologyreview.com/s/609958/no-ripple-isnt-the-next-bitcoin/>.
- Ordonnance n° 2017-1674 du 8 de cembre 2017 relative a l'utilisation d'un dispositif d'enregistrement e lectronique partage pour la repre sentation et la transmission de titres financiers, JORF 9 december 2017, no 0287, text no 24, [www.legifrance.gouv.fr/eli/ordonnance/2017/12/8/2017-1674/jo/texte](http://www.legifrance.gouv.fr/eli/ordonnance/2017/12/8/2017-1674/jo/texte).
- Ozelli, S., "Malta Emerges as World's Cryptocurrency Hub Despite EU's TAX3 Investigation: Expert Take", June 2018, <https://cointelegraph.com/news/malta-emerges-as-world-s-cryptocurrency-hub-despite-eu-s-tax3-investigation-expert-take>.
- PAECH, P., "Securities, Intermediation and the Blockchain: An Inevitable Choice between Liquidity and Legal Certainty", LSE Law, Society and Economy Working Paper 20/2015, 26-28.
- PERPER, R., "China is moving to eliminate all cryptocurrency trading with a ban on foreign exchanges", February 2018, [https://www.businessinsider.nl/china-eliminates-all-cryptocurrency-trading-2018-2/?international=true&r=US&sm\\_au=iVV6bs5Z45DMRVfr](https://www.businessinsider.nl/china-eliminates-all-cryptocurrency-trading-2018-2/?international=true&r=US&sm_au=iVV6bs5Z45DMRVfr).
- PETERSON, B., "The founder of litecoin, a cryptocurrency that has gained 650% in 7 months, told us he's worried about all the scams in the nascent market", January 2018, <http://www.businessinsider.com/litecoin-founder-charlie-lee-on-bitcoin-and-the-cryptocurrency-bubble-2018-1?international=true&r=US&IR=T>.
- PLASSARAS, N.A., "Regulating Digital Currencies: Bringing Bitcoin Within the Reach of the IMF", Chicago Journal of International Law, 2013, 26p. (electronically available <http://ssrn.com:80/abstract=2248419>).
- POLLOCK, D., "G20 and Cryptocurrencies: Baby Steps Towards Regulatory Recommendations", March 2018, <https://cointelegraph.com/news/g20-and-cryptocurrencies-baby-steps-towards-regulatory-recommendations>.
- POPOV, S., "The Tangle", October 2017, [http://iotatoken.com/IOTA\\_Whitepaper.pdf](http://iotatoken.com/IOTA_Whitepaper.pdf).
- POSNAK, E. "On the Origin of Cardano", December 2017, <https://medium.com/on-the-origin-of-smart-contract-platforms/on-the-origin-of-cardano-a6ce4033985c>.
- Q. SHENTU, Q., and YU, J., "Research on Anonymization and De-anonymization in the Bitcoin System", October 2015, 14p. (electronically available via <https://arxiv.org/pdf/1510.07782.pdf>).

- Ramesh, A., “Features of various Blockchains: A Comparison”, February 2018, <https://www.xoken.org/blog/features-of-various-blockchains-a-comparison/>.
- Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community, *OJ L* 309, 25 November 2005, 9 (electronically available via: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005R1889&from=EN>).
- Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006, *OJ L* 141, 5 juni 2015, 1 (electronically available via <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015R0847>).
- RIZZO, P., “Ether, Litecoin and More: Overstock Now Accepts Cryptocurrencies as Payment”, August 2017, <https://www.coindesk.com/ether-litecoin-overstock-now-accepts-cryptocurrencies-payment/>.
- ROHR, J. and WRIGHT, A., “Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets”, October 2017, 115p. (electronically available via <https://ssrn.com/abstract=3048104>).
- ROSE O’LEARY, R., “Atomic Action: Will 2018 Be the Year of the Cross-Blockchain Swap?”, January 2018, <https://www.coindesk.com/atomic-action-will-2018-year-cross-blockchain-swap/>.
- ROSIC, A., “What is Ethereum Casper Protocol? Crash Course”, November 2017, <https://blockgeeks.com/guides/ethereum-casper/>.
- ROSIC, A., “What is Litecoin? A Basic Beginners Guide”, December 2017, <https://blockgeeks.com/guides/litecoin/>.
- ROYER, S., “Bitcoins in het Belgische strafrecht en strafprocesrecht”, *RW* 2016-17, No. 13, 483- 501.
- SAIDOV, U., “Cryptocurrencies: The Rise of Decentralized Money”, April 2018, <https://blogs.cfainstitute.org/investor/2018/04/03/cryptocurrencies-the-rise-of-decentralized-money/>.
- SAMEEH, T., “What If Ripple’s Transactions Can Be Fully Anonymous?”, May 2017, <http://www.livebitcoinnews.com/ripples-transactions-can-fully-anonymous/>.
- SERRES, T., “2017’s Ransomware Attacks: Could Blockchain Technology Have Prevented Them?”, May 2017, <https://medium.com/animal-media/2017s-ransomware-attacks-could-blockchain-technology-have-prevented-them-ed9ca6bf348b>.
- SETH, S., “Is Bitcoin Banned in China?”, February 2018, <https://www.investopedia.com/news/bitcoin-banned-china/>.
- SHAH, K, ‘Ethereum Supply Limit to 120 million – Prank or Reality?’, April 2018, <https://www.cryptoground.com/a/ethereum-supply-limit-to-120-million>.
- SHAWDAGOR, J., “Blockchain Against Tax Fraud As Tencent Partners Up With Shenzhen National Taxation Bureau”, May 2018, <https://bitrazzi.com/blockchain-against-tax-fraud-as-tencent-partners-up-with-shenzhen-national-taxation-bureau/>.
- SHOBHIT, S., “Public, Private, Permissioned Blockchains Compared”, April 2018, <https://www.investopedia.com/news/public-private-permissioned-blockchains-compared/>.

- SNYERS, A. and PAUWELS, K., "ICOs in Belgium: down the rabbit hole into legal no man's land? (Part 1)", ICCLR, 2018, to be published.
- SOETEMAN, K., "Werking dBft via Neo in kaart gebracht", February 2018, <https://www.computable.nl/artikel/achtergrond/technologie/6306817/5182002/werking-dbft-via-neo-in-kaart-gebracht.html>.
- SPAVEN, E., "Online payment network Ripple Labs receives \$3.5 Million in new funding", September 2014, <https://www.coindesk.com/online-payment-network-ripple-labs-receives-3-5m-new-funding/>.
- SUBERG, W., "Ban Complete: China Blocks Foreign Crypto Exchanges To Counter 'Financial Risks'", February 2018, <https://cointelegraph.com/news/ban-complete-china-blocks-foreign-crypto-exchanges-to-counter-financial-risks>.
- SUBERG, W., "NEO DevCon Sees Microsoft Judge Network's Potential Uses", November 2017, <https://cointelegraph.com/news/neo-devcon-sees-microsoft-judge-networks-potential-uses>.
- SUNDARARAJAN, S., "Chinese City to Use Blockchain In Fight Against Tax Evasion", May 2018, <https://www.coindesk.com/tencent-partners-with-city-authority-to-combat-tax-evasion-with-blockchain/>.
- TEAGUE, S., "G20 ministers wrestle with cryptocurrency oversight", 29 March 2018, [https://www.euromoney.com/article/b17jt5vnb3fn3m/g20-ministers-wrestle-with-cryptocurrency-oversight?utm\\_source=FX%20this%20week%20v2&utm\\_medium=email%20editorial&utm\\_content=Editorial&utm\\_campaign=636579242347129780&utm\\_term=G20%20ministers%20wrestle%20with%20cryptocurrency%20oversight](https://www.euromoney.com/article/b17jt5vnb3fn3m/g20-ministers-wrestle-with-cryptocurrency-oversight?utm_source=FX%20this%20week%20v2&utm_medium=email%20editorial&utm_content=Editorial&utm_campaign=636579242347129780&utm_term=G20%20ministers%20wrestle%20with%20cryptocurrency%20oversight).
- TENNANT, L., "Improving the Anonymity of the IOTA Cryptocurrency", October 2017, [https://assets.ctfassets.net/r1dr6vzfxhev/6StLLAy9b26eyUG8SGQqeu/e30c20f91e77e54d88b7644658912c7d/Improving\\_the\\_Anonymity\\_of\\_the\\_IOTA\\_Cryptocurrency.pdf](https://assets.ctfassets.net/r1dr6vzfxhev/6StLLAy9b26eyUG8SGQqeu/e30c20f91e77e54d88b7644658912c7d/Improving_the_Anonymity_of_the_IOTA_Cryptocurrency.pdf), 20p.
- TOWN, S., "Introduction to Stellar Lumens (XLM) – The Future of Banking", April 2018, <https://cryptoslate.com/stellar-lumens/>.
- TRAUTMAN, L.J., "Virtual currencies: Bitcoin & what now after Liberty Reserve, Silk Road, and Mt. Gox?", Richmond Journal of Law and Technology, Vol. 20, No. 4, 2014, 108p. (electronically available via [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2393537](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2393537)).
- TUWINER, J., "Introduction to NEO – An Open Network For Smart Economy", April 2018, <https://cryptoslate.com/introduction-to-neo-an-open-network-for-smart-economy/>.
- VALCKE, P., VANDEZANDE, N., and VAN DE VELDE, N., "The evolution of third party payment providers and cryptocurrencies under the EU's upcoming PSD2 and AMLD4", 2015, Swift Institute Working Paper No. 2015-001, 77p.
- VALENTE, P., "Bitcoin and Virtual Currencies Are Real: Are Regulators Still Virtual?", INTERTAX, Volume 46, Issue 6 & 7, 541-549.
- VAN DE LOOVERBOSCH, M., "Crypto-effecten: tussen droom en daad", TRV-RPS 2018, 193-207.
- VAN HUMBEECK, A., "The Blockchain-GDPR Paradox", November 2017, <https://medium.com/wearetheledger/the-blockchain-gdpr-paradox-fc51e663d047>.

- VAN WIRDUM, A., "Is Bitcoin Anonymous? A Complete Beginner's Guide", November 2015, <https://bitcoinmagazine.com/articles/is-bitcoin-anonymous-a-complete-beginner-s-guide-1447875283/>.
  - VANDEZANDE, N., *Virtual currencies: a legal framework*, Antwerp, Intersentia, 2018, 500p.
  - WITZIG, P., and SALOMON, V., "Cutting out the middleman: a case study of blockchain-induced reconfigurations in the Swiss Financial Services Industry", Working Paper 1, 2018/E, the Circulation of Wealth, Université de Neuchâtel, [http://www.unine.ch/files/live/sites/maps/files/shared/documents/wp/WP-1\\_2018\\_Witzig%20and%20Salomon.pdf](http://www.unine.ch/files/live/sites/maps/files/shared/documents/wp/WP-1_2018_Witzig%20and%20Salomon.pdf), 27p.
  - World Bank Group (H. NATARAJAN, S. KRAUSE and H. GRADSTEIN), "Distributed Ledger Technology (DLT) and blockchain", 2017, FinTech note, no. 1. Washington, D.C., <http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf>, 46p.
  - X, "A Definitive Guide To NEO (2nd Edition)", January 2018, <http://storeofvalueblog.com/posts/a-definitive-guide-to-neo/>.
  - X, "An introduction to IOTA", 2017, <https://iotasupport.com/whatisiota.shtml>.
  - X, "Blockchain en GDPR: een moeilijk huwelijk", May 2018, <https://www.techzine.nl/blogs/404986/blockchain-en-gdpr-een-moeilijk-huwelijk.html?redirect=1>.
  - X, "IOTA Coin Review", January 2018, <https://hackernoon.com/iota-coin-review-6a1c73c5cfa3>.
  - X, "True scale of Bitcoin ransomware extortion revealed", MIT Technology Review, April 2018, <https://www.technologyreview.com/s/610803/true-scale-of-bitcoin-ransomware-extortion-revealed/>.
  - X, "What is NEO, and what is GAS?", September 2017, <https://hackernoon.com/what-is-neo-and-what-is-gas-5b9828a1aa65>.
  - ZAINUDDIN, A., "Coins, Tokens & Altcoins: What's the Difference?", 2017, <https://masterthecrypto.com/differences-between-cryptocurrency-coins-and-tokens/>.
  - ZAINUDDIN, A., "Guide on Privacy Coins: Comparison of Anonymous Cryptocurrencies", 2017, <https://masterthecrypto.com/privacy-coins-anonymous-cryptocurrencies/>.
  - ZETZSCHE, D., BUCKLEY, R.P., ARNER, D.W., and FÖHR, L., "The ICO Gold Rush: It's a scam, it's a bubble, it's a super challenge for regulators", November 2017 (electronically available via <https://ssrn.com/abstract=3072298>), 47p.
- 
- <http://data.consilium.europa.eu/doc/document/ST-15849-2017-INIT/en/pdf>.
  - <http://docs.neo.org/en-us/index.html>.
  - <http://drapis.com>.
  - <http://ethdocs.org/en/latest/introduction/history-of-ethereum.html>.
  - <http://fortune.com/2018/03/14/playboy-cryptocurrency-vice-vit-crypto/>.



- <http://www.consilium.europa.eu/en/press/press-releases/2018/04/16/malicious-cyber-activities-council-adopts-conclusions/>.
- [http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-revision-of-the-anti-money-laundering-directive-\(aml\)](http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-revision-of-the-anti-money-laundering-directive-(aml)).
- [http://www.fsma.be/nl-in-the-picture/Article/press/div/2014/2014-01-14\\_virtueel.aspx](http://www.fsma.be/nl-in-the-picture/Article/press/div/2014/2014-01-14_virtueel.aspx).
- <http://www.monero.cc>.
- <http://www.weidai.com/bmoney.txt>.
- <https://99bitcoins.com/who-accepts-bitcoins-payment-companies-stores-take-bitcoins/>.
- <https://acceptbitcoin.cash/>.
- <https://anycoindirect.eu/>.
- <https://bitcoin.org>.
- <https://bitcoin.org/bitcoin.pdf>.
- <https://bitcoin.org/en/faq#who-created-bitcoin>.
- <https://bitsane.com/exchange/xrp-eur>.
- <https://bittrex.com/home/markets>.
- <https://btcdirect.eu/>.
- <https://cardanodocs.com/cardano/monetary-policy/>.
- <https://cardanodocs.com/introduction/#cryptocurrency-basics>.
- <https://coinfalcon.com>.
- <https://coinmarketcap.com/charts/>.
- <https://coinmarketcap.com/coins/views/all/>.
- <https://cryptocoincharts.info/markets/info>.
- <https://cryptocurrencyfacts.com/asic-mining-basics/>.
- <https://cryptonote.org/whitepaper.pdf>.
- <https://digiconomist.net/bitcoin-energy-consumption>.
- <https://docs.dash.org/en/latest/introduction/features.html>.
- <https://docs.dash.org/en/latest/introduction/features.html#privatesend>.
- <https://docs.dash.org/en/latest/masternodes/understanding.html>.
- [https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/money-laundering\\_en](https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/money-laundering_en).
- [https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/criminal-justice/financial-crime\\_en](https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/criminal-justice/financial-crime_en).
- [https://ec.europa.eu/taxation\\_customs/sites/taxation/files/com\\_2016\\_825\\_en.pdf](https://ec.europa.eu/taxation_customs/sites/taxation/files/com_2016_825_en.pdf).
- <https://ethereumprice.org/what-is-ethereum/>.

- [https://eur-lex.europa.eu/procedure/EN/2016\\_208](https://eur-lex.europa.eu/procedure/EN/2016_208).
- [https://exmo.com/en/news\\_view?id=1912](https://exmo.com/en/news_view?id=1912).
- <https://geti2p.net/en/>.
- <https://getmonero.org/community/merchants/>.
- <https://getmonero.org/get-started/what-is-monero/>.
- <https://getmonero.org/resources/about/>.
- <https://getmonero.org/resources/moneropedia/cryptocurrency.html>.
- <https://getmonero.org/resources/moneropedia/fungibility.html>.
- <https://github.com/dashpay/dash/wiki/Whitepaper>.
- <https://hitbtc.com>.
- <https://jaxx.io>.
- <https://litecoin.com>.
- <https://litecoin.com/services#merchants>.
- <https://localbitcoins.com>.
- <https://neo.org>.
- <https://people.csail.mit.edu/rivest/pubs/RST01.pdf>.
- [https://people.xiph.org/~greg/confidential\\_values.txt](https://people.xiph.org/~greg/confidential_values.txt).
- <https://ripple.com>.
- <https://ripple.com/build/xrp-ledger-consensus-process/>.
- <https://ripple.com/insights/ripple-escrows-55-billion-xrp-for-supply-predictability/>.
- <https://ripple.com/insights/ripple-receives-new-yorks-first-bitlicense-institutional-use-case-digital-assets/>.
- <https://ripple.com/use-cases/banks/>.
- <https://ripple.com/xrp/>.
- <https://ripple.com/xrp/market-performance/>.
- <https://stellar.shop/products>.
- <https://support.coinbase.com/customer/en/portal/topics/601112-wallet-services/articles>.
- <https://support.coinbase.com/customer/portal/articles/2911542>.
- <https://support.microsoft.com/nl-be/help/13942/microsoft-account-add-money-with-bitcoin>.
- <https://vapourdepot.com/>.
- <https://whycardano.com>.
- <https://www.binance.com>.
- <https://www.bitcoincash.org>.

- 
- <https://www.bitcoincash.org/en/>.
  - <https://www.bitfinex.com>.
  - <https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=235707311>.
  - <https://www.cardano.org>.
  - <https://www.cardano.org/en/ada-distribution-audit/>.
  - <https://www.cardano.org/en/philosophy/>.
  - <https://www.cardano.org/en/the-daedalus-wallet/>.
  - <https://www.cardano.org/en/what-is-cardano/>.
  - <https://www.coinbase.com>.
  - <https://www.coindesk.com/lot-polish-airlines-accept-bitcoin/>.
  - <https://www.coinwarz.com/cryptocurrency>.
  - <https://www.cryptomercado.com>.
  - <https://www.dash.org>.
  - <https://www.dash.org/merchants/>.
  - <https://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf>.
  - <https://www.ethereum.org>.
  - <https://www.ethereum.org/ether>.
  - <https://www.ethereum.org/foundation>.
  - <https://www.expedia.com/Checkout/BitcoinTermsAndConditions>.
  - <https://www.hotelginebra.com.es/welcome/ada/>.
  - <https://www.investopedia.com/terms/m/mediumofexchange.asp>.
  - <https://www.investopedia.com/terms/p/premining.asp>.
  - <https://www.iota.org>.
  - <https://www.iota.org/get-started/faqs>.
  - <https://www.kraken.com>.
  - <https://www.ledgerwallet.com/products>.
  - <https://www.litebit.eu/>.
  - <https://www.luno.com>.
  - <https://www.openbazaar.org>.
  - <https://www.preludebreakfast.com>.
  - [https://www.reddit.com/r/NEO/comments/6su31n/here\\_are\\_some\\_things\\_you\\_should\\_know\\_if\\_you\\_are/](https://www.reddit.com/r/NEO/comments/6su31n/here_are_some_things_you_should_know_if_you_are/).
  - <https://www.sproutgrowers.world/product/sprout-grower/>.

- <https://www.stellar.org>.
- <https://www.stellar.org/about/>.
- <https://www.stellar.org/about/mandate/>.
- <https://www.stellar.org/developers/guides/walkthroughs/stellar-smart-contracts.html>.
- <https://www.stellar.org/how-it-works/stellar-basics/>.
- <https://www.stellar.org/lumens/>.
- <https://www.tapjets.com>.
- <https://www.virgin.com/richard-branson/bitcoins-space>.
- <https://www.xrpchat.com/topic/5679-ripple-xrp-merchants-directory/>.

---

More and more regulators are worrying about criminals who are increasingly using cryptocurrencies for illegitimate activities like money laundering, terrorist financing and tax evasion. The problem is significant: even though the full scale of misuse of virtual currencies is unknown, its market value has been reported to exceed EUR 7 billion worldwide. This paper prepared by Policy Department A elaborates on this phenomenon from a legal perspective, focusing on the use of cryptocurrencies for financial crime, money laundering and tax evasion. It contains policy recommendations for future EU standards.

---

---

PE 619.024  
IP/A/TAX3/2018-03

Print ISBN 978-92-846-3199-5 | doi:10.2861/280969 | QA-03-18-060-EN-C  
PDF ISBN 978-92-846-3200-8 | doi:10.2861/263175 | QA-03-18-060-EN-N

EDITORS' PICK | Jul 13, 2021, 07:27am EDT | 7292 views

# British Police Seize \$250 Million Of Cryptocurrency In International Money Laundering Crackdown



**Robert Hart** Forbes Staff

Business

*I cover breaking news.*

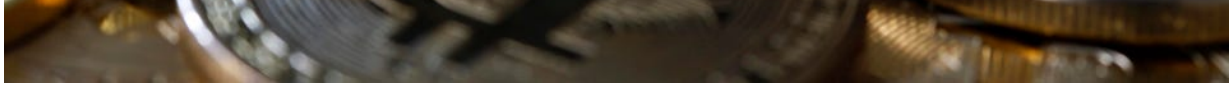
Follow

Listen to this article now -02:21

Powered by [Trinity Audio](#)

**TOPLINE** British police have confiscated around \$250 million worth of cryptocurrency as part of an ongoing money laundering investigation, London’s Metropolitan Police **announced** Tuesday, marking one of the largest crypto seizures in the world and **breaking** a record the force set last month.





London police seized millions in cryptocurrency, though it is unclear which tokens were taken.

GETTY IMAGES

### KEY FACTS

- The seizure, which follows a \$160 million crypto haul the force made three weeks ago, is part of an ongoing investigation into international money laundering by the force's Economic Crime Command.
- It comes after a 39-year-old woman was arrested on “suspicion of money laundering offenses” on June 24 after the first cache was confiscated and the woman was subsequently released on bail, the force said.
- The woman was interviewed again last weekend—this time under caution—after the latest discovery was made and has been bailed until late July.
- Detective Constable Joe Ryan said the “seizure is another significant landmark in this investigation which will continue for months to come as we hone in on those at the centre of this suspected money laundering operation.”
- The force did not disclose what cryptocurrencies had been confiscated.

### KEY BACKGROUND

Cryptocurrencies are traded digitally, relatively anonymous, have low barriers to entry, can be convenient to use and are international by nature, making them an attractive prospect to some criminals. While most crypto transactions are legitimate, the specter of financial crime has become a strong **motivator** for **regulators** around the world to

**bolster** scrutiny of digital assets. With growing demand for cryptocurrency services, in part spurred on by a growth in value for many major assets and meme tokens during parts of the Covid-19 pandemic, many major financial **institutions** have **moved into crypto**

1 of 4 free articles



**Introducing the Forbes.com subscription.** Unlimited content.  
Improved ad experience.

**Learn  
more**

**ransomware, terrorism, and drug trafficking.** The digital assets are also the payment method of **choice** for ransomware hackers, which adds to calls for enhanced regulatory scrutiny.

#### **CRUCIAL QUOTE**

While the “proceeds of crime are laundered in many different ways,” Deputy Assistant Commissioner Graham McNulty said, organized criminals are increasingly “using cryptocurrency to launder their dirty money.” However, McNulty added: “Cash still remains king in the criminal world.”

#### **FURTHER READING**

[U.K. Police Seize \\$160 Million In Cryptocurrency In Money Laundering Investigation \(Forbes\)](#)

[Met police seize nearly £180m of bitcoin in money laundering investigation \(Guardian\)](#)

[Ransomware Hackers Demand \\$70 Million In Bitcoin, Claim Massive U.S. Attack As Biden Investigates Possible Russian Involvement \(Forbes\)](#)



**Forbes** | Topline

## Be the first to get expert analysis as breaking news happens.

Sign up for Topline email alerts for breaking news of the day.

**Submit**

You may opt out any time. By signing up for this newsletter, you agree to the [Terms and Conditions](#) and [Privacy Policy](#)

*Follow me on [Twitter](#). Send me a secure [tip](#).*



**Robert Hart**

Follow

I am a London-based reporter for Forbes covering breaking news. Previously, I have worked as a reporter for a specialist legal publication covering big data and as a... **Read More**

Print

Reprints & Permissions

ADVERTISEMENT

**Cyber Security**

## The rise of crypto laundries: how criminals cash out of bitcoin

Criminals are locked in battle with Forensics firms tracking how Treasure Men, privacy wallets and gift cards are used to turn virtual hauls into hard cash



Hannah Murphy in San Francisco MAY 28 2021

### Cyber Security updates

Sign up to myFT Daily Digest to be the first to know about Cyber Security news.

**Sign up**

In the world of online crime, anonymous cryptocurrencies are the payment method of choice. But at some point, virtual hauls need to be turned into hard cash. Enter the “Treasure Men”.

Finding a Treasure Man is easy if you know where to look. They are listed for hire on Hydra, the largest marketplace on the dark web by revenues, a part of the internet that is not visible to search engines and requires specific software to access.

“They will literally leave bundles of cash somewhere for you to pick up,” said Dr Tom Robinson, chief scientist and co-founder of Elliptic, a group that tracks and analyses crypto transactions. “They bury it underground or hide it behind a bush, and they’ll tell you the coordinates. There’s a whole profession.”

The Russian-language Hydra offers plenty of other ways for criminals to cash out of cryptocurrencies, including exchanging bitcoin for gift vouchers, prepaid debit cards or iTunes vouchers, for example.

The ability to hold cryptocurrencies without divulging your identity has made them increasingly attractive to criminals, and particularly to hackers who demand ransoms after breaking into companies.

In 2020, at least \$350m in crypto ransoms was paid out to hacker gangs, such as DarkSide, the group that shut down the Colonial Pipeline earlier this month, according to Chainalysis, a research group.

But at the same time, every transaction in a cryptocurrency is recorded on an immutable blockchain, leaving a visible trail for anyone with the technical knowhow.

Several crypto forensics companies have sprung up to help law enforcement track criminal groups by analysing where the currencies flow to.

These include New York’s Chainalysis, which raised \$100m at more than a \$2bn valuation earlier this year, London-based Elliptic, which boasts Wells Fargo among its investors, and US government-backed CipherTrace.

## Dark exchanges

In total, in 2020 some \$5bn in funds were received by illicit entities, and those illicit entities sent \$5bn on to other entities, representing less than 1 per cent of the overall cryptocurrency flows, according to Chainalysis.

In the early days of cryptocurrencies, criminals would simply cash out using the major cryptocurrency exchanges. Elliptic estimates that between 2011 and 2019, major exchanges helped cash out between 60 per cent to 80 per cent of bitcoin transactions from known bad actors.

By last year, as exchanges began to worry more about regulation, many of them bolstered their anti-money laundering (AML) and know-your-customer (KYC) processes and the share shrank to 45 per cent.

Stricter rules have pushed some criminals towards unlicensed exchanges, which typically require no KYC information. Many operate out of jurisdictions with less stringent regulatory requirements or lie outside of extradition treaties.

But Michael Phillips, chief claims officer at cyber insurance group Resilience, said such exchanges tend to have lower liquidity, making it harder for criminals to transfer crypto into fiat currencies. “The aim is to impose further costs on the business model,” he said.

There are an array of other niche off ramps into fiat currency. Analysis by Chainalysis suggests that over-the-counter brokers in particular help facilitate some of the largest illicit transactions — with some operations clearly set up for that purpose alone.

Meanwhile smaller transactions flow through the more than 11,600 crypto ATMs that have sprung up globally with little to no regulation, or through online gambling sites that accept crypto.

## Forensics firms

Against this backdrop, the crypto forensics firms use technology that analyses blockchain transactions, together with human intelligence, to work out which crypto wallets belong to which criminal groups, and map out a picture of the wider, interlocking crypto criminal ecosystem.

With an overview of how criminals move their money, their research has shone a light in particular on how hackers are renting out their ransomware software to networks of affiliates, while taking a cut of any proceeds.

Kimberly Grauer, head of research at Chainalysis, added that hackers are increasingly paying for support services from other criminals, such as cloud hosting or paying for the login credentials of their victims, with crypto, giving investigators a more complete picture of the ecosystem.

“There’s actually fewer needs to cash out in order to sustain your business models,” said Grauer. This means “we can see the ransom paid, and we can see the splitting and going to all the different players in the system”.

## Losing the trail

But cyber criminals are increasingly wielding their own high-tech tools and techniques in a bid to muddy the crypto trail that they leave behind them.

Some criminals undertake what is known as “chain-hopping” — jumping between different cryptocurrencies, often in rapid succession — to lose trackers, or use particular “privacy coin” cryptocurrencies that have extra anonymity built into them, such as Monero.

Among the most common tools for throwing investigators off the scent are tumblers or mixers — third-party services that mix up illicit funds with clean crypto before redistributing them. In April, the Department of Justice [arrested and charged](#) a dual Russian-Swedish national who operated a prolific mixing service called Bitcoin Fog, moving some \$335m in bitcoin over the past decade.

“It is possible to untumble coins,” said Katherine Kirkpatrick, a partner at law firm King & Spalding with expertise in anti-money laundering. “But it’s highly technical and takes a lot of processing power and data.”

The “preferred obfuscation tool” in 2020 — which helped facilitate 12 per cent of all bitcoin laundering that year — were highly sophisticated “privacy wallets” that have anonymisation techniques including mixing capabilities built into them, according to Elliptic.

“They’re basically a trustless version of a mixer and it’s all done within software,” said Robinson, noting that an open-source project called Wasabi Wallet was the dominant player in the space.

## What comes next?

Authorities “need to modernise forfeiture and asset freezes” so that it is easier for law enforcement to seize crypto from exchanges, said Tom Kellermann, head of cyber security strategy for VMware and cyber investigations advisory board member for the US Secret Service.

Individual exchanges can today sign up to services from the forensics firms that will notify them of suspicious activity based on their intelligence.

But experts have in the past touted the idea of having shared blacklists of wallets known to be used by bad actors — a kind of Interpol alert, with exchanges, analytics groups and the government openly sharing information on their investigations in order to make this possible.

“Perhaps now is a better time to reconsider some of those policy initiatives,” said Kemba Walden, assistant general counsel at Microsoft’s Digital Crimes Unit.

---

[Copyright](#) The Financial Times Limited 2021. All rights reserved.



# The Daily Swig

Cybersecurity news and views

Data Breaches

Cyber-attacks

Vulnerabilities

Bug Bounties

Infosec Research

Deep Dives

## Binance reveals how data analytics led to ransomware-linked money laundering bust

John Leyden



*Crypto-exchange exploits OpSec mistakes to bust crooks*



The Binance cryptocurrency exchange has explained how advances in data analytics helped it track down a group of money launderers involved with various cybercrimes, including the notorious Clop [ransomware](#) scam.

Ukrainian police [announced](#) the arrest of individuals and the takedown of infrastructure related to the ‘Clop’ ransomware operation earlier this month.

Binance’s statement confirms that those arrested were cashing out and laundering funds, rather than being behind the creation of the ransomware.

The group – also known as FANCYCAT – had their fingers in numerous [criminal](#) scams including laundering money for dark web operators as well as ransomware peddlers.

### Follow the (digital) money

Analogous with drug dealers, the funds extracted from victims through criminal activity such as ransomware need to be disguised before they can be safely spent in the real world to buy goods. That’s because any funds tied back to criminal activity can become the target of forfeiture orders.

Even if money is already in digital form there is a need to launder it, with abusing exchanges being one of the main techniques in play.

“Blockchain analysis shows a network of money launderers living inside macro exchanges which deposit and withdraw to each other to wash the money,” according to Binance, the Cayman Islands-domiciled crypto

#### Latest Posts

##### Bug Bounty Radar

The latest bug bounty programs for September 2021

31 August 2021

##### Exchange Server

Microsoft patches ‘ProxyToken’ flaw that leaked incoming emails

31 August 2021

##### ML security

Deserialization bug in TensorFlow allowed arbitrary code execution

31 August 2021

exchange.

Based on this insight, Binance was able to apply detection mechanisms to identify and interdict suspect accounts before working with law enforcement to build cases and take down criminal groups, as it explained in a [blog post](#) about the investigation.

We applied the two-pronged approach to the FANCYCAT investigation: our AML detection and analytics program detected suspicious activity on Binance.com and expanded the suspect cluster. Once we mapped out the complete suspect network, we worked with private sector chain analytics companies TRM Labs and Crystal (BitFury) to analyze on-chain activity and gain a better understanding of this group and its attribution.

Based on our analysis we found that this specific group was not only associated with laundering Clop attack funds, but also with Petya and other illegally-sourced funds. This led to the identification and eventual arrest of FANCYCAT.

We are continuing to investigate the FANCYCAT criminal syndicate across multiple jurisdictions and the connections associated with other cyber-attacks.

Earlier this year, Binance released a [case study](#) explaining how it worked with the Ukrainian Cyber Police to arrest a major cybercriminal group laundering over \$42 million of illicit funds in a separate investigation.

All this work against money laundering has not gone far enough for some regulators, who are also concerned about the role of cryptocurrency exchanges in tax evasion.

Binance was ordered by the UK's Financial Conduct Authority to stop all regulated activity in the United Kingdom, Reuters [reports](#). Buying and selling cryptocurrencies is not regulated in the UK but trading in derivatives is regulated and it seems to be the activities of Binance Markets in this area that has brought the whole company an unwelcome sanction.

**BACKGROUND** [Cybercrooks steal \\$40m in Bitcoin from crypto-exchange Binance](#)



**John Leyden**  
[@jleyden](#)

- Twitter
- WhatsApp
- Facebook
- Reddit
- LinkedIn
- Email

## Related stories

### Bug Bounty Radar

The latest bug bounty programs for September 2021  
31 August 2021

### Exchange Server

Microsoft patches 'ProxyToken' flaw that leaked incoming emails  
31 August 2021

### ML security

Deserialization bug in TensorFlow allowed arbitrary code execution  
31 August 2021

### Remote takeover

Microsoft warns of critical Azure Cloud vulnerability impacting Cosmos DB accounts  
27 August 2021

---

**Burp Suite**

[Web vulnerability scanner](#)  
[Burp Suite Editions](#)  
[Release Notes](#)

**Vulnerabilities**

[Cross-site scripting \(XSS\)](#)  
[SQL injection](#)  
[Cross-site request forgery](#)  
[XML external entity injection](#)  
[Directory traversal](#)  
[Server-side request forgery](#)

**Customers**

[Organizations](#)  
[Testers](#)  
[Developers](#)

**Company**

[About](#)  
[PortSwigger News](#)  
[Careers](#)  
[Contact](#)  
[Legal](#)  
[Privacy Notice](#)

**Insights**

[Web Security Academy](#)  
[Blog](#)  
[Research](#)  
[The Daily Swig](#)



© 2021 PortSwigger Ltd.



## *Pipeline Investigation Upends Idea That Bitcoin Is Untraceable*

The F.B.I.'s recovery of Bitcoins paid in the Colonial Pipeline ransomware attack showed cryptocurrencies are not as hard to track as it might seem.



By Nicole Perlroth, Erin Griffith and Katie Benner

June 9, 2021

When Bitcoin burst onto the scene in 2009, fans heralded the cryptocurrency as a secure, decentralized and anonymous way to conduct transactions outside the traditional financial system.

Criminals, often operating in hidden reaches of the internet, flocked to Bitcoin to do illicit business without revealing their names or locations. The digital currency quickly became as popular with drug dealers and tax evaders as it was with contrarian libertarians.

But this week's revelation that federal officials had recovered most of the Bitcoin ransom paid in the recent Colonial Pipeline ransomware attack exposed a fundamental misconception about cryptocurrencies: They are not as hard to track as cybercriminals think.

On Monday, the Justice Department announced it had traced 63.7 of the 75 Bitcoins — some \$2.3 million of the \$4.3 million — that Colonial Pipeline had paid to the hackers as the ransomware attack shut down the company's computer systems, prompting fuel shortages and a spike in gasoline prices. Officials have since declined to provide more details about how exactly they recouped the Bitcoin, which has fluctuated in value.

Yet for the growing community of cryptocurrency enthusiasts and investors, the fact that federal investigators had tracked the ransom as it moved through at least 23 different electronic accounts belonging to DarkSide, the hacking collective, before accessing one account showed that law enforcement was growing along with the industry.

That's because the same properties that make cryptocurrencies attractive to cybercriminals — the ability to transfer money instantaneously without a bank's permission — can be leveraged by law enforcement to track and seize criminals' funds at the speed of the internet.

Bitcoin is also traceable. While the digital currency can be created, moved and stored outside the purview of any government or financial institution, each payment is recorded in a permanent fixed ledger, called the blockchain.

That means all Bitcoin transactions are out in the open. The Bitcoin ledger can be viewed by anyone who is plugged into the blockchain.

"It is digital bread crumbs," said Kathryn Haun, a former federal prosecutor and investor at venture-capital firm Andreessen Horowitz. "There's a trail law enforcement can follow rather nicely."

Ms. Haun added that the speed with which the Justice Department seized most of the ransom was "groundbreaking" precisely because of the hackers' use of cryptocurrency. In contrast, she said, getting records from banks often requires months or years of navigating paperwork and bureaucracy, especially when those banks are overseas.

Deputy U.S. Attorney General Lisa Monaco, center, announcing the recovery of part of the Colonial Pipeline ransom on Monday. Pool photo by Jonathan Ernst

Given the public nature of the ledger, cryptocurrency experts said, all law enforcement needed to do was figure out how to connect the criminals to a digital wallet, which stores the Bitcoin. To do so, authorities likely focused on what is known as a “public key” and a “private key.”

A public key is the string of numbers and letters that Bitcoin holders have for transacting with others, while a “private key” is used to keep a wallet secure. Tracking down a user’s transaction history was a matter of figuring out which public key they controlled, authorities said.

Seizing the assets then required obtaining the private key, which is more difficult. It’s unclear how federal agents were able to get DarkSide’s private key.

Justice Department spokesman Marc Raimondi declined to say more about how the F.B.I. seized DarkSide’s private key. According to court documents, investigators accessed the password for one of the hackers’ Bitcoin wallets, though they did not detail how.

The F.B.I. did not appear to rely on any underlying vulnerability in blockchain technology, cryptocurrency experts said. The likelier culprit was good old-fashioned police work.

Federal agents could have seized DarkSide’s private keys by planting a human spy inside DarkSide’s network, hacking the computers where their private keys and passwords were stored, or compelling the service that holds their private wallet to turn them over via search warrant or other means.

“If they can get their hands on the keys, it’s seizable,” said Jesse Proudman, founder of Makara, a cryptocurrency investment site. “Just putting it on a blockchain doesn’t absolve that fact.”

The F.B.I. has partnered with several companies that specialize in tracking cryptocurrencies across digital accounts, according to officials, court documents and the companies. Start-ups with names like TRM Labs, Elliptic and Chainalysis that trace cryptocurrency payments and flag possible criminal activity have blossomed as law enforcement agencies and banks try to get ahead of financial crime.

Their technology traces blockchains looking for patterns that suggest illegal activity. It’s akin to how Google and Microsoft tamed email spam by identifying and then blocking accounts that spray email links across hundreds of accounts.

“Cryptocurrency allows us to use these tools to trace funds and financial flows along the blockchain in ways that we could never do with cash,” said Ari Redbord, the head of legal affairs at TRM Labs, a blockchain intelligence company that sells its analytic software to law enforcement and banks. He was previously a senior adviser on financial intelligence and terrorism

at the Treasury Department.

Several longtime cryptocurrency enthusiasts said the recovery of much of the Bitcoin ransom was a win for the legitimacy of digital currencies. That would help shift the image of Bitcoin as the playground of criminals, they said.

“The public is slowly being shown, in case after case, that Bitcoin is good for law enforcement and bad for crime — the opposite of what many historically believed,” said Hunter Horsley, chief executive of Bitwise Asset Management, a cryptocurrency investment company.

In recent months, cryptocurrencies have become increasingly mainstream. Companies such as PayPal and Square have expanded their cryptocurrency services. Coinbase, a start-up that allows people to buy and sell cryptocurrencies, went public in April and is now valued at \$47 billion. Over the weekend, a Bitcoin conference in Miami attracted more than 12,000 attendees, including Twitter’s chief executive, Jack Dorsey, and the former boxer Floyd Mayweather Jr.

As more people use Bitcoin, most are accessing the digital currency in a way that mirrors a traditional bank, through a central intermediary like a crypto exchange. In the United States, anti-money laundering and identity verification laws require such services to know who their customers are, creating a link between identity and account. Customers must upload government identification when they sign up.

Ransomware attacks have put unregulated crypto exchanges under the microscope. Cybercriminals have flocked to thousands of high-risk ones in Eastern Europe that do not abide by these laws.

More than 12,000 people attended Bitcoin 2021 in Miami last week. Alfonso Duran for  
The New York Times

After the Colonial Pipeline attack, several financial leaders proposed a ban on cryptocurrency.

“We can live in a world with cryptocurrency or a world without ransomware, but we can’t have both,” Lee Reiners, the executive director of the Global Financial Markets Center at Duke Law School, wrote in The Wall Street Journal.

Cryptocurrency experts said the hackers could have tried to make their Bitcoin accounts even more secure. Some cryptocurrency holders go to great lengths to store their private keys away from anything connected to the internet, in what is called a “cold wallet.” Some memorize the string of numbers and letters. Others write them down on paper, though those can be obtained by search warrants or police work.

“The only way to obtain the truly unseizable characteristic of the asset class is to memorize the keys and not have them written down anywhere,” Mr. Proudman said.

Mr. Raimondi of the Justice Department said the Colonial Pipeline ransom seizure was the latest sting operation by federal prosecutors to recoup illicitly gained cryptocurrency. He said the department has made “many seizures, in the hundreds of millions of dollars, from unhosted cryptocurrency wallets” used for criminal activity.

In January, the Justice Department disrupted another ransomware group, NetWalker, which used ransomware to extort money from municipalities, hospitals, law enforcement agencies and schools.

As part of that sting, the department obtained about \$500,000 of NetWalker’s cryptocurrency that had been collected from victims of their ransomware.

“While these individuals believe they operate anonymously in the digital space, we have the skill and tenacity to identify and prosecute these actors to the full extent of the law and seize their criminal proceeds,” Maria Chapa Lopez, then the U.S. attorney for the Middle District of Florida, said when the case was announced.

In February, the Justice Department said it had warrants to seize nearly \$2 million in cryptocurrencies that North Korean hackers had stolen and put into accounts at two different cryptocurrency exchanges.

Last August, the department also unsealed a complaint outing North Korean hackers who stole \$28.7 million of cryptocurrency from a cryptocurrency exchange, and then laundered the proceeds through Chinese cryptocurrency laundering services. The F.B.I. traced the funds to 280 cryptocurrency wallets and their owners.

In the end, “cryptocurrencies are actually more transparent than most other forms of value transfer,” said Madeleine Kennedy, a spokeswoman for Chainalysis, the start-up that traces cryptocurrency payments. “Certainly more transparent than cash.”



MILLIONEN VON MITARBEITERN ARBEITEN VON ZUHAUSE AUS. ZEIT, DASS IHRE IT-SICHERHEIT DAS AUCH TUT!

**TRENDING** Alder Lake Windows 11 ISO Ryzen 5 5600G Intel Process Roadmap 2025

Tom's Hardware is supported by its audience. When you purchase through links on our site, we may earn an affiliate commission. [Learn more](#)

[Home](#) > [News](#)

# Bitcoin Mixing CEO Pleads Guilty to Money Laundering Charges

By [Nathaniel Mott](#) 13 days ago

Company's services were advertised to criminals.

      [Comments \(5\)](#)



(Image credit: Shutterstock)

Helix CEO Larry Dean Harmon pleaded guilty to one count of conspiracy to launder monetary instruments today, CoinDesk [reported](#), after the U.S. Department of the Treasury Financial Crimes Enforcement Network (FinCEN) accused him of helping criminals launder hundreds of millions of dollars via a process called Bitcoin mixing.

FinCEN [said](#) in October 2020 that Harmon "conducted over 1,225,000 transactions for customers and is associated with virtual currency wallet addresses that have sent or received over \$311 million" via Helix between 2014 and 2017. But he never registered Helix or his other company, Coin Ninja, as money services businesses.

Helix also "advertised its services in the darkest spaces of the internet as a way

for customers to anonymously pay for things like drugs, guns, and child pornography," [according](#) to FinCEN, which also said that Harmon "engaged in transactions with narcotics traffickers, counterfeiters and fraudsters, as well as other criminals."

All of those factors led to Harmon being the first person charged in the U.S. for offering a Bitcoin mixing service. But what exactly is Bitcoin mixing? It's essentially a cooperative effort to make Bitcoin more private by combining a bunch of people's funds into one transaction that is later split evenly among all the participants.

---

RECOMMENDED VIDEOS FOR YOU...

tom's **HARDWARE**

---

"Basically, if a hundred users all send exactly 0.1 BTC to a new address they control, and then merge these 100 transactions into one big transaction, everyone gets 0.1 bitcoin back, but no one can see where they got it from," Bitcoin Magazine [explained](#), adding that these mixers "can be designed in such a way that not even the entity that 'merges' the transaction can figure out which coins went where."

Not everyone — and perhaps not even the majority — of Bitcoin owners who use mixers are looking to launder money. Some might simply be looking to increase the privacy of their transactions based on their principles rather than the practical desire to evade law enforcement agencies, financial regulators, and others.

But there's no denying that Bitcoin mixers, much like the dark web Antinanalysis blockchain analysis service, do [appeal to cybercriminals](#). The question now is if FinCEN and other financial regulators will target more Bitcoin mixing service providers now that the case against Harmon has set a precedent.

As for Harmon: FinCEN issued him a \$60 million penalty in October 2020. The charge to which he pleaded guilty carries a maximum sentence of 20 years in a federal prison, and according to CoinDesk, his lawyer said that he will also be subject to "a large and lengthy forfeiture agreement."

MORE ABOUT...

LATEST

**Malware Attacks From Fake PC Games Numbered Over 5.8 Million in Past Year** ▶

**Cyberhack Hides Malicious Code in Your Graphics Ca**

SEE MORE LATEST ▶

TOPICS

---

CRYPTOCURRENCY

[SEE ALL COMMENTS \(5\)](#)

---

**5 COMMENTS****COMMENT FROM THE FORUMS** ▶**InvalidError**

One more domino falls and I bet there will be many more in the governments and law enforcement's quest to stop crypto-based tax evasion and money laundering.

**REPLY** ▶**freedomfries**

Meanwhile multinational banks have been busted laundering literally 100 billion dollars of drug cartel money, and just pay a fine (cost of business), and no one ever goes to jail. Well done FinCEN! You guys are true heroes.

**REPLY** ▶**USAFRet**

As a shocked face, my avatar is appropriate.

**REPLY** ▶**Jim90**

Methinks a new internet is long overdue.

**REPLY** ▶**SHOW MORE COMMENTS** ▶



MOST POPULAR

## **This Musical Raspberry Pi Cyberdeck Plays at Live Concerts**

By Ash Hill about 3 hours ago

---

## **RTX 3080 Laptops: All the Models You Can Buy Right Now**

By Avram Piltch about 3 hours ago

---

## **Best Dell and Alienware Deals: nearly \$1,000 off RTX 30 Series Gaming PCs and Laptops**

By Jason England about 3 hours ago

---

## **This AMD and Intel Vending Machine Is Literally a CPU Gamble**

By Francisco Pires about 3 hours ago

---

## **Get This Pixio QHD Gaming Monitor for Under \$260**

By Jason England about 3 hours ago

---

## Ultra Mobile Raspberry Pi Returns With Latest Upgrades

By Les Pounder about 3 hours ago

---

## Microsoft Says Windows 11 Won't Be Able to Run Android Apps at Launch

By Nathaniel Mott about 5 hours ago

---

## Raspberry Pi 4 Resurrects Motorola 68000 Educational Computer Board

By Aleksandar Kostovic about 5 hours ago

---

## Researchers Disclose Meltdown-like Vulnerability for AMD Processors (Updated)

By Aleksandar Kostovic about 5 hours ago

---

## Former Micron Employees Imprisoned for Giving Trade Secrets to China Fab

By Aleksandar Kostovic about 5 hours ago

---

Advertisement

---

---

### BE IN THE KNOW

---

Get instant access to breaking news, in-depth reviews and helpful tips.

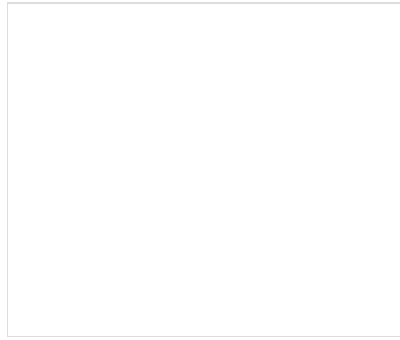
- Contact me with news and offers from other Future brands
- Receive email from us on behalf of our trusted partners or sponsors

**SIGN ME UP**

By submitting your information you agree to the [Terms & Conditions](#) and [Privacy Policy](#) and are aged 16 or over.

---

Advertisement



MOST POPULAR

MOST SHARED



- 1 **Former Micron Employees Imprisoned for Giving Trade Secrets to China Fab**
- 2 **Gigabyte Just Dropped the Best RTX 3080 Laptop Deal We've Ever Seen — \$1,000 off!**
- 3 **First Ransomware to Use Intermittent Encryption Revealed**
- 4 **Windows 10 Tips and Tricks: From Troubleshooting to Life-Changing Productivity Hacks**
- 5 **Windows 11 Launching October 5**

Advertisement

---

Tom's Hardware is part of Future US Inc, an international media group and leading digital publisher. **Visit our corporate site.**

[Terms and conditions](#)

[Privacy policy](#)

[Cookies policy](#)

[Accessibility Statement](#)

[Advertise](#)

[About us](#)

[Contact us](#)

[Coupons](#)

© Future US, Inc. 11 West 42nd Street, 15th Floor, New York, NY 10036.