HELENA ISABEL GONÇALVES DE LIMA

CRYPTOCURRENCIES AND FUNDRAISING: A CHALLENGE TO THE EU COUNTER TERRORIST FINANCING LEGAL FRAMEWORK

Dissertation aimed at obtaining a Master's in Law degree, in the field of Law and Technology

Supervised by

Athina Sachoulidou

Assistant Professor at NOVA School of Law

September 2021

HELENA ISABEL GONÇALVES DE LIMA

CRYPTOCURRENCIES AND FUNDRAISING: A CHALLENGE TO THE EU COUNTER TERRORIST FINANCING LEGAL FRAMEWORK

Dissertation aimed at obtaining a Master's in Law degree, in the field of Law and Technology

Supervised by

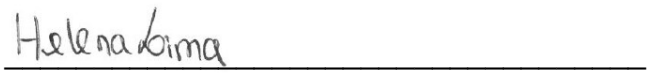
Athina Sachoulidou

Assistant Professor at NOVA School of Law

September 2021

ANTI PLAGIARISM STATEMENT

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



Helena Lima

To my grandmother

ACKNOWLEDGEMENTS

Writing this thesis was a challenging adventure which would not have been possible without the support of several people.

A special acknowledgment is due to my supervisor, Professor Athina Sachoulidou, for her exceptional guidance over the past year and for her prompt responses. With her advice and rigor, I was challenged at every step, whilst feeling encouraged to do more and better. Above all, I feel grateful for the optimism she transmitted to me.

To my colleagues and friends, particularly Maria Inês, Nicole and Maria Carolina, my gratitude for their friendship and words of comfort.

To my boyfriend and best friend, my eternal safe haven in the tightest hours, whose patience and companionship was endless, a "thank you" is not enough.

To my parents and my brother, pillars of my personal and professional formation, to them I owe everything.

To my grandmother Isabel, who left me before the conclusion of this work, to whom I dedicate this thesis. I miss you forever.

… To all, my most sincere and profound gratitude.

CITATION MODE AND OTHER MENTIONS

I. Unless otherwise stated, all the Articles and Annexes cited in the present thesis belong to 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 ("4AMLD"), as amended by the Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849, and thus will be referred to as "5AMLD", as a consolidated version. Unless otherwise stated, the Recitals cited in the thesis belong to the Directive (EU) 2018/843 itself.

II. When references to webpages are made on footnotes, following citations referring to the same source will be done by using the expression "*op. cit*.", followed by the number of the footnote where the source is first cited. Where the source cited is the last on a footnote, the expression "*ult. op. cit*." will be used.

III. The European Union case-law used in this thesis was cited according to the Court of Justice of the European Union citation mode.

IV. When figures and graphics are elaborated according to information found on the scholarship and institutions, the expression "Based on" will be employed. When nothing is declared, the figures and graphics are of my own authorship.

V. The table of contents is presented at the beginning of the thesis, according to the English tradition.

DECLARATION OF CHARACTERS NUMBER CONFORMITY

I declare that the body of the present dissertation, including spaces and footnotes, has a total of 198,711 characters.

Helena Lima

Helena Lima

ABSTRACT

Although bitcoin appeared more than 10 years ago for the first time, cryptocurrencies are still perceived as a novelty and there are persistent doubts regarding their legal treatment and the regime applicable to the respective services. The risks cryptocurrencies pose have attracted a great deal of attention from the Financial Action Task Force and the EU legislator. In 2018, the EU addressed the money laundering and terrorism financing risks arising from the use of cryptocurrencies. This thesis will examine whether and to what extent the existing legal framework responds to the challenges associated with cryptocurrencies, especially when it comes to tackle terrorism financing. In doing so, it will argue that despite the great steps made at EU level, legal gaps and implementation hurdles still exist. Lack of clarity leads to different interpretations of the existing rules – fact that inevitably poses further challenges to be addressed by the multiple anti-money laundering and countering terrorism financing actors.

Keywords: cryptocurrencies; terrorism financing; exchanges; wallets; P2P; Directive (EU) 2018/843.

RESUMO

Não obstante a existência da bitcoin remontar há mais de 10 anos, as criptomoedas são ainda vistas como uma inovação e dúvidas persistem quanto ao seu enquadramento legal e quanto ao regime aplicável aos serviços em seu torno. Os riscos criados pelas criptomoedas atraíram a atenção do Grupo de Ação Financeira Internacional e do legislador da UE. Em 2018, a UE abordou os riscos de branqueamento de capitais e de financiamento do terrorismo originados pelo uso de criptomoedas. A presente tese irá analisar se e em que medida o quadro jurídico existente responde aos desafios associados às criptomoedas, especialmente no que ao combate ao financiamento do terrorismo diz respeito. Ao fazê-lo, defenderá que, apesar dos importantes passos dados a nível da UE, continuam a existir lacunas na lei e obstáculos à sua implementação. Falta de clareza gera diferentes interpretações das regras existentes – facto que inevitavelmente coloca mais desafios a serem endereçados pelos agentes da luta contra o branqueamento de capitais e o financiamento do terrorismo.

Palavras-chave: criptomoedas; financiamento de terrorismo; serviços de troca; serviços de carteira; P2P; Diretiva (UE) 2018/843.

TABLE OF CONTENTS

ACRONYMS AND ABREVIATIONS

29WP	Article 29 Data Protection Working Party
4AMLD	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
5AMLD	Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849
9/11	September 11, 2001 attacks
AECs	Anonymity-enhanced cryptocurrencies
AML	Anti-money laundering
AML/CTF	Anti-money laundering/Countering Terrorist Financing
AMLA	Anti-money laundering authority
AQB	Izz ad-Din al-Qassam Brigades
Art./ Arts.	Article/ Articles
BO	Beneficial owners
BTC	Bitcoin
BTM/ BTMs	Bitcoin Automated Teller Machine/ Bitcoin Automated Teller Machines
CC/ CCs	Cryptocurrency/ Cryptocurrencies
CDD	Customer Due Diligence
Cf.	Confront
CJEU	Court of Justice of the European Union
CoE	Council of Europe
CSP/ CSPs	Cryptocurrency Service Provider/ Cryptocurrency Service Providers

CTF	Countering Terrorist Financing
DeFi	Decentralized Finance
DEXs	Decentralized exchanges
DLT	Distributed Ledger Technology
DOJ	Department of Justice
EBA	European Baking Authority
EC	European Commission
ECB	European Central Bank
EDD	Enhanced Due Diligence
EDPS	European Data Protection Supervisor
EP	European Parliament
EU	European Union
EUCFR	Charter of Fundamental Rights of the European Union
FATF	Financial Action Task Force
FIU/FIUs	Financial Intelligence Unit/ Financial Intelligence Units
GDPR	General Data Protection Regulation/ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC
HRTCs	High-risk third countries
ie	*id est*/ namely/ that is to say
ICOs	Initial Coin Offerings
ICSFT	International Convention for the Suppression of the Financing of Terrorism
IMF	International Monetary Fund

ISIS	Islamic State of Iraq and Syria
ITMC	Ibn Taymiyya Media Center
LEAs	Law enforcement agencies
MAITIC	Meir Amit Intelligence and Terrorism Information Center
MEMRI	Middle East Media Research Institute
MS/ MSs	Member State/ Member States
NCAs	National competent authorities
No.	Number
OECD	Organisation for Economic Co-operation and Development
op. cit.	opera citato/ work cited
p./ pp.	page/ pages
P2P	Peer-to-peer
PPPs	Public-private partnerships
RBA	Risk-based approach
RegTech	Regulatory Technology
SDD	Simplified Due Diligence
STR/ STRs	Suspicious transaction report/ Suspicious transaction reports
SupTech	Supervisory Technology
TEU	Treaty on the European Union
TF	Terrorist/ Terrorism Financing
ult. op. cit.	latest work cited
US	United States

INTRODUCTION

2009 was marked by the appearance of the first successful implementation of a cryptocurrency (CC): bitcoin[1]. It was firstly accepted on May 22, 2010, when two pizzas were bought for 10,000 bitcoins (Higgins, 2019; Frick, 2019). The first bitcoin Automated Teller Machine (BTM) appeared in 2013, in Canada, allowing users to convert cash into bitcoin, and vice-versa[2]. Nowadays, several e-commerce websites and shops accept it as a means of payment (Rothstein, 2017.). The University of Nicosia, which offers a Master of Science degree in Digital Currency, accepts bitcoin to pay for tuition (Rothstein, 2017). In the beginning of 2021, bitcoin surpassed the $30,000 barrier (Bentley, 2021). Thus far there are almost 12,000 CCs[3]. CC payment networks such as Monero and ZCash provide for increased privacy and criminals have taken refuge on anonymity features. Terrorists use CC as a tool to raise funds, instructing its supporters how to conduct such transactions without getting noticed, posing new challenges to public authorities.

The European Commission (2016ª) identified in CCs a significant risk due to their legal voidness. After years of discussion and uncertainty, CCs commendably conquered a place in the European Union (EU) legislation through the Directive (EU) 2018/843 (5AMLD), which strengthened the EU countering terrorist financing (CTF) arsenal, amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (4AMLD). It responded to "emerging new trends, in particular regarding the way terrorist groups finance and conduct their operations" (Recital 2) by limiting CCs' and CC service providers anonymity (EC, 2019). When referred in combination, exchanges and wallet providers are referred to as "cryptocurrency service providers" (CSPs).

---

[1] Capital letter and lower-case letter are used, respectively, to describe the payment network and the cryptocurrency *per se*. The term applied throughout this dissertation will be "cryptocurrency", as it highlights the use of cryptography. Both International Monetary Fund (IMF – He *et al*, 2016) and World Bank Group (2017) consider cryptocurrencies (CCs) as a subset of digital currencies due to cryptography. It is also the most widely used term among the CC industry. Coin Market Cap defines CC as the "digital medium of exchange using strong cryptography to secure financial transactions". Available at https://coinmarketcap.com/alexandria/glossary, accessed on 14.11.2020.

[2] Available at https://www.bbc.com/news/av/technology-24756030, accessed on 14.11.2020.

[3] Available at https://coinmarketcap.com/, accessed on 09.09.2021. On 26.11.2019, when the present research started, there were almost 5,000 CCs. On 10.10.2020, that number reached around 7,500.

The present thesis will examine the EU response to the use of CCs for terrorism financing (TF) purposes. The topic is of pivotal importance as funds are at the core of any terrorist organisation, in its various sizes and shapes, and CCs present new risks that need to be tackled. In 2019 alone, €117 to €210 billion were linked to suspicious transactions and activities occurring in the EU financial and economic ecosystems (EC, 2021[a]). In 2020, 449 individuals were arrested in the EU for terrorism-related offences. On December 15, 2020, the Criminal Court of Lisbon sentenced an individual eight and a half years imprisonment for TF. Despite CC use in TF is deemed low, empirical data demonstrates that it is a potential threat (Europol, 2021[a]).

I. PHENOMENOLOGY AND CENTRAL CONCEPTS

1.1. Cryptocurrencies and blockchain: a paradigm shift

The idea of a CC has its origin long before the year of 2009. Its economic foundations lay on the Austrian School of Economics, which postulates that government intervention leads to inefficiencies (European Central Bank – ECB, 2012) and that private currencies should exist (Eiserman, 2020). CC materialize the libertarian *ethos* of supporting individual freedom (Karlstrøm), and are associated with anarcho-capitalism, *ie* private property, free markets and giving masses the control (Flood *et al*, 2017). Private banks did not escaped distrust due to privacy concerns (Higgins, 2019), and cypherpunks, activists advocating for the proliferation of privacy-oriented technologies, also played a role on this evolution (Karlstrøm, 2014; Rothstein, 2017). There were several attempts to put these ideas into practice: eCash in 1982, B-money project in 1998, and BitGold, publicly presented in 2005 (Tsikhilov, 2020). Distributed Ledger Technology (DLT) and cryptography were the solutions presented by Satoshi Nakamoto, whose identity remains a mystery, to accomplish a full working system. Bitcoin was presented in November 2008 as "[a] purely peer-to-peer version of electronic cash [which] would allow online payments to be sent directly from one party to another" (Nakamoto, 2008, p. 1). Bitcoin was launched in January 2009 (Frick, 2019). Following a CC-oriented definition,[4] blockchain technology, a type of DLT,[5] is "a ledger that lists all of the units of the cryptocurrency and who owns them" (Rothstein, 2017). Centralization gives place to peer-to-peer (P2P) networks, a decentralization of authority (Kethineni *et al*, 2019). Nodes validate transactions, and miners perform "something like the record-keeping service of blockchain" (Daskalakis *et al*, 2020, p. 12). Blockchain came to be the solution "to the age-old human problem of trust" (Werbach, 2018, p. 489), through a system where records are kept public (Nakamoto, 2008). Encryption is crucial to repel unauthorized access and ensure that only the intended recipients view the information (Malik, 2018; Daskalakis *et al*, 2020). Private keys are used to sign transactions and prove identity, whereas public

[4] Although we refer to blockchain in connection with CC, blockchain exists without it (Tsikhilov, 2020).
[5] DLT is sometimes used interchangeably with the term blockchain. However, DLT is the broader category of which blockchain is part of (Eisermann, 2020).

keys are used to receive funds (Daskalakis *et al*, 2020) and might be linked to a person in the physical world – *ie* a person remains identifiable, which is referred to as pseudonymity (Keatinge *et al*, 2018; Barone, 2018[a]; Frick, 2019).

With a total market capitalization of € 388,064,694,943,[6] CCs do not yet have a defined taxonomy and are assigned with several designations: (decentralised) virtual currencies (Salami, 2017; ECB, 2012), electric coins (Karlstrøm, 2014) or even electronic coins (Nakamoto, 2008). Resorting to the term "virtual currencies", the EU legislator defined it as the "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" (Art. 3[18]). CCs are thus opposed to fiat currency, e-money, funds as defined in Art. 2(2) Directive 2009/110/EC, local currencies, the instruments laid down in Art. 3(k; i) Directive (EU) 2015/2366 on payment services in the internal market, in-game currencies, and should not be mislabeled as e-payment networks such as Visa or PayPal (Recital 10; Barone, 2018[a]). Although bitcoin has a 66,2% market dominance,[7] there are other CCs, such as ether and monero, which are called alternative coins or alt-coins[8]. Some of them are often described as privacy coins, as they obfuscate "senders, receivers, or amounts […] exchanged" (Chainalysis, 2020, p. 68). Financial Action Task Force (FATF, 2020) uses the term "anonymity-enhanced cryptocurrencies" (AECs) instead[9] – this term will be used in turn.

The following fictional scenario is designed to assist the reader understand the key elements of this ecosystem:

Mary goes on an exchange to convert fiat for bitcoin to send it to Bob. Through exchanges CCs are convertible to fiat, and vice-versa[10]. This is an exchange service *stricto sensu*, which includes, for instance BTMs. Decentralized Exchanges (DEXs),

---

[6] *Ult. Op. Cit.* footnote 3.
[7] *Ult. Op. Cit.* footnote 3.
[8] *Ult. Op. Cit.* footnote 1.
[9] FATF's role in shaping AML/CTF legislation will be analysed in Section IV.
[10] E.g., Binance, Coinbase Pro and Kraken. Available at https://coinmarketcap.com/rankings/exchanges/, accessed on 12.11.2020. On 06.06.2021, there were 383 exchanges. Available at *Op. Cit.* footnote 3.

on the contrary, allow P2P exchange of CCs[11]. Mary and Bob have wallets, a sort of an account, installed on their computers, a software to send, receive, and store CCs (Daskalakis *et al*, 2020). Wallets can be self-hosted/non-hosted/non-custodian, where a person does not resort to any middleman to safeguard the private keys[12]; or hosted/custodian wallet, where a third party gets involved to control user's CCs. Wallets can also assume two forms: hot/online storage, *ie* software wallets installed on devices connected to the Internet, allowing the user to store private keys online[13]; or cold/offline storage, which amount to USB or hardware wallets, software installed and running on offline computers, or most rudimentarily, paper. Hot/online wallets can be custodian and non-custodian wallets, whereas cold/offline wallets are always non-custodian. To sum up, there are two types of control over CCs (custodian/non-custodian), and two types of storage (online/offline) (Lielacher, 2021). Back to the example outlined above: Mary sends a message to the network announcing "I am Public Key 193Sh5LWc89NQLpaxVeziUExcn8RHrB3J4. Please transfer 2 (two) coins to Public Key 2N8gxtiN8SgcEgFWhLwS4rsIRhcxowPjTg" and signs that request with her private key (Higgins, 2019, p. 31). Her and Bob's public keys will be visible on blockchain and known to everyone when the transaction gets concluded (Daskalakis *et al*, 2020). Should Mary have had privacy concerns, she could have resorted to AECs or to mixers/tumblers, *ie* services making it possible to sort of "breaking down transactions into smaller parts — and mixing them with others"[14] reducing the risk of traceability (Keatinge *et al*, 2018). Therefore, blockchain and CCs lead to a paradigm-shift allowing not only for disintermediation and transparency, but also to the implementation of a trustless system (Whyte, 2019).

1.2. Cryptocurrency-enabled (cyber)crimes

Despite its use does not constitute an illegal practice, Europol (2020[a]) warns that CCs pose criminal threats. Some authors (Higbee, 2018; Mabunda, 2018) consider that it is undeniable that CCs are transforming cybercrime, and that monero was the most targeted CC (Goldman *et al*, 2017). On the contrary, Harvey (2014)

[11] Available at http://gpml-crypto.org/modules/Crypto%20English/launch.html, accessed on 26.10.2020.
[12] E.g., Trezor and SafePal (Lielacher, 2021).
[13] E.g., Electrum, Armory, Edge and Trust Wallet (Lielacher, 2021).
[14] *Ult. Op. Cit.* footnote 1. E.g., DarkWallet, Samurai and BitcoinFog (Zenko, 2017).

points out that bitcoin is not a viable and wanted alternative for criminals, as cash is anonymous. However, Eisermann (2020) draws the important conclusion that assuming that bitcoin is not suitable to conduct illegal activities due to traceability is wrong as there are various mechanisms that allow criminals to obfuscate their steps. Thus, most of the scholars agree that CCs are being used by criminals. CCs are often associated with crimes of tax evasion, money laundering (ML), and extortion (Kethineni *et al*, 2019). In addition, privacy-enhancing tools have started magnetizing criminals (Europol, 2020[a]) and are widely accepted and encouraged to be used on the Dark Web – *ie* a segment of the Internet which contains "content that has been intentionally concealed" (Weimann, 2016, p. 40). The Internet is comprised of several layers: one accessible to all users, known as Surface Web, and two deeper layers, known as Deep Web and Dark Web, whose websites are not indexed on search engines such as Google, and access is only granted by specialized browsers which obfuscate IP addresses and communications such as The Onion Router and Invisible Internet Project, respectively (Weimann, 2016). Criminals have resorted to botnets, *ie* thousands of hacked computers which gather all the necessary computational power required, to mine monero (Brill *et al*, 2014; Higgins, 2019). The Deep Web Silk Road black market, which operated from January 2011 to October 2013, is one of the most widely known examples of how CCs and particularly bitcoin was abused by criminals (Brill *et al*, 2014). CCs are being used in the monetization of child sexual abuse material, and associated with online investment fraud through Initial Coin Offerings (ICOs),[15] scams[16] and Ponzi schemes. Besides this, CCs are employed to perpetrate sextortion and ransomware[17]. In 2019, 10 exchange hacks resulted in the theft of €240 million (Europol, 2020[a]). There were also cases of people being physically robbed (Cuthbertson, 2019). Lastly, CCs serve as a lure for money mules (Europol, 2020[h]). That said, although CCs are not used only by criminals, it is indeed abused in the

[15] ICOs "are generally a means to raise funds for new projects from early backers" (FATF, 2019, p. 16).
[16] The most recent CC-scam took place on July 15, 2020. Several hacked public figures' Twitter accounts published the message "send me BTC [*ie* bitcoin] and I'll send you back double, I promise!" (Zuckerman, 2020).
[17] The most widely known CC ransomware attack was WannaCry 2.0., in May 2017. It targeted public services and companies in more than 100 countries, demanding bitcoin as ransom to unlock access to computers' systems and data (Kethineni *et al*, 2019).

(cyber)crime settings. As such, CCs are defined as (cyber)crime facilitators (Europol, 2020[a]).

1.3. The "old school" terrorism financing and cryptocurrencies

Defining TF presupposes defining terrorism. However, despite the quite often claim that "[o]ne knows terrorism when one sees it" (Deen, 2010), the definition of terrorism has not been crystalized yet – with the Council of Europe (CoE) calling for uniformisation to avoid exploitable gaps (Committee of Ministers of the CoE, 2015). The definition of terrorism used in the present dissertation is the one provided by the EU legislator in Art. 3(2) Directive (EU) 2017/541 in terms of a definition commonly accepted at supranational level (e.g., §10 of the CoE Convention on the Prevention of Terrorism preamble). According to that, terrorism entails behaviours "(a) seriously intimidating a population; (b) unduly compelling a government or an international organisation to perform or abstain from performing any act; (c) seriously destabilizing or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation".

It was December 9, 1999 when the International Convention for the Suppression of the Financing of Terrorism (ICSFT) was adopted and it provided for the first definition of TF as a standalone crime to harmonise national legislations and enhance international cooperation. Nonetheless, it was the September 11, 2001 events (9/11) that make it a priority (Keatinge *et al*, 2018). Hence, the TF definition provided on Directive (EU) 2017/541 is based on the definition provided by the ICSFT. TF is the act of "providing or collecting 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, to commit, or to contribute to the commission of, any of the offences referred to in Articles 3 to 10" (Art. 11[1]). As such, it is unlawful to finance (1) terrorist offences committed with the aims listed on Art. 3(2); (2) terrorist groups; (3) public provocations to commit terrorism; (4) recruitment, (5) training, and (6) travelling for the purposes of terrorism. TF will be punishable irrespective of the funds are used or effectively contribute to those offences, and the financial supporter does not need to know which specific expenses the funds are aimed to cover for (Art. 11[2]). TF is prescribed with a maximum sentence of no less than 8 years (Arts. 15[3]; 4[b]).

Terrorists need funds to cover their (1) operational expenses, which comprise planning and executing attacks and (2) organisational expenses, which are the natural consequence of an organisation day-to-day maintenance (Norton *et al*, 2016). The scale of costs incurred varies depending on the magnitude of the attack and the type of organisation *in casu*: larger organisations are able to commit large scale attacks, incurring more costs; a medium-scale attack may cost less than $15,000; the so-called lone wolves[18] and cell structures commit low-scale but high impact attacks (Durner *et al*, 2018), reducing the need for major funding[19] (e.g., guns or cars used to target civilians on the streets) (Rose, 2018) – involving amounts easy to transmit but difficult to detect (Goldman *et al*, 2017; Durner *et al*, 2018). Territory-attached groups need more funds (Rose, 2018). Other expenses include recruitment, training and the payment of wages, as terrorist organisations act as employers. Palestine terrorist organisations paid about $30,000 to suicide bombers' families (Koh, 2006). Lastly, there is also the need for financial resources to "equip" the propaganda machine as shown by a December 2020 job advertisement for poster designers, video producers, and singers for jihadi songs (Middle East Media Research Institute - MEMRI, 2020[a]). Concerning the money-making process, the literature distinguishes terrorists' proceeds into licit and illicit forms (Rébé, 2019), criminal proceeds, donations and legitimate businesses (Koh, 2006), and emphasizes the abuse of charitable funds or the diversion of funds from legitimate organisations into spurious ones (Rose, 2018). TF can have legitime sources as, precisely, donations – when it is originated from lawful income (Durner *et al*, 2018). TF does not entail a predicate offence as ML; its unlawfulness is based on the distribution of or making available funds to terrorists. TF is preparatory in nature (Tofangsaz, 2015). Prior to the 9/11 events, it is estimated that the al-Qaeda had a $30 million annual budget, and that the majority of it was comprised by donations (Bernardi, 2019). There are reports suggesting that Islamic State of Iraq and Syria (ISIS) raised around $2 billion in 2014[20].

Contrary to ML, TF usually involves small amounts of money precisely to avoid detection (Eisermann, 2020). The Organisation for Economic Co-operation and

[18] *Ie* "isolated religious fundamentalist actors deciding to act on their own, in the name of a foreign leader" (Rébé, 2019, p. 9).
[19] Also known as hybrid or low-cost terrorism (Barone, 2018[a]).
[20] Available at https://thesoufancenter.org/intelbrief-2021-march-12, accessed on 16.08.2021.

Development (OECD, 2019) clarifies that in ML the offense is the source of proceeds, whereas in TF the offense is the destination of the proceeds. Anti-money laundering and countering terrorist financing (AML/CTF) obligations placed on financial institutions led to the marginalization of high-risk individuals and the migration effect to informal value transfer schemes. The *hawala* network is an informal remittance system "which rel[ies] on networks of trusted individuals in the countries from which the funds originate and those to which funds are transferred, without leaving formal records of the transaction" (Europol, 2020[c], p. 24). It is a long in use scheme by terrorists (Salami, 2017) and is largely based on trust, honor and reputation (Whyte, 2019)[21]. The most recent use of the *hawala* scheme occurred in 2020, facilitating "the final transactions sent from Spain to the conflict zones" (Europol, 2020[e]). Resorting to *hawala* presents, nevertheless, drawbacks: it is not suitable to collect funds from multiple sources neither to allocate funds to dispersed locations and it might be difficult to arrange trustworthy intermediaries (Irwin *et al*, 2016). Thus, terrorists are "more and more shifting in the online realm", resorting to social media to call for funds due to its pragmatic nature (Barone, 2018a, p. 17; Hasbi *et al*, 2018). Keatinge *et al* (2018) state that CCs are not attractive due to their volatile nature and usability barriers. Goldman *et al* (2017) claim that it is not a viable solution as TF entails a kind of trust that is not achievable in the CC settings as it is not completely anonymous. With a dissident opinion, Whyte (2019, p. 19) even resorts to the term "cryptoterrorism" to describe the numerous ways in which terrorists might benefit from CCs. Several authors (Norton *et al*, 2016; Eisermann, 2020; Barone, 2018[a]) and Europol (2016) recognize that CCs pose significant TF risks *inter alia* when calling for funds as they provide for financial anonymity (Weimann, s.d.). Empirical data shows that terrorists are resorting to CC, even if not systematically or not to the same extent as other criminals (Barone, 2018[a]). CCs are employed by the so-called lone wolves to anonymously supply themselves, by small cells to either receive CCs from the central group or to finance lone wolves, and by territory attached large groups that need big amounts of money to manage their lands (Bernardi, 2019). Al-Sadaqah, a Syrian Internet-based terrorist organisation (Liv, 2019), implemented in September 2012 the first known bitcoin

[21] There are other informal value transfer systems such as Hue, Fei-Ch'ien, Phei Kwan, Hundi and Hui Kuan (Weiss, 2005).

fundraising (Azani *et al*, 2013)[22]. However, by August 2020, the wallet address was seized by the United States (US) government (United States of America v. 155 Virtual Currency Assets). ISIS is reported to have collected $23 million worth in bitcoin in August 2015 alone (Sanders IV, 2015). The "Albanian hacker", tied to ISIS, committed a bitcoin ransomware attack against an Illinois Internet retailer, gaining access to the identities of 1,351 US government and military workers and drafting a "kill list" (Goldman *et al*, 2017). The July 2016, Munich shopping center shooting, classified as an act of terrorism, involved the use of bitcoin for the purchase of the weapon and ammunition (Eisermann, 2020). In 2018, Rod and Rachel Saunders were abducted and murdered in South Africa by four ISIS-affiliated groups, and their stolen credit cards were used to acquire bitcoin (Barone, 2018[a]). In September 2019, French authorities arrested 29 individuals for buying CC coupons ranging from €10 to €160, which were then converted into CCs by whom the coupons were credited to (Grauer *et al*, 2021; CipherTrace, 2021). It is thought that hundreds of thousands of euros were supplied to al-Qaeda and ISIS through such scheme[23]. Kais Mohammad was charged in the US for having conducted in-person exchange of up to $25 million (CipherTrace, 2021). It is believed that, in October 2020, a Telegram account belonging to a pro-jihadi news network run by a US-born journalist advertised the acceptance of bitcoin and monero donations (MEMRI, 2020[b]). Therefore, evidence shows that terrorists have already adapted their financing methods to the new digital environment, namely to CCs.

[22] There is no agreement on such date, with literature (Liv, 2019; Barone, 2018a) arguing it began in November 2017. However, Azani *et al* (2013) reported on this campaign, stating that it was active since September 2012.

[23] Available at https://apnews.com/article/arrests-terrorism-archive-france-701371a367d1ae26ff057d6e3d08245, accessed on 21.04.2021.

II. RESEARCH QUESTIONS AND METHODOLOGICAL APPROACH

The present thesis followed a qualitative and exploratory methodology. Through the research process, the research was narrowed, from illicit practices associated with CCs in general, to TF. The scope was even further narrowed to cover a very specific form of TF, *ie* donations.

The research was conducted through the following central and derived questions:

- Is the EU CTF legal framework able to tackle CC fundraising campaigns?
  (1) Are terrorists and their supporters resorting to CCs? If so, how?
  (2) Does the EU legal approach respond to all problems? Which problems does the EU solve and which does not?
  (3) Which approaches can complement the 5AMLD's loopholes?

Following the introduction of basic concepts pertaining to the CC setting, related criminality and its connection to TF, Section III proceeds to provide empirical data. Such exercise was, nonetheless, limited to the most representative examples. Section IV is devoted to critically analyse the EU regulatory response, focusing on the CC-related services brought under its scope, its main obligations, as well as the roles fulfilled by public authorities, and the potential existence of regulatory gaps. Section V introduces the last part of this investigation, which analyses possible solutions and improvements to the problems encountered, not disregarding potential limitations.

III. CRYPTOCURRENCIES AND TERRORISM FINANCING 2.0.

3.1. The background ecosystem

The year of 2020 marked the uncovering, investigation and prosecution of more CC TF schemes than ever before (Grauer *et al*, 2021). It results from terrorists encountering low barriers to enter a permissionless system, materialized by no Customer Due Diligence (CDD) (Barone, 2020), as well as to the fact that investigations focus very much on *hawala* (Habib, 2017). Yet, economic and religious reasons might constitute obstacles for terrorists when resorting to CC. Terrorists might be hacking victims. *In loco* CSPs might present high costs (Brill *et al*, 2014). Its resemblance with gambling, due to its volatility, makes it not *sharia*-compliant (Barone, 2018[a]). Despite the counter-narrative prohibiting the use of bitcoin, CC use is being encouraged by terrorists trying to turn it into a *sharia*-compliant value to avoid reputational impacts for those who resort to it and stressing its advantages: Ali Shukri Amin – a 17-year-old Virginia teenager convicted for 136 months in prison in August 2015 for providing material support to ISIS (US Department of Justice – US DOJ, 2015) – presented CCs as a convenient tool to circumvent and limit economic support of the Western banking systems (Hasbi *et al*, 2018); the Muhammad ibn Muneer's May 2019 Telegram post discussing bitcoin and its permission under *sharia's* concepts of buying, selling and trading, as opposed to other CC (MEMRI, 2019) (cf. Figure 10); and the Technical Support of *Afaq* Electronic Foundation's – an ISIS' associated media group – explanation on bitcoin's security on Telegram, stating, however, zcash to constitute a securer alternative (Weimann, s.d.). Through CCs, terrorists can create wallets and continuously buy and change cheap computers and electronic devices every month to avoid detection (Teichmann, 2018). They can post addresses online and raise funds with little to no effort (Keatinge *et al*, 2018), whilst guaranteeing anonymity for their supporters as well (Teichmann, 2018). CCs are used by the various categories of terror actors – organisations *per se*, support and propaganda groups, and individuals (Azani *et al*, 2018). As remarked by Bernardi (2019, p. 9) "[o]verall, the use of cryptocurrencies should be seen as part of a general shift towards online terrorism".

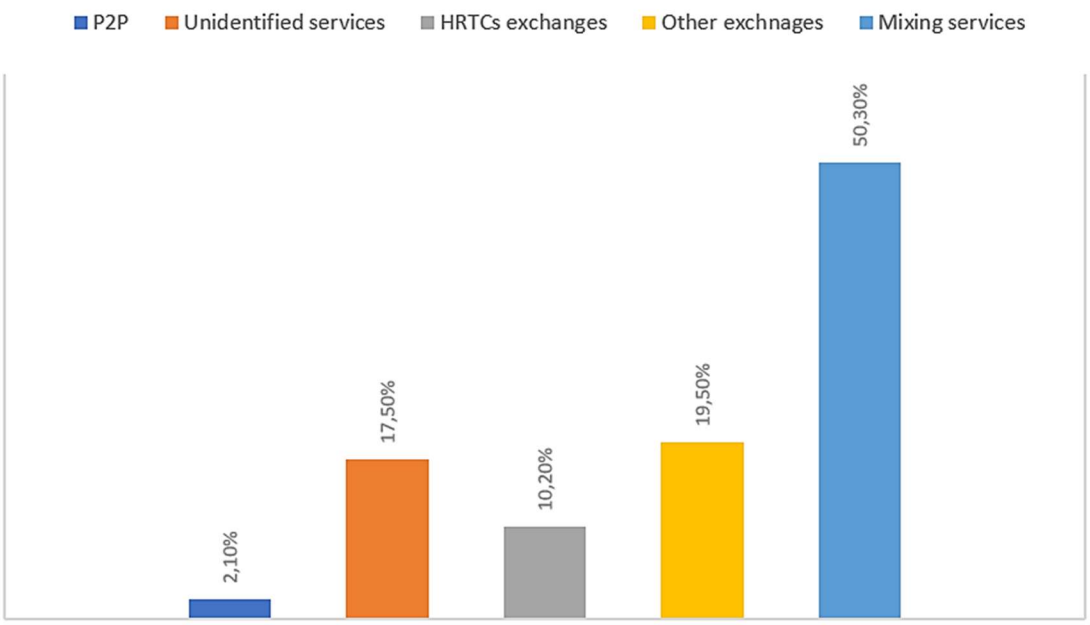
3.2. Explicitly financing terror and deluding donors

Supporting al-Qaeda. Ibn Taymiyya Media Center (ITMC), also known as al-Raya foundation (Meir Amit Intelligence and Terrorism Information Center - MAITIC, 2020[a]), is the media outlet unit of Mujahideen Shura Council in the Environs of Jerusalem placed in the Gaza Strip (Chainalysis, 2020). The "*Jahezona*"[24] bitcoin fundraising campaign started in July 2015 (Barone, 2018[a]) to support the jihad in Palestine (MAITIC, 2020[a]). It was from June 2016 to January 2018 that the campaign, driven annually (Barone, 2018[a]) under the slogan "from you money and from us our blood" (Bernardi, 2019, p. 12), started calling for $2,000 (MAITIC, 2019[e]) to $2,500 contributions to equip each Salafi Army fighter (Fanusie, 2016) (with graphics showing the desired equipment and its cost – Barone, 2018[a]) (cf. Figure 11). A wallet address was spread in the form of a QR code on Twitter (Fanusie, 2016). The campaign received two transactions of around $540, believed to be a test (Barone, 2018[a]). Those funds were transferred to unknown wallets. The campaign was continuously running, even though Twitter kept taking down *Jahezona*'s account. Its followers granted the continuous act by repeatedly retweeting *Jahezona*'s graphics (Fanusie, 2016).

Visiting al-Raya Foundation's website for the purposes of this research on December 18, 2020, it could be seen that a bitcoin fundraising campaign was still operating in May 2020 to acquire weaponry[25]. Incoming and outgoing e-mails, Telegram and Threema contacts, were provided, as well as a click-button that displayed a box, with a $9 default donation which could be increased or decreased (cf. Figure 12-Figure 15). In June 2020, a new plea is made on Twitter and replicated on the al-Raya website. ITMC explains that bitcoin is an optimal solution as it is "the most secure service, [t]he most accessible of our time" and directs donors to the crypto payment processor Blockonomics[26].

[24] In Arabic means "Equip us" (Keatinge *et al*, 2018, p. 29).
[25] The website does not provide a specific date for the content. However, through the method showed on the search bar on Figure 16, plus the append of the expression "&as_qdr=y15" at the end of the hyperlink in the Google Chrome bar, we can reach the publication date.
[26] Available at https://alraia.net/en/bitcoin-digital-currency/, accessed on 18.12.2020. Crypto payment processors are "services that help businesses handle payments in crypto". Available at https://coinmarketcap.com/headlines/news/crypto-payment-gateways-similarities-and-differences/, accessed on 17.02.2021.

Graphic 1 - ITMC's campaign statistics.



Based on Chainalysis (2020)

A low percentage of transactions with ITMC resulted from P2P interactions. Unidentified services were involved as well as exchanges located in high-risk third countries (HRTCs)[27] (Chainalysis, 2020). Funds were originated from services such as BTC-e.com, and destination wallets pertained to addresses present on localbitcoins.com, matbea.com and cloudbet.com (Fanusie, 2016), which are used for P2P in-person trading and are useful tools when looking for anonymity to withdraw CCs (Barone, 2018[a]). A major percentage of transactions involved mixing services. Tens of thousands of dollars were raised, largest donations involving amounts ranging from $1,000 to $2,500. ITMC scattered the funds over several addresses, presumed to have been converted into cash, to obfuscate any traces (Chainalysis, 2020). Nevertheless, by providing a single wallet address and spreading it online US law enforcement agencies (LEAs) were able to track CC flows and shut down the campaign in August 2020 (Popper, 2019).

[27] HRTCs are “jurisdictions which have strategic deficiencies in their national AML/CFT regimes that pose significant threats to the financial system of the Union” (Art. 9[1]). The quality and effectiveness of the legal and institutional AML/CTF framework, as well as the powers detained by competent authorities are the features considered when determining a state’s risk (Art. 9[2]).

Supporting ISIS. In November 2017, Akhbar al-Muslimin's website, which updates data on ISIS both on Clear and Dark Web, set the stage for a bitcoin fundraising campaign (Barone, 2018[a]; Liv, 2019). Despite claimed to cover the website activities, it is presumed that funds were intended to cover ISIS' other activities as well (MAITIC, 2019[b]) namely its propaganda machine (MAITIC, 2017). A hyperlink directed donors to CoinGate (Barone, 2018[a]). Then, it started to direct them to an internal webpage, set to generate unique wallet addresses each time it was open (Azani *et al*, 2018), a practice that demonstrates ISIS' quick adaptability to avoid being tracked. In addition, Akhbar al-Muslimin provided how-to videos on the use of the VirWoX exchange to acquire bitcoin, and localbitcoins.com (MAITIC, 2019[a]; MAITIC, 2019[c]). In March 2019, as the website was apparently being successively closed, visitors received instructions to send a blank e-mail to a provided contact, receiving, then, the updated hyperlink to a mirrored website. By November 2019, after a long period of inactivity, the group designed a new website to request donations (MAITIC, 2019[c]). In June 2020, Akhbar al-Muslimin requested monero, instead, including a tutorial on the CC. By that time, the group's wallet was reported to contain approximately $2,700 (Fadilpašić *et al*, 2020) (cf. Figure 18).

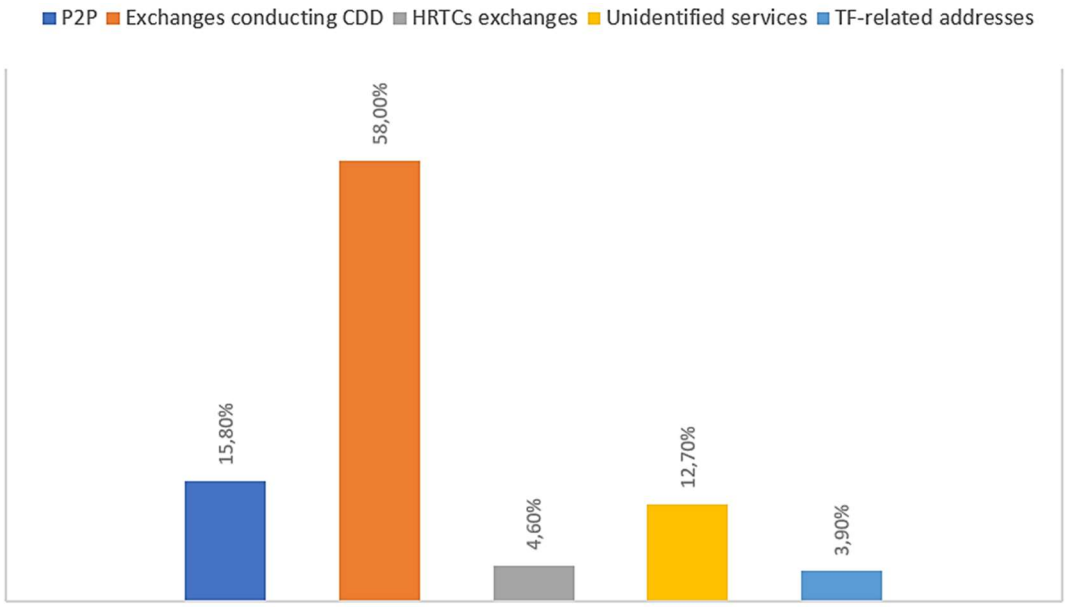
Between March and August 2017, Zoobia Shahnaz illegitimately obtained bank loans and stole credit cards, gathering around $85,000, from which around $62,000 was converted into bitcoin and other CCs. Shahnaz transferred the funds to individuals and vehicle-entities located in China, Pakistan and Turkey to support ISIS militants in Iraq and Syria, which seem to have been designed to avoid CDD requirements. Shahnaz tripped up in the scheme as LEAs detected suspicious transfers of more than $150,000 and was arrested for financially supporting ISIS in December 2017 (Stalinsky, 2019; US DOJ, 2017; Alexander, 2017).

Supporting Hamas. Izz ad-Din al-Qassam Brigades (AQB), the military wing of Hamas, put into action one of the most pioneering and complex CC fundraising campaigns (Chainalysis, 2020). *Method 1* was employed in January 2019, when Abu Obeida, AQB's spokesman, incited supporters to finance the cause through bitcoin. To solve the Palestinian public apparent doubts, an article and an infographic on bitcoin was posted in a Hamas-affiliated newspaper (MAITIC, 2019[d]). Under the slogan "Support the Resistance", the campaign shifted to AQB's official websites (MAITIC, 2020[b]). The group received around $3,000 between February

and March (Liv, 2019). In June 2019, Obeida used Telegram to warn donors that they would receive authentic messages, which should be disseminated. It included explanatory videos, hyperlinks and QR codes directing to donation webpages displayed in eight languages (e.g., French) (MAITIC, 2019f). In July 2019, a transfer stood out as it involved $2,519 (International Institute for Counter-Terrorism, 2019). Between December 2019 and May 2020, a hyperlink was published calling for more donations (MAITIC, 2020[b]). AQB employed its *method 2* and enhanced its fundraising campaign techniques by holding its private key, instead of trusting a middleman. AQB improved its *modus operandi* through *method 3*: a website-integrated wallet and an algorithm to generate a one-donation-one-wallet address system built to safeguard security and privacy (Chainalysis, 2020). A how-to video guide presented users with two arrangements for increased concealment: the delivery of cash to a *hawaladar*, which, in turn, would send the correspondent bitcoin amount to the provided wallet address; the creation of self-hosted wallets by donors themselves, recommending the use of public wi-fi for such setting (Chainalysis, 2020). In August 2020, US LEAs seized AQB's websites and wallet address as it was linked to an US-based regulated exchange (US DOJ, 2020)[28]. Despite all these efforts into breaking down AQB's fundraising campaign, in September 2020 it launched a new campaign with a new address (MAITIC, 2020[b]). Yet, it is believed to has stopped in October (Grauer *et al*, 2021). AQB's method 3 produced more than $10,000, method 2 less than $5,000 and method 1 less than $2,000. In a normal scenario, Chainalysis blockchain analysis company would send a small amount to the address to learn more on it, recognizing however that it is "illegal to transact with an address belonging to a designated terror organization" (Chainalysis, 2020, p. 76). Nevertheless, crossed information with associated cases and transactions that took place in methods 1 and 2, as well as its blockchain analysis tool, provided for the uncover of more than 100 addresses involved in method 3. In a universe of more than 100 donations, 98% involved amounts in a range from $1 to $1,000. Only three donations involved amounts between $1,000 and $2,500 (Chainalysis, 2020).

[28] Coinbase was the US-based exchange used. Its chief compliance officer said that AQB's wallet was immediately frozen after being tied to group and that US authorities were alerted (Popper, 2019).

Graphic 2 - AQB's campaign statistics.



Based on Chainalysis (2020)

AQB's campaign involved a considerable percentage of P2P transactions and exchanges already conducting CDD and, most problematically, wallet addresses already identified as pertaining to terrorism supporters (Chainalysis, 2020).

On May 2019, Jonathan Xie, 20 years old, was arrested in New Jersey and charged, among others, for financially supporting Hamas. In April 2019, besides sending $20 in bitcoin to Hamas, which appeared to be a test, Xie explained an undercover agent how to donate the CC to the group (US DOJ, 2019).

Al-Qaeda opaque humanitarian aid. Among the wallets forfeited on August 2020 by the US LEAs, there were wallets linked to al-Ikhwa Independent Charity (US v. 155 Virtual Currency Assets). The group asked for bitcoin to assist widows and orphans, the smoking gun being the fact that it was tied to Telegram chat groups posting jihadist material (Barone, 2019). Al-Ikhwa was even linked to Malhama Tactical Team, a known terror-linked organisation. The group stated that bitcoin was an alternative to the traditional banking system and that it was untraceable. It posted 11 bitcoin addresses and after 4 months renewed the used addresses on Telegram and Facebook posts. Telegram posts were forwarded by the Reminders from Syria, which requested donations to provide weapons to terrorists in Syria (US v. 155

Virtual Currency Assets; US Immigration and Customs Enforcement, 2020). Al-Ikhwa received around $3,000 (Barone, 2019), having resorted to layering techniques by transferring bitcoin through several addresses to conceal the intended recipient (US v. 155 Virtual Currency Assets). The campaign involved both wealthy and relatively poor addresses, demonstrative of a complex and solid arrangement (Barone, 2019).

3.3. Entrepreneurial terrorists(?)

Theoretically, terrorists can abuse ICOs, either overtly or fraudulently. Nevertheless, it is presumably unlikely, as implementing an ICO is much more complex than simply asking for funds in a non-formal way (Keatinge *et al*, 2018). The closest example of what might look like an ICO structure in the terror ecosystem is SadaqaCoins, which is conceived as a marketplace platform where funders can donate and terrorists can pitch their projects. For instance, "Project: We Hunt" was implemented in August 2018 to equip experienced snipers with sniper rifles and jeeps. Monero was the default CC, donation of other CCs being dependent on support contact (Liv, 2019). The platform also contained an advertisement calling for the ones with powerful computers and proficient programmers, and included a "Four digital ways to support us" guide[29]. Therefore, despite these fundraisings are implemented as projects, similarly to what happens with ICOs, these could have as well been analysed through the lens of a CC fundraising campaign.

Al-Sadaqah campaign mentioned on Subsection 1.3 was connected to a Syrian-based exchange, BitcoinTransfer. Active since December 2018, it is believed to be controlled by terrorists. It handled more than $280,000 worth of bitcoin between December 2018 and July 2020 (Grauer *et al*, 2021). BitcoinTransfer is considered to have been a central hub for *inter alia* al-Ikwa and Reminders from Syria, demonstrating an al-Qaeda effort to "centraliz[e] the communication and the donations" (Barone, 2020).

[29] Available at https://krypt3ia.files.wordpress.com/2018/08/screenshot-from-2018-08-27-08-57-31.png, accessed on 15.12.2020.

3.4. Legal assessment on the terrorism financing nature

Following the previous analysis, it is important to ask whether those cases constitute or not TF[30]. Prior to this, it is important to determine whether the individuals or organisations involved in those cases are classified as terrorists. The United Nations[31] and the EU[32] designed their own lists of groups, persons or entities involved in terrorism. The groups and individuals identified in the previous subsections supported ISIS and al-Qaeda, which are terrorist organisations. Hamas is also considered a terrorist organisation under EU criteria after Court of Justice of the European Union (CJEU) confirmation (Hamas/ Council of the European Union; Council of the EU, 2015). In addition, the analysis needs to focus on the content of the following terms: (1) providing/collecting; (2) funds; (3) by any means; (4) (in)directly; (5) intention and knowledge; (6) use of funds; and (7) ignorance of specific actions covered by funds.

Art. 11 is intended to cover both *actus reus* of financing*:* providing (donating) or collecting (fundraising) funds.

The reference to “assets of every kind” (Art. 2[1]) seems to introduce an extensive interpretation of the notion of funds, which is followed by an exemplificative typology of it.

The “by any means” sieve was included to encompass any tools to which terrorists and their supporters resort to when collecting/providing funds. It includes the use of the Internet and social media (Recital 6).

The “directly or indirectly” concept is intended to cover not only the direct financer, but also intermediaries (Recital 15).

The next task is that of proving *mens rea*, *ie* the mental element. The *mens rea* element varies across national jurisdictions. The EU legislator requires “intention” and “knowledge”; *ie* a person cannot be convicted for having committed TF by negligent or reckless behaviour. *Mens rea* entails the intentional act of providing or collecting funds and that those funds are to be used “with a specific terrorist aim” as

[30] The provisions and recitals mentioned on this subsection pertain to Directive (EU) 2017/541.
[31] Cf. https://scsanctions.un.org/7kpuben-all.html, accessed on 23.07.2021.
[32] Cf. Council Decision (CFSP) 2021/1192 of 19 July 2021.

the actions listed on Art. 3(2) (Recital 8). In other words, the mental element entails both willful or deliberate actions as well as intention and knowledge that funds will finance terrorist acts. Intention requires not only an individual to know that is helping terrorists but also that such act represents the agent's will to do so (IMF, 2003). As such, Recital 17 clarifies that intention must be inferred from "objective, factual circumstances".

Art. 11 does not require all the funds to be used for the act to constitute TF. Part of the amount might be used for other legitimate economic purposes (FATF, 2016). In addition, funds do not need to be actually used when intended to cover the actions codified in Arts. 3, 4 and 9 (Art. 11[2]). The EU legislator plan was to criminalise TF even in absence of a connection to a specific terror act (EC, 2015). TF is characterized by the likely absence of a principal offence – the terrorist act – as funds might be used for basic maintenance or the terror act is not yet attempted (Koh, 2006). As such, the mere intention and knowledge that funds are destinated to fund terrorism is sufficient, even if no concrete link to a specific act exists or even if funds are not delivered to an actual terrorist organisation or terrorist. It constitutes the criminalisation of the mere conscience of the danger (Figueiredo, 2018).

In addition, contributors do not need to know which specific offence(s) will be covered when contributing to the actions codified in Arts. 3, 4 and 9 (Art. 11[2]) – despite the dissident opinion that the intention concept shall be interpreted narrowly as a "specific intent to contribute […] to the commission of the principal offence of terrorism" (Duffy *et al*, 2020, p. 34).

Following this analysis, it is important to determine whether the fundraising campaigns presented on this section fulfill the TF mental and material criteria.

Providing or collecting. Whereas ITMC, Akhbar al-Muslimin, AQB and al-Ikhwa were unlawfully collecting funds, Zoobia Shahnaz and Jonathan Xie were donating to terror causes. Therefore, both providing and collecting actions were present on the cases analysed in the present section.

Funds. Another important question is to assess whether CCs fill the legal definition of "funds" provided on Art. 2(1). In addition to be considered as "assets of every kind", CCs fulfill the notions of intangibility and mobility. It was the EU legislator

intention to punish supplying terrorism not only with money, but with assets of all kind. Therefore, the “funds” criterion is fulfilled.

By any means. Internet, social media, official websites and messaging applications were the tools deployed in the cases presented in the previous subsections, fulfilling this criterion. Recourse to wallets service providers to conduct such financing also meets this criterion.

Directly or indirectly. The *hawaladars* that AQB urged its sympathizers to resort to as well as the BitcoinTransfer exchange – which is believed to be a vehicle owned and used by terrorists and their supporters (Grauer *et al*, 2021; Barone, 2020) – are captured by this criterion. Zoobia Shahnaz also resorted to intermediaries when sending funds to shell-companies. All the other cases involved direct support of terrorism.

Intention and knowledge. ITMC CC fundraising campaign is the most explicit as to its TF intent by operating under the slogan “from you money and from us our blood” and by posting videos demonstrating its fighters’ skills. AQB is also clear as to its purposes by acting under the slogan “Support the Resistance”. When it comes to SadaqaCoins, TF intention is demonstrated by the call for monero donations to acquire sniper rifles and jeeps. What these cases have in common, and strengths the argument that TF schemes are in place, is the fact that both ITMC and AQB’s *modus operandi* included insistence and layering moments. ITMC presented bitcoin as a secure instrument and transferred CCs to overt addresses and reiterated its intent by constantly countering the fact that Twitter was shutting down its webpage. AQB was the most artful by sending private messages to financiers and by instructing them how to conceal their transactions urging disintermediation, employing a one-donation-one-wallet scheme and guiding donors through the combined use of *hawala*, non-hosted wallets and public wi-fi. Akhbar al-Muslimin’s fundraising campaign is said to be implemented to collect funds to feed its website, although intelligence entities believe that it is intended to cover terror propaganda (MAITIC, 2017). In addition, the fact that its website was constantly being shut down, and a mirrored one being provided to sympathizers through private message is indicative of an intention to operate overtly and avoid detection, which demonstrates a clear knowledge on the TF nature by the participants. Art. 11 might impact

legitimate activities of the civil society, including the ones providing humanitarian assistance to local and most vulnerable communities which present a higher risk of defunding due to avoidance to interact with such jurisdictions (Duffy *et al*, 2020). Yet, the explicit terrorist intent of the "charity" presented in this section is undeniable and cannot be regarded as a legitimate activity of the civil society. Cross-checked information – such as advertisement by assumed terrorists and by terrorists claiming that such funds were needed to equip terrorists in Syria – revealed al-Ikhwa's terrorist goal. Presenting themselves as a charity is not an argument in itself. Similarly, al-Ikhwa presented CCs as untraceable tools and intended to erase the path leading to wallet addresses by scattering funds over several wallets. When it comes to Shanaz, the fact that funds were obtained illicitly, maybe through false administrative documents, is seen by the EU legislator as an intentional act to commit an offence related to terrorist activities, *in casu* TF (Arts. 12[c)]; 4[b)]). Moreover, Shahnaz sent the funds to shell enterprises located in China, Pakistan and Turkey, which demonstrates intention to overt funds. In turn, Xie donated and even provided guidance to a third person, an undercover agent, on how to donate to a terrorist organisation's cause. Xie's intention to assist terror was explicit if we cross-check this information, for instance, with his actions in December 2018. On that moment, Xie sent $100 to an individual he believed to be a member of AQB and bragged about it on Instagram: "[j]ust donated $100 to Hamas. Pretty sure it was illegal but I don't give a damn" (Shea, 2020).

(Actual) use of funds, in full or in part, to commit terrorist acts. This requirement is useful to analyse al-Ikwha campaign which claim to call for CCs to assist widows and orphans. As such, even if part of the collected funds is used to cover those expenses, it does not prevent it from being framed as TF as crossed information revealed the organisation was linked with clearly declared terrorist actors and was also procuring financing to acquire weapons. When it comes to actual use of funds, no specific information was found relating the analysed CC fundraising campaigns with accomplished attacks, but the EU legislator did not require actual use.

Ignorance of specific actions covered by funds. Terrorists most of the times explained which specific expenses they needed to be covered, whether specific

weaponry or its fighters' equipment. More evasive requests for donations involved asking support for the cause or the resistance (AQB). These specifications should be regarded as sufficient as requiring indication on which attack donations were intended to contribute and proving financiers' knowledge on that would be disproportional – something that is even considered abnormal in the context of operational confidentiality, as details are expected to be shared among a restricted number of people. It might also happen that donations are used to other purposes than the ones asked for – donations might be required to buy weaponry but end up being used to cover day-to-day expenses, or vice-versa.

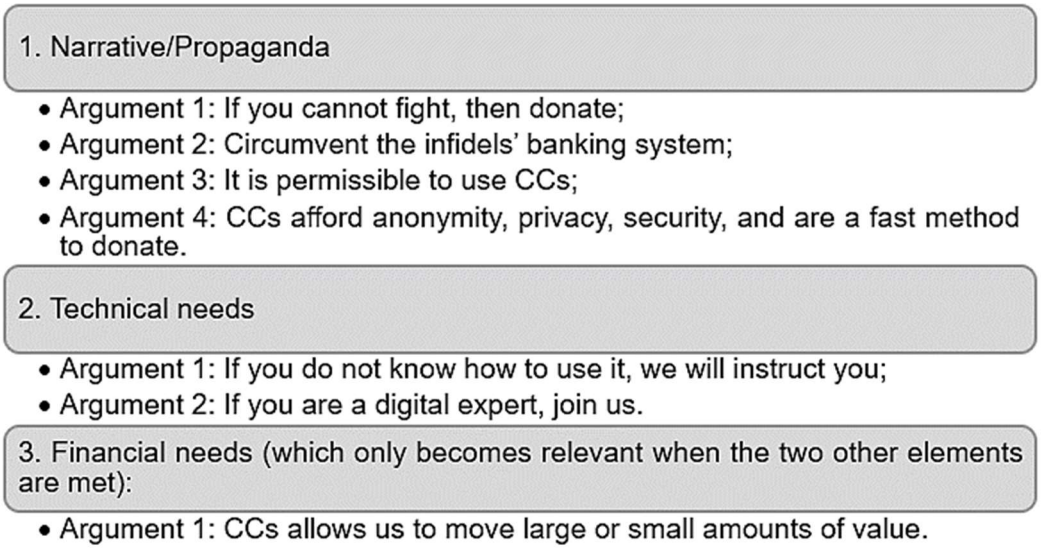
Therefore, the terror-CC stage presented in this section is caught by the EU counter terrorism law. Thus, not only the ones directing a terrorist group, but also the ones "funding its activities in any way" (Art. 4[a-b)]) may be punished as criminal offenders.

3.5. Intermediary conclusions

"Are terrorists and their supporters resorting to CCs? If so, how?".

Empirical evidence demonstrated that terrorists are resorting to CCs, rationalizing their use and explaining supporters their main features and advantages. Risk, simplicity, costs, and speed are the main features that terrorists consider when moving funds (Freeman *et al*, 2013). Terrorists strive for anonymity and security, perceiving CCs as a tool to enhance impunity (Eisermann, 2020; Kethineni *et al*, 2019). CCs' portability makes them a suitable "vehicle for global terrorist funding" (Brill *et al*, 2014, p. 8) *inter alia* between the members of a terrorist group (Keatinge *et al*, 2018). Therefore, terrorists' attitude towards CCs will, at different points in time, result from a continuous assessment and balancing of all variables (Brill *et al*, 2014). Considering the cases *sub judice*, terrorist use of CCs can be described according to three key elements:

Figure 1 – Main arguments presented to persuade supporters.



Based on Barone (2020)

Most terrorists asked for bitcoin; only Akhbar al-Muslimin and SadaqahCoins diversified its portfolio by requesting monero. In addition to social media and official websites, messaging applications such as Telegram and Threma were used as contact points between donors and fundraisers. Such encrypted messaging applications represent an additional level of anonymity and an emerging risk as applications are willing to incorporate CCs, totally shielding what is happening inside that atmosphere, allowing terrorists to "fundraise without disruption" (Poe *et al*,

2018; Keatinge *et al*, 2018). Hyperlinks and QR codes were implemented to direct donations, and multilingual webpages and explanatory videos were provided. Akhbar al-Muslimin and AQB stood out by designing a sophisticated method to generate unique wallet addresses for supporters to send their donations. Traceability becomes considerably difficult as no transaction related to such address was previously recorded, not existing available information on the concerned wallet. This scenario is of special concern and requires in-depth analysis as it turns financial investigations much more difficult to manage (Liv, 2019; Smith, 2019[a]). AQB went even further and added concealing layers. Although CCs might rapidly evolve to be a substitute of *hawala* (Barone, 2018b), especially as younger terrorists emerge (Harsono, 2020), it seems that *hawala* is, instead, complementing the terrorist abuse of CCs. Akhbar al-Muslimin directed donors to CSPs based in Europe, whilst AQB referred its donors to conduct P2P transfers, which might explain the 15,8% of P2P interactions. Although CSPs are collecting information on their customers, it is not enough as some wallet addresses were already acknowledged to be TF-related. Several exchanges are not yet registered, and a high fraction of ITMC's supporters relied on such unidentified services. AQB's donors not resorting to mixing services might be linked with the fact that they perceive that the one-use wallet address provided sufficient protection – which might also explain their recourse to registered exchanges. ITMC's bulk of donations came from mixers, which might demonstrate its donors higher CC knowledge. On AQB campaign, any mixing services were used, presumably because donors assumed that sufficient anonymity was already provided. Lastly, AQB's donors were more cautious with the donated amounts. The fundraise orchestrated by AQB is demonstrative of a highly dynamic and adapting behaviour and should raise concerns. Its efforts resulted in the collection of more than $10,000, being much more efficient when compared with ITMC's, as for nine months the previous group raised roughly the same amount as the second group did in two years – which might be related with increased anonymity perceptions (Chainalysis, 2020) (cf. Figure 19).

Façade humanitarian structures might be part of a bigger network. They might be operating as digital money mules, similarly to mixing services (Barone, 2019), hiding wealthier transactions, and thus facilitating TF.

Overall, terrorists are already demonstrating a high-level and dynamic pool of technological skills. TF is difficult to detect due to the fragmented nature of terror organisations and individuals, which is exacerbated by their shift to the informal financial system (Tierney, 2017). Hence, it is important to consider how to tackle CC abuse by terrorists, namely through Directive (EU) 2018/843.

IV. DIRECTIVE (EU) 2018/843: THE EU RESPONSE TO CRYPTOCURRENCIES AND TERRORISM FINANCING. LEGAL (UN)CERTAINTY, LOOPHOLES, AND CHILLING EFFECT?

The 4AMLD was not transposed by all the Member States (MSs), when the European Commission (EC, 2016[a]) communicated an action plan to strengthen the fight against TF making clear its intention to amend the regulatory framework to address *inter alia* the risks associated with CCs. Regulation in this field was deemed urgent as Europe was experiencing high levels of bitcoin-related ML (Keatinge *et al*, 2018). On July 5, 2016, the EC (2016[b]) presented a proposal to amend the 4AMLD. It was deemed unjustifiable that "[c]ertain modern technology services (…) remain[ed] outside the scope of Union law or [was] benefit[ing] from exemptions from legal requirements" (Recital 2). The Directive (EU) 2018/843 (5AMLD) establishes minimum standards that its addressees must comply with (Art. 5). Its main goal is to continue the legacy of the 4AMLD by identifying, understanding and mitigating ML and TF risks (Recital 1), while addressing novel actors: CSPs. The 5AMLD shall have been transposed until January 10, 2020. However, only 19 MSs, including Portugal, have transposed it so far[33].

The 5AMLD was adopted to absorb and update the EU framework to FATF standards as well (EC, 2021[a]). It was after the Silk Road and Liberty Reserve[34] cases that FAFT (2014) firstly addressed CCs, recognizing LEAs' increasing concern on their abuse for terrorist purposes (FATF, 2015). FATF (2019) amended its Recommendation 15 to bring CSPs into a gatekeeper approach, adding "virtual asset" and "virtual asset service provider" definitions to its glossary. According to FATF (2019), virtual asset service providers include (1) crypto-to-fiat and (2) crypto-to-crypto exchanges, (3) transfer of CCs, (4) safekeeping and/or administrating CCs or instruments that enable their control, and (5) ICOs' issuers[35]. FATF's legitimacy as an AML/CTF bastion and its democratic nature are highly disputed. It is an

[33] Austria, Bulgaria, Croatia, Denmark, Estonia, Finland, France, Germany, Greece, Italy, Latvia, Lithuania, Luxembourg, Malta, Portugal, Romania, Slovakia, Slovenia, and Sweden. More information on transposition status available at https://ec.europa.eu/info/publications/anti-money-laundering-directive-5-transposition-status_en, accessed on 05.05.2021.

[34] Liberty Reserve was an exchange which facilitated ML and was shut down in May 2013 by US authorities. *Op. cit.* footnote 11.

[35] For the purposes of the present dissertation, only activities (1) to (4) will be considered as no relevant empirical evidence was found on ICOs being abused by terrorists.

international inter-governmental structure, which started to set the rules for anti-money laundering (AML), and whose mission evolved to accommodate TF and the financing of proliferation of weapons of mass destruction risks (FATF, 2015). The EC and 14 EU MSs are members of it (EC, 2020[b]). FATF anchors its action on soft law instruments, being vested under informal authority to build global consensus on these matters (Turner, 2015). Votes are of a symbolic nature with decision-making being achieved on a consensual basis (Nance, 2017). FATF is seen as an organisation that inevitably reflects geopolitical power asymmetries. It is regarded as an extension of US and/or EU preferences (Nance, 2017). The US-EU predominance is such that it is reflected on FATF recommendations that are flexible enough to accommodate the points that raise discussion between the two titans (Drezner *apud* Nance, 2017). However, FATF tremendously reflects an alignment with the US, especially following the 9/11 events (Turner, 2015). FATF's "peer-based diagnostic" (Pavlidis, 2020) is perceived as an instrument to eliminate competition between states (Sharman *apud* Nance, 2017). In addition to FATF's monitoring powers (the on-site mutual evaluations on states willing to comply with international standards), such diagnostic scheme has a two-fold design: jurisdictions under increased monitoring by FATF and committed to solve identified inconsistencies are included on its "grey" list (FATF, 2021[c]); the "black" list identifies high-risk jurisdictions, *ie* jurisdictions with significant AML/CTF and financing of proliferation of weapons of mass destruction deficiencies and which are not committed to solve it (FATF, 2021[d]). Despite reluctances towards FATF's legitimacy, the acceptance of its standards may reflect the support of International Monetary Fund (IMF) and World Bank (Nanyun *et al*, 2020).

4.1. EU regulatory framework main actors

a) Cryptocurrency Service Providers

Art. 2(1)(3) of the 4AMLD was amended through the introduction of points g) and h) to include: (1) exchanges, which are defined as "providers engaged in exchange services between virtual currencies and fiat currencies" (crypto-to-fiat exchanges); and (2) custodian wallet providers, *ie* "services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies" (Art. 3[19]).

CSPs were considered to represent interconnection points which could be supervised and pushed into more transparency (Keatinge *et al*, 2018). Thus, they are addressed with general legal duties of registration, identification and CDD, monitorization, report and refusal to conduct transactions, record-keeping, cooperation, control, formation and training.

Registration. CSPs must be registered (Art. 47[1]). However, registration requirements' strictness (*ie* registration as financial institutions, non-financial business or other distinct category) may vary across jurisdictions (Pavlidis, 2020). FATF – whilst also establishing the possibility of licensing – determines that registration should occur at least in the jurisdiction within CSPs are created or where business is conducted, in case of natural persons. Host jurisdictions might also require registration and/or licensing (FATF, 2019). However, sometimes it is challenging to identify CSPs' jurisdiction as frequently they deliberately obscure it to avoid obey legal requirements despite obviously serving a jurisdiction customer. For instance, the fact that a CSP had a website in Russian, promoted rubles-to-bitcoin exchange and interacted with Russian banks was not sufficient for CipherTrace researchers to find clear legal connections and attribute this CSP to the Russian jurisdiction (CipherTrace, 2020[a], p. 13).

Identification and CDD. CDD is an extremely important process intended to sufficiently understand customers and the risks they might originate, especially as face-to-face contact is not the rule in the CC environment. Collected data might be resumed to e-mail addresses or mobile phone numbers, and real-world identity might not be corroborated (Brill *et al*, 2014). CSPs must confirm their customers' identity, preventing nefarious actors from infiltrating into the system through fake identities. As such, CDD mechanisms will be activated prior to the establishment of the business relationship or occasional transaction (Art. 14[1]) when (Art. 11[a-b]):

(1) A *business relationship* is established. It amounts to the opening and maintenance of an account (FATF, 2019) which is expected to last in time (Art. 3[13]); or
(2) An *occasional transaction* takes place, which the Union legislator handled with caution by establishing *de minimis* thresholds. Thus, identification and CDD will be applied on transactions of at least:

- €15,000, measured on a single or cumulative basis to prevent threshold circumvention. The cumulative amount will be assessed where several transactions seem to be connected; or
- €1,000, when there is a transfer of funds "which are sent or received by a payment service provider or an intermediary payment service provider established in the Union" (Art. 2[1] Regulation (EU) 2015/847).

Art. 11 reflects the lack of clarity that permeates the 5AMLD. The European Baking Authority (EBA) stressed the importance to provide further guidance on *occasional* and *linked* transactions (EC, 2021[a]). Considering the business relationship criterion, occasional transactions constitute, *a contrario,* sporadic transactions – no account is opened or maintained (FATF, 2019). In turn, it might be difficult to practically determine, specifically on the CC setting, what transactions *which appear to be linked* or *seem to be connected* are, as the linking criterion might be missing. As demonstrated in the case of unique wallet address generation schemes deployed by Akhbar al-Muslimin and AQB, each contributor might conduct several *de minimis* operations linked to different wallet destination addresses. AQB's financiers were provided with guidance on how to further conceal their identity, hampering such linking criterion as well. EBA considers that it is necessary to provide for a single CDD threshold for occasional transactions due to the regulatory arbitrage problem (EC, 2021[a]). FATF (2019) even encourages states not to apply a threshold at all. France intends to follow such approach (CipherTrace, 2021)[36]. In the previous analysis, it was shown that just a few donations involved large sums of money. Therefore, the anonymity permitted under such thresholds is a concern. Below both thresholds, CDD will only be activated if a TF suspicion exists, or where the veracity or adequacy of the previously provided data raises doubts (Art. 11[e-f]). When assessing TF risks, CSPs must evaluate, at least, the purpose of the account or relationship; the volume of assets to be deposited or the size of the transactions; and the consistency or duration of the business relationship (Annex I *ex vi* Art. 13[3]).

Lack of interplay between sectoral legislation such as AML/CTF rules and Regulation (EU) 2015/847, has a result that the €1,000 threshold – the "travel rule" – does not apply to CC transactions, as the Regulation (EU) 2015/847 does not

[36] Compliance costs will increase from €1 to €5 (CipherTrace, 2021).

consider CCs as funds. Under the “travel rule”, CSPs would need to gather their customers’ and counterparties’ information when cross-border operations take place (EC, 2021[a]). Nevertheless, where a customer makes transactions with a non-custodian wallet counterparty, it remains questionable whether CSPs will be able to comply with CDD rules when the counterparty wallet does not hold such information.

Customers shall be allowed to provide information on a voluntary basis, which is advised to CC users resorting to unregulated services as well (Recital 9). For users resorting to regulated gatekeepers, it might not be an issue. However, in other cases of users, whether legitimate or criminals, it is unlikely that they will provide such information (Houben *et al*, 2021). Still, CSPs must collect the following elements:

(i) Customers’ – and, where applicable, the customer’s beneficial owners’ (BO) – documents, data or information, from reliable and independent sources (Art. 13[1][a-b]);
(ii) The purpose and nature of the business relationship (Art. 13[1][c)]).

In addition to government-issued identification, e-mail, phone number and physical address (CipherTrace, 2020[a]), other customer data might include public keys, addresses or accounts involved, time-stamped IP addresses, geo-localization, device identifiers, wallet addresses and transaction hashes (FATF, 2021[a]). Such elements shall also be assessed from “any person purporting to act on behalf of the customer” as well (Art. 13[1][§2]). CDD information must be kept in a system that allows CSPs to effectively and securely reply to Financial Intelligence Units (FIUs) requests (Art. 42).

CSPs must evaluate their upcoming and current customers’ risks, including when a customer’s relevant circumstances change (Art. 14[5]). Risk assessments are needed to determine the depth that must be given to the CDD process.

In addition to the “regular” CDD process, the 5AMLD prescribes simplified (SDD) and enhanced due diligence procedures (EDD):

CDD must be (1) lessened when, *after proper evaluation*, lower risk geographical areas customers, products, services, transactions, delivery channels or lower state specific AML/CTF risk factors are in place (Art. 15[1-2]; Annex II *ex vi* Art. 16); or (2) enhanced, *mandatorily*, in the cases described in Arts. 18 to 24, being relevant for

the theme under analysis: (a) when a TF risk exists (Art. 18[3]). It includes business relationships being conducted in unusual circumstances, customers being resident in HRTCs, as well as risks related to product, service, or delivery channels (Annex III *ex vi* Art. 18[3]); (b) when HRTCs are involved (Art. 18a). Only when EDD measures are implemented can a CSP interact with HRTCs' CSPs (Recital 12). EDD measures include obtaining (1) additional information on the customer and BO, (2) namely their source of funds and wealth, (3) on the intended business relationship nature, (4) the transactions rationale, and (5) senior management approval to establish or continue the business relationship (Art.18a[1][a-e]). In addition, EDD must comprise measures to mitigate risks such as tracing customer's IP address and cross-check information available on the Internet to assess whether customer's activity information is consistent with the transaction profile (FATF, 2019). The use of analysis tools such as blockchain analytics can be added to this EDD scheme (FATF, 2021[a]). Customers must, however, be informed on the type of CDD that is going to be conducted (European Data Protection Supervisor – EDPS, 2020) – whether "regular", SDD or EDD. The cases set down in the 5AMLD are not of an exhaustive nature. EDD can be applied "in other cases of higher risk" identified by MSs and CSPs (Art. 18[1]), namely to complex, unusually large, with unusual patterns, or without an apparent economic or lawful purpose transactions (Art. 18[2]).

Already in 2016, the EC recognized the need to provide for concrete EDD measures, as the 4AMLD was already presenting vagueness problems on this topic (EC, 2016[a]). The EBA urges the EU legislator to provide clearer criteria for the 5AMLD' addressees as well, to help them to determine which CDD measures are commensurate with different risks. In fact, the lack of such connection leads MSs and obliged entities to implement diverging measures to the same risks (EC, 2021).

Monitorization. Customers and business relationships should be monitored on a regular basis to continuously diagnose potential risks and guarantee that the initial CDD process was properly conducted (Recital 24; Art. 13[1][d]). CSPs should categorize customers according to a holistic view of the data collected, at customer or cluster level, and monitor eventual deviations (FAFT, 2019). Where a customer is attributed a lower risk, it does not prevent CSPs from maintaining monitorization

(Art. 15[3]). Tight monitoring must occur as well when customers are originated from HRTCs by increasing its frequency and pinpointing transactions that, by its patterns, require more focus (Art. 18a[1][f]).

Report. Bringing CSPs into the specific obligation to report suspicious activity to FIUs by completing Suspicious Transaction Reports (STRs) is of utmost importance (Recital 8) and reflects an EC (2016[a]) concern to fill reporting gaps in this novel environment. The lack of such requirement played a central role in facilitating the illicit practice in the Liberty Reserve case (Salami, 2017). Europol is expected to play a pivotal role in sharing STRs, namely through FIU.net,[37] and coordinate investigations emerging from those files (Keatinge *et al*, 2018). In addition to not entering such business relationships or conclude such transactions, STRs must be filled when (1) CSPs cannot obtain customers' identification data or assess the purpose and nature of the business relationship (Art. 14[4]); or (2) a TF suspicion exists (Art. 33[1][a]). Yet, if transactions suspension "is likely to frustrate efforts to pursue the beneficiaries of a suspected operation" it can be completed and the STR must occur "immediately afterwards" (Art. 35[1-2]). STRs should not be disclosed to the concerned customers and their access to personal information must not be granted, to preserve the utility of such report (Art. 39[1]). Whereas STRs preventive nature cannot be neglected, data protection issues arise (cf. Subsection 5.5).

Control and Record-keeping. CSPs are required to, according to their organisation size, implement appropriate policies, procedures, and controls to identify, understand, manage and mitigate risks, and implement regular risk assessments (Art. 8[1; 3]). The appropriate and proportional steps to identify and grasp TF risks includes CDD, risk management models, reporting mechanisms, internal controls, compliance management, and an independent audit function where necessary (Art. 8[4]). This assessment shall be documented, updated, and made available to national competent authorities (NCAs) and self-regulatory entities (Art. 8[2]). Data is to be retained for a 5-year period after the conclusion of the business relationship or after the occasional transaction, and an additional 5-year

[37] It is "a decentralized intelligence platform that enables Member State FIUs to share and exchange information on STRs generated within their borders" (Keatinge *et al*, 2018, p. 59).

period must never be exceeded. When the 5 or 10-year period reaches its end, data shall be deleted unless otherwise provided by MSs' national law (Art. 40[1]). The data retention period provided by the 5AMLD also poses data protection challenges (cf. Subsection 5.5).

Suitability, formation, and check-balances. At an organisational level, risk is dealt with through three levels. CSPs' managers should be "fit and proper persons" (Art. 47[2]), while its employees must be provided with ongoing training to pinpoint money laundering and TF-related transactions and knowledge on data protection requirements (Art. 46[1]). An independent internal auditor might be employed where justified to test the fitness of internal policies, controls and procedures adopted by obliged entities to tackle identified risks (Art. 8[4][b]).

b) Financial Intelligence Units

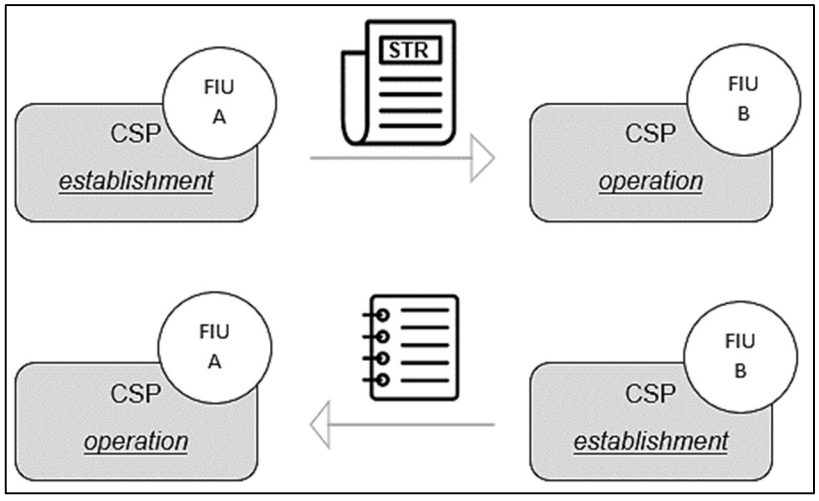
Financial Intelligence Units (FIUs) assist intelligence, investigative and judicial authorities to prevent, detect and tackle TF (Art. 32[1]) and are expected to play an important role in the CC legal vacuum (Recital 9). They are a bridging mechanism between the private and public sectors (Koh, 2006).

STRs analysis. FIUs filter *stricto sensu* financial information contained in the STRs (Art. 32[3]; Nunes, 2018), but their powers include obtaining (supplementary) information held by obliged entities as well, even if those entities do not report (Art. 32[3; 9]). Despite assigned with such role, EU FIUs are not afforded with sufficient budget and staff. In 2019 alone, each EU FIU received, on average, 50,000 STRs. The high volume of analysis to conduct and lack of personnel to do so hugely impacts these entities' capacity to interact and cooperate with other FIUs (EC, 2021). In turn, CSPs must receive feedback on the STRs they sent to FIUs (Art. 46[3]). However, they rarely receive feedback, especially when it concerns other MS. Few FIUs reported to provide for feedback mechanisms such as reports and guidelines, meetings with the stakeholders namely in the context of public-private partnerships (PPPs), and training (EC, 2019). The EDPS (2020, p. 14) contends that such lack of feedback on STRs is, however, "a safeguard for the privacy of individuals" (cf. Subsection 5.5). In addition, obliged entities tend not to use reporting templates (EC, 2020[a]). Even if they do, the common EU FIUs Platform template is not binding. As such, each entity uses its own, which impacts on the type and the

extent of the information gathered (EC, 2021[a]). Updates of this template might be necessary to accommodate CC-related indicators (e.g., IP addresses, timestamps, hashes, wallet addresses and device identifiers) (FATF, 2019).

Information exchange and Cooperation. One of 5AMLD's main goals is to enhance FIUs access to data (Andreeva, 2019). Proactively or upon request, in a timely manner and without impediments, these units must exchange information with each other. FIUs must pursue a model of maximum exchange of information, employing the whole spectrum of available means (Mouzakiti, 2020) – namely through cooperation with LEAs (Art. 53[1-2]; Recital 16). FIUs are now afforded with a pool of powers which might benefit other MSs' FIU. For instance, a FIU might contact a national bank to require a customer's data to answer another FIU's request. Hence, FIUs will have access to a greater amount of information at EU level (Mouzakiti, 2020). FIUs are obliged to promptly share data with an EU counterpart when they receive a STR concerning other MS (Art. 53[1][§3]). That requirement responds to the situations where an obliged entity is established in a MS and, according to the principle of territoriality, reports to that MS' FIU, despite conducting its activity across the EU. It represents a "'data sharing by default' attitude" (Mouzakiti, 2020, p. 358). Additional information exchange requests can be addressed to other MS' FIU when a CSP is operating on that territory but is established on the requested MS. Direct requests to the concerned CSP are not allowed (Art. 53[2][§2]). It shows that the EU legislator wanted to eliminate obstacles to information sharing as much as possible (Mouzakiti, 2020).

Figure 2 - FIUs' data sharing model.



Information requests should contain the pertinent facts, background data, motives underlying such requests and intended use on the information (Art. 53[1][§2]. FIUs can refuse information exchange requests when they are contrary to the "fundamental principles of its national law" – an exception that must be properly justified (Art. 53[3]). In principle, EU law and national constitutional rules on fundamental rights are compatible. However, when discrepancies exceptionally arise, the normal course of action is a preliminary reference to the CJEU (Dimitrakopoulos, s.d; Art. 19[3][b] Treaty on the European Union – TEU). After CJEU's reply, the national rules should be applied in accordance with the EU law as interpreted by the CJEU (Dimitrakopoulos, s.d.). Hence, the CJEU is entitled to carry out such interpretation role whilst ensuring "an ever-closer Union" (Boin *et al*, 2021, p. 136; Article 19[1] TEU).

Receiving FIUs, in turn, shall use the received information only for those identified purposes unless additional use is granted. Refusals on such approval must be justified to prevent unlawful refuse on information exchange (Art. 55).

The vagueness of the 5AMLD rules is reflected in different approaches to the conditions and the time limits to reply to information requests, which hampers FIUs cooperation. It remains unclear what "in a timely manner", "sufficiently defined conditions", "without impediments", "all available means" means. Replies to FIUs information requests on directed to obliged entities diverge from 5 to 20 business days. On the other hand, information exchange between FIUs occurs, on average, with hiatus of one month, which is a result of the EU law not imposing or specifying deadlines. As a result, some FIUs report much more than others (EC, 2021[a]).

FIUs are a vehicle for international cooperation (Recital 16). They must disseminate operational (specific targets) and strategic (TF trends and patterns) analysis results to other FIUs and NCAs, especially if it resulted in a TF suspicion (Arts. 32[3; 8]; Recital 18). Joint analysis between FIUs in cross-border cases should be enhanced through the EU FIUs' Platform (Art. 51). However, the EU legislator did not define what joint analysis is and how to conduct it (Mouzakiti, 2020). FIUs must resort to protected channels and embrace state-of-art technologies which promote security and interoperability (Art. 56[1-2]). They resort to different tools when reporting information to other FIUs, ranging from fax to AI-supported mechanisms, which

hinders cooperation in building joint cases (EC, 2021[a]). Moreover, FIU.net was deemed obsolete, urgently needing updates to expedite cooperation (EC, 2020[a]).

FIUs shall intensively cooperate irrespective of their organisational status (Art. 52). However, FIUs' organisational set-up underpins their access to information. There are administrative-, law-enforcement-, judicial-, and hybrid-type FIUs, depending on states' options. If FIUs are established as administrative entities, their powers are very limited: they only receive and analyse STRs filled by private entities and disclosure of such confidential information is restricted to LEAs; they experience a delay in law enforcement measures (e.g., freezing and arresting) and in obtaining evidence, as this requires judicial authorisation. Law enforcement-type FIUs also present disadvantages: access to obliged entities' data might require the opening of a formal investigation and they might be reluctant to share such information; in addition to the same difficulties as law enforcement-type, judicial-type FIUs information exchange with non-judicial FIUs is problematic, as they have different powers to obtain evidence or access information (IMF, 2004). Therefore, the diverging powers and rights to access to and exchange of information by FIUs results in inefficient outcomes hampering its direct and swiftly access to information. As such, minimum common rules on its functions and powers are required (EC, 2021[a]). It must be stressed that information sharing between FIUs with different status pose data protection issues as well (cf. Subsection 5.5).

The alignment of rules on access to information with the international practice is important, namely the elimination of the requirement of a prior STR that exists in some MSs. There is a need to evolve from a suspicious to an intelligence-based disclosure system (EC, 2016[a]), as FIUs' course of action is guided also by its own analysis and data provided by other NCAs and FIUs (Recital 17). Hence, such intelligence-based scheme entails enhanced cooperation among NCAs (Art. 49). However, it also poses privacy and data protection concerns as FIUs will be granted with mass access to information as the prior STR obstacle is dismantled (cf. Subsection 5.5).

Cooperation between FIUs – as well as with HRTCs' – must not be hindered by differences between national law definitions of predicate offences (Art. 57). These differences inevitably pose practical obstacles on cross-border cooperation (Recital

18). FIUs requested to cooperate usually require the predicate offence to constitute a crime in their jurisdiction as well. It might create a regulatory arbitrage effect, *ie* criminals will explore jurisdictions that do not criminalise such offences. EU legislation tends to present lists of predicate offences, but sometimes it merely refers to international standards or other EU legislative acts. The actual content of such offences is not defined, leaving broad margin for MSs adopt their own strategies (EC, 2016[c]). For instance, the 5AMLD lists tax offences as predicate offences; however, no harmonised definition of tax crimes exists at EU level (Mitsilegas *et al*, 2016). Furthermore, Art. 3(4)(f) establishes that tax offences will be considered as (serious) predicate offences where its maximum and minimum deprivation of freedom or detention penalties are of at least two years and six months, respectively, which represents an additional alignment layer for MSs. It results in discrepancies across the EU (EC, 2016[c]). Therefore, a standard categorization of predicate offences and harmonising its definitions throughout the EU to enhance cooperation and to avoid jurisdictions cherry-picking is required (EC, 2016[c]). Satzger (2019, p. 118) proposes a system of "relative comparability": while it is for the EU legislator to draft the "nucleus of an EU sanctioning system" and attribute common severity levels for each crime, MSs assign a specific sanction according to that severity level and their own legal system (Satzger, 2019). Such system would allow harmonisation whilst recognizing MSs' sovereignty at least at some extent.

Suspend transactions. FIUs are allowed to take urgent actions where a TF suspicion exists, suspending or withholding consent to the transaction to analyse it, confirm suspicions and report them to competent authorities. These actions can be required by other MSs' FIU "for the periods and under the conditions specified in the national law" of the requested FIU (Art. 32[7]). However, FIUs lack the capacity to suspend transactions as the 5AMLD abstraction is manifested in the conditions and the time limits to suspend such operations (EC, 2021[a]).

Therefore, the use of indetermined concepts, despite allowing flexibility to MSs, brings along a lot of uncertainty. Concepts such as "promptly" were identified as being difficult to concretize in practice (EU FIU Platform, 2017). Those broad concepts increase the difficulties inherent to the nature of the FIUs' tasks. Contrary to ML, in which a *post-facto* analysis is conducted, in TF the analysis entails anticipating whether funds will be delivered to terrorists. This kind of futuristic or *ex*

ante evaluation becomes more difficult by the fact that funds might have a legitime source (Nunes, 2018).

c) Supervisors

Supervision. Supervisors must monitor and take the necessary measures to ensure that the 5AMLD's requirements are met, through the necessary supervisory and investigatory powers and resources (Arts. 48[1-2]; 58[4]). Globally, countries are considered to perform poor AML/CTF supervision, due to limited or different powers to apply administrative sanctions, limited resources, non-application of the risk-based approach (RBA) (cf. Subsection 4.5), poor coordination, and insufficient guidance (Basel Institute on Governance, 2020). In the EU, such shortcomings are related with the fact that supervision is operated at MS-level, individually, with various stages of quality and effectiveness due to different available resources, and different agendas as well (EC, 2020[a]). Human resources indeed diverge substantially – e.g., the Finnish supervisor is equipped with 10 people, whilst the Austrian one with 27. It is estimated that the German supervisor has 15 people assigned to the non-financial sector, which entails the monitorization of around 1 million entities (EC, 2021[a]). It is reported that non-financial entities are in fact inadequately supervised (EC, 2020[a]). Such problems are exacerbated by the CC setting. The supervised population sample is difficult to predict due to the novelty of the sector and due to its global nature (FATF, 2021[b]). Hence, the EU experiences both national and cross-border inadequate supervision (EC, 2021[a]).

Enforcement. "[E]ffective, proportionate and dissuasive" sanctions (Art. 58[1]) should be applied, at least, to breaches on CDD, STR, record-keeping and internal controls (Art. 59[1]). The 5AMLD provides for administrative sanctions on CSPs: public statements, orders to cease the conduct, withdrawal or suspension of licenses and temporary bans (Art. 59[2][a-d]). Pecuniary sanctions comprise, at least (1) twice the amount of the breach's benefit; or (2) €1,000,000 (Art. 59[2][e]). The application of such sanctions takes into consideration the severity and the duration of the conduct, the responsibility level of the natural persons involved, the financial strength of the entities involved (e.g., annual turnover), the benefits derived from the conduct, determinable losses to third parties, cooperation level, and incidence (Art. 60[4]). Pecuniary sanctions can be imposed on natural persons as

well: managers; companies' representatives, who takes decisions or have control on its course; and supervisors or persons that occupy leading positions (Arts. 58[3]; 60[5]).

Other problems also arise from the 5AMLD's lack of clear and consistent rules. This blurriness leads to diverging sanctions being applied to similar infringements. The EBA stresses the importance of clarifying what constitutes a serious breach and to provide clear guidance on sanctions to be applied. For instance, whilst the Italian financial supervisory may apply a €5 million pecuniary sanction on a natural person, the sanctions applied in Estonia are deemed too low (EC, 2021[a]). In turn, the European Parliament (EP) urges the EC to better harmonise sanctions. In this way, sanctions will be better aligned across the EU, contributing to the effectiveness and the deterrence effect of the AML/CTF rules (Ferber *et al*, 2020).

MSs can also impose criminal sanctions and may, in such a case, decide not to impose administrative sanctions (Art. 58[2]). This means that an administrative, criminal or administrative and criminal sanctions scheme is allowed (Mitsilegas *et al*, 2016), as MSs are sovereign as to the sanctions applied, particularly criminal ones, which will produce a sanctions puzzle across the EU. Thus, harmonisation in this regard is required to ensure the effectiveness of the EU law (Mitsilegas *et al*, 2016).

4.2. Regulating gatekeepers and gate circumvention

A substantial part of the CC environment escapes the EU regulatory scope as users can interact directly whilst remaining anonymous (Recital 9). There are entities not covered by the 5AMLD which presents TF risks. In addition, several features of this ecosystem are challenging investigations: AECs, mixing features, poor CDD measures, nested services,[38] clandestine trading, DEXs (Europol, 2020[a]), and blockchain protocols (Chainalysis, 2020; Paesano, 2019). Despite the EU followed an approach not fully consistent with international standards, CSPs activities must be analysed in the light of the principles of (1) technology-neutrality and future-proofing, *ie* law must be sufficiently flexible to be applied to existing and emerging technologies, despite the technological platform involved and without

[38] An exchange incorporated within a wallet (Europol, 2020a).

entailing new revisions; and (2) conducted activity (FATF, 2019), considering the functionalities already described above – (1) to (4) – and that are relevant to the present analysis.

Crypto-to-crypto exchange, AECs and BTMs. Despite exchanging certain CCs for fiat frequently requires first obtaining bitcoin, which might reduce altcoins' privacy benefits, crypto-to-crypto exchange regulation is a priority. Such unregulated space creates an incentive to conduct CC swaps on conversion points with poor or inexistent CDD (Keatinge *et al*, 2018). The rationale behind the legislative option to only cover crypto-to-fiat exchanges derives from the fact that it was considered the most reliable method to introduce obstacles for terrorists (EC, 2016[b]) and that CCs risks only arise when they attain a status of value which can be used (Salami, 2017). However, CCs value is not limited to their convertibility to fiat. They are accepted in several e-commerce shops and, most problematically, on Dark Web marketplaces. Therefore, CCs risks do not solely arise from their withdrawing.

AECs exacerbate the issues arising from the crypto-to-crypto exchange non-regulation, and an increase in its use has been registered (Europol, 2020[a]). CSPs are prone to abuse precisely due to the possibility of conversion to AECs (Kfir, 2020). The act of publicizing wallet addresses online and pleading for donations hampers CCs underlying anonymity as the wallet address is going to relate to a specific entity (Koerhuis *et al*, 2020). AECs do not provide for the same level of transaction details (e.g., sender, receiver, amount). Monero has a one-time use address feature. This disposable address is what prevents deanonymization from happening as the address is only known by sender and receiver and is only going to be published on blockchain once (Koerhuis *et al*, 2020). Merging this feature with the one-transaction-one-*receiving* wallet presented on Akhbar al-Muslimin and AQB's cases is of concern. The dreadful scenario in which one transaction corresponds to both different sending and receiving addresses might happen. Users can conduct several *de minimis* transactions, avoiding CDD thresholds, and hamper the "which appear to be linked" requirement established on Art. 11 as many different addresses will be involved in the same transactional relationship. According to Adelstein (2018), the Japanese financial regulator's approach was to consider prohibiting exchanges from using AECs. Yet, AECs that technically allow for

information to be disclosed, might allow CSPs to comply with regulation (Shin, 2020). If CSPs include AECs on their portfolios, CDD will have to be nonetheless conducted; thus, such a built-in feature will be important for compliance purposes, although customer data might not be visible on blockchain. Yet, if blockchain public available data might be the starting point of investigations, such opt-in-opt-out feature will hamper LEAs and FIUs opportunity to pinpoint suspicious activity.

BTMs are exponentially growing, surpassing 21,000 in 2021[39]. It is often perceived as a tool to privately obtain and sell CCs (Europol, 2020[a]). Irwin *et al* (2016) even suggest that terrorists can acquire their own BTMs – for an amount that ranges from $6,500 to $12,000 – and apply their own AML/CTF controls and implement cherry-picking STRs. Keatinge *et al* (2018) called for clarification on BTMs legal status to avoid practical inconsistencies across MSs. Despite existing doubts, it may be concluded that BTMs will be caught under the EU piece of legislation, as long as it involves crypto-to-fiat exchange because it is, in essence, an exchange service. FATF (2019) states that where a jurisdiction considers the use of BTMs to entail an occasional transaction – as a customer resorting to an exchange service might be deemed as a one-off transaction – the €1,000 threshold shall be applicable.

P2P interactions. Although the EC (2016[a]) was reluctant to address wallet service providers, it was included on Art. 2(1)(3)(h). If at least one of the parties in the transaction resorts to an intermediary – a custodian wallet – such transaction will fall into the 5AMLD's scope, but only regarding the obliged entity. *Stricto sensu* P2P transactions (*ie* when both CC users transact directly through non-custodial wallets) remain, however, non-regulated.

For CC transactions to be caught under the law, *custody* and *transfer* activities must be present for a wallet service provider to be considered as an obliged entity. Custodians are services that provide private keys safekeeping *inter alia* to transfer CCs (Art. 3[19]). It entails retaining access to customers' private keys, whereas "transfer means to 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" (FATF, 2021[a], p. 18). FATF constantly refers to "custodians" and expressly states

[39] Available at https://coinatmradar.com/charts/geo-distribution/, accessed on 07.06.2021.

that it does not want to regulate non-custodian service providers. Through its revised guidelines (FATF, 2021ª), which is under public consultation, FATF eliminated some expressions that could lead to misunderstandings as to the custodianship concept it provided in its previous guidance (2019). There, FATF resorted to expressions such as "*a certain level* of […] 'control' of the virtual asset, or 'ability to actively facilitate the financial activity'" which seemed to eliminate the necessity of wallet providers' exclusive control over CCs (FATF, 2019, p. 14; added emphasis). That could lead to the interpretation that non-custodianship service providers were covered by FATF standards of conduct. FATF (2021ª), however, did not want to cover ancillary or facilitation services that provide transfer-only tools. Houben *et al* (2021) argue that, although the EU legislator must broaden 5AMLD's scope, non-custodian services should not be included as they typically do not act as intermediary services but only provide technical tools that assist users. Reflection on cold (non-custodian) wallets is needed as well. P2P interaction might occur through the recourse to such physical devices. For instance, terrorists may request donors to send these cold wallets via posting (Whyte, 2019). Only the CCs' holder personal information entered the regulated space; CCs' ownership changes, but information on the final recipient is not available. CCs' portable nature allows terrorists to travel with USB flash drives containing thousands of euros. In such a case, a comparison with cash declaration makes sense as CCs provide as much anonymity as cash.

As crypto-to-fiat exchanges are captured by the 5AMLD, new forms to exchange CCs are arising to preserve the libertarian *ethos* inherent to Bitcoin and altcoins. DEXs are part of the DeFi (Decentralized Finance) environment and lay on the perception that centralized exchanges present disadvantages. DEXs came to offer "theoretically complete anonymity and, crucially, non-custodian transactions", and this crypto-sector is expected to be expanded[40]. This kind of platforms claims to "*never take possession of a user's funds*, and instead simply route them between users' wallets based on the conditions outlined in the underlying smart contracts *without human intervention*", two characteristics leading many to believe that it is

[40] *Ult. op. cit.* footnote 1, accessed on 05.01.2021. E.g., CryptoBridge, Bitshares and Bitsquare (Keatinge *et al*, 2018).

not subject to regulation (Grauer *et al*, 2021, p. 108; added emphasis)[41]. In the light of EU law, DEXs must be considered, indeed, as exchanges. In essence, it entails an exchange of CCs service. As clarified by FATF (2019), CSPs' analysis shall be conducted irrespective of its underlying technology; the smart contract element is irrelevant. FATF (2021[a]) furthermore states that the control element is only required when a custodian wallet service is in place, which is not the case.

There are other DeFi-type P2P networks which are, nonetheless, a more rudimental way to by-pass exchanges (Keatinge *et al*, 2018). Localbitcoins.com kind of services make it possible for users to find others who want to exchange directly. By 2017, only usernames and e-mails addresses were collected from localbitcoins.com's customers, and this platform even permitted in-person CC exchange against cash (MAITIC, 2019[b]). Such feature is no longer available on the website due to efforts to meet regulatory standards (Langridge, 2020) despite one cannot presume that such kind of services ceased to exist. This kind of websites do not fit in the 5AMLD legal definition of exchanges. According to FATF (2019) these services provide a matching service between buyers and sellers, a point of contact to which users can resort to. Differently is to consider the CSPs used to conclude such interaction. If the platform only provides a forum to match CCs' buyers whilst they trade at an outside venue, such service will not constitute a CSP. If the platform entails the acquisition of CCs from a seller and selling them to a buyer, after a match occurred through the website, then it will be an exchange and/or transfer activity, observed the custodianship element on the transfer on behalf of its customers – although localbitcoins.com-type platforms legal treatment will depend on each jurisdiction's framework (FATF, 2019).

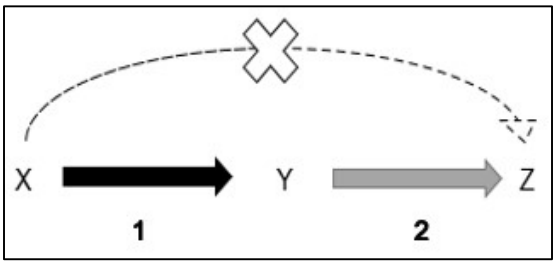
Crypto payment processors as Blockonomics – the bitcoin payment processor used by ITMC – announces on its webpage that "[o]nly e-mail [is] required!"[42]. Taking the example of other crypto payment processor, BitPay, it is explicitly mentioned that it "provides payment buttons"[43]. It seems that this kind of services are mere service providers of "click" buttons for customers to put on their websites to facilitate

[41] Smart contract technology is a self-executable contract that operates when certain conditions are met. *Ult. op. cit.* footnote 1, accessed on 27.10.2020.
[42] Available at https://www.blockonomics.co/docs/blockonomics-brochure.pdf, accessed on 18.12.2020.
[43] Available at https://bitpay.com/online-payments, accessed on 17.02.2021.

payments. Hence, under the 5AMLD's scope and FATF's understanding, Blockonomics would not be considered an exchange, nor a custodian wallet, if it does not transact CCs whilst providing private keys' safeguarding services. It is, hence, a non-custodian service. BitPay's Terms & Conditions explain that it provides wallet services, but that it does not take custody over users' funds[44]. This entity would not be caught by Art. 3(19) of the 5AMLD and FATF's standards as well as it is a mere facilitator.

Programming code improvements. Bitcoin lightning network offers an example of new methods used by CC users to avoid regulatory intervention. Lightning network technology allows its users to create a payment channel which, once closed when the transaction is completed, is published on blockchain. It might happen that this channel is continuously open, with transactional data never being published on the network. When the parties decide to close it, only their final balance will be published, with all the other transactional data being concealed. In the worst scenario, X and Y may share a payment channel, but X also wants to transact with Z. Then, X can send bitcoin to Y, who, in turn, will send it to Z. Transactions 1 and 2 will be recorded on blockchain. But the X-to-Z transaction will never be recorded (Paesano, 2019).

Figure 3 - Payment channels.



FATF provides us with a simple answer to such cases: regulation is applicable irrespective of its underlying technology. If the parties resort to a custodian wallet service implementing such technology, CDD on customer and on BO must be provided (FATF, 2019); however, on the blockchain setting, analysis by public authorities will be hampered, as the X-to-Y transaction was not recorded. Moreover,

[44] Available at https://bitpay.com/legal/terms-of-use/, accessed on 17.02.2021.

where such technology is implemented on a pure P2P basis, such information will be irremediably concealed.

Schnorr signatures is the latest improvement on Bitcoin protocol to enhance privacy (Chainalysis, 2020). It will make multi- and single-signature – *ie* multiple users can use the same aggregated public and private keys instead of each one using its own. It will conceal the identity of the participants in the transaction as one address belongs to a group of persons [45]. In addition, it resorts to smart contract technology, making those transactions "carried out on P2P exchanges look identical to standard transactions on the blockchain" (Chainalysis, 2020, p. 81). The same considerations above mentioned are applied: where an obliged entity is at stake, CDD must be conducted; however, in practice, CDD is not entirely useful for public authorities.

4.3. Entering the back door: obfuscation techniques

Privacy wallets. Terrorists are aware of the existent obfuscation techniques that erase the path leading to them as, for instance, ISIS' supporters were incited to resort to privacy wallets as DarkWallet[46]. CoinShuffle, Wasabi and Samourai are examples of privacy wallets which offer native in-wallet mixing. It resorts to CoinJoin technology, *ie* "all of the inputs are combined, [so] it becomes impossible to say with certainty which output belongs to which user"[47]. As the mentioned wallets are non-custodian-type,[48] these practices will fall outside the 5AMLD's scope.

Mixing services. There are mixers/tumblers which are, in essence, online platforms allowing users to mix their CCs (e.g., ChipMixer, BitMix.Biz and BitBlender)[49]. Yet, one difference remains in comparison to the services mentioned in the precedent paragraph. In this case the custody over funds is lost. Thus, such entities can be framed as custodian wallet providers under the 5AMLD.

[45] Available at https://medium.com/galaxy-digital-research/taproot-schnorr-scalability-and-privacy-upgrades-for-bitcoin-e81b0df9101b, accessed on 05.01.2021.
[46] Available at https://krypt3ia.files.wordpress.com/2014/07/btcedit-21.pdf, accessed on 30.11.2020.
[47] Available at https://academy.binance.com/en/articles/coin-mixing-and-coinjoins-explained, accessed on 05.01.2021.
[48] Available at https://coinshuffle.io, https://wasabiwallet.io and https://samouraiwallet.com, accessed on 09.04.2021, where it is expressly stated that these businesses offer non-custodian services.
[49] For instance, bestmixer.io was shut down by Europol on 22.05.2019 as it was connected to ML (Europol, 2019).

4.4. Building bridges: a two-speed EU and regulatory arbitrage

CCs cross-border nature can be exploited by terrorists to transact internationally whilst avoiding regulated gatekeepers (Keatinge *et al*, 2018). Although CC regulation is already in place, CDD application is not optimal – as shown in the AQB's case where wallet addresses were already identified as pertaining to terrorism supporters. There are numerous services presenting porous or weak CDD policies. For instance, in the EU context, Spain, Italy, Slovenia, Greece, Ireland, and Poland present poor results, which can be exploited by terrorists (CipherTrace, 2020[a]). Different regulatory approaches result in legislative fragmentation in the internal market and lead to inefficiencies and gaps within the EU which can lead to regulatory arbitrage towards jurisdictions where rules are more relaxed (EC, 2020[b]). The Dutch CSP Deribit announced its intention to move to Panama to precisely avoid the 5AMLD requirements (CipherTrace, 2021). Despite unavoidable loopholes, resulting from the 5AMLD's ambiguity and the large margin for appreciation, it will place burdens on CSPs which may need to adopt a MS-by-MS approach or even adopt a wait-and-see strategy as long as MSs do not implement specific rules. Indeed, it might not only be a question of avoiding the law, but a question of legal certainty. In fact, it is important to ensure a steady approach to CSPs to ensure clarity and a level regulatory playing field (Meijer, 2021). In addition to lack of clear rules, the EU regulatory fragmentation is an inevitable result of (1) MSs wanting to meet the FATF's standards (crypto-to-crypto exchange regulation and travel rule); and (2) full transpositions not being met EU-wide, with only 19 MSs having fully transposed the 5AMLD into domestic law,[50] after the sending of formal notices to Cyprus, Hungary, the Netherlands, Portugal, Romania, Slovakia, Slovenia and Spain on February 12, 2020 (EC, 2020[c]).

The 5AMLD harmonises check procedures towards HRTCs, but there are still persisting challenges. Lack of regulatory coordination creates an entropy at both domestic and international level, as transactions will (mostly) assume an international nature. States competition exacerbates the problem: instead of competing to provide the most crypto-friendly regime, national approaches should be coordinated as possible (Meijer, 2021). The fact that many jurisdictions, and

[50] *Op. cit.* footnote 33.

particularly those of developing countries, have no clear regulatory position on CCs – which might be a result of lack of resources and other priorities than applying international standards (Nanyun *et al*, 2020) – creates the risk of an incoherent international framework (Keatinge *et al*, 2018). Lack of international regulatory coordination is problematic for CSPs and exacerbates the difficulties already described at EU level. According to FATF (2021ª, p. 79), as they will interact with many other CSPs located in jurisdictions with different regimes and even in HRTCs, they will have to conduct counterparty CSP due diligence or "[o]therwise, […] face a tough decision in whether to deal with VASPs based in that country". CSPs must remain alert of customers sending or receiving funds from HRTCs' CSPs (FATF, 2020). Fragmentation will be explored by criminals and terrorists (Keatinge *et al*, 2018) to "fly under the radar" to "unregulated safe havens" (CipherTrace, 2020ª, p. 4; Barone, 2018ª, p. 42; respectively). These states will function as analogues to mixing services (CipherTrace, 2020ª). It is not enough to put in place regulation when practice hampers it. Thus, the legal space where CSPs operate is of utmost importance as it creates undesirable gaps (Salami, 2017). As CCs know no borders, "the framework to regulate them must be global as well" (Lawder, 2018).

4.5. The risk-based impasse

Despite the criticism surrounding FATF's legitimacy and democratic nature, the shift from a rules-based to a RBA is deemed as tool to provide states with discretion in the implementation of FATF's principles (Campbell-Verduyn, 2018). It is considered as a FATF's call for the private sector to participate in the decision-making process as well (Nance, 2017). The 5AMLD urges MSs to ensure that CSPs and supervisors evaluate risks and tackle them properly. Supervisors must employ a RBA to have a clear-cut image of its MS' TF situation, adjusting the supervision frequency and intensity and take proportional administrative measures (Arts. 8; 48[6]). However, supervisors have different risk understandings. Some do not even address risks; others do, despite not acting in a timely and effective manner. Divergent methods lead MSs to call for a common and consistent methodology to identify and assess risks (EC, 2021ª).

In addition to (1) respect MSs' sovereignty, providing them with flexibility, the RBA is (2) a model of efficient allocation of resources, which postulates that actions must

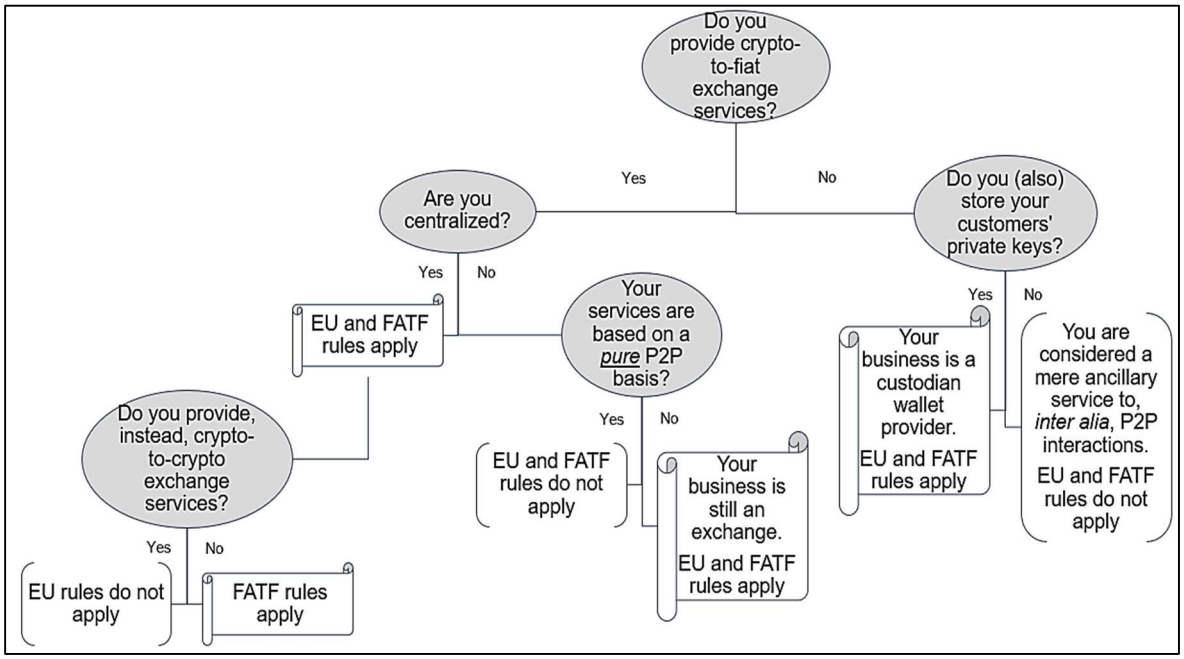
be commensurate with detected risks and (3) represents a dynamic approach to changing and emerging threats. Yet, it presents shortcomings, such as its (a) subjectiveness, leading to divergent applications of regulations. It is dependent on different levels of risk-sensitiveness and its openness to different interpretations generates different alignments between risk appetite and management – regulators might perceive an X risk, supervisors a Y risk and CSPs a Z risk. It might result into (b) inequal treatments. A same customer might be attributed a different risk-rating by different services. A same service might be treated differently across jurisdictions as well. Such risk-model might lead to (c) both scenarios of under and over attention to the risks – the de-risking phenomena (Durner *et al*, 2018). De-risking consists in overreactions and adoption of strategies to reduce risk exposure. Sanctions and reputational damages are its main drivers (Moneyval, 2015). De-risking might be responsible for pushing higher-risk customers or transactions out of the regulated perimeter, might happen towards entire sectors and jurisdictions as well (Silva, 2019). The most nefarious effect will be the generation of defensive reporting, turning risk identification, monitorization and mitigation even harder (Moneyval, 2015).

4.6. Intermediary conclusions

"Does the EU legal approach respond to all problems? Which problems does the EU solve and which does not?".

The 5AMLD came to address a novel and challenging reality. Silva (2019) considered the regulation of CSPs' activities to be premature, as an approach consistent with the RBA would have been to left margin for MSs to extend the 5AMLD scope to encompass such entities; nevertheless, its importance is undeniable, at least *prima facie*. The previous analysis intended to critically analyse the EU approach. It was assigned with two main drawbacks: the list of CSPs brought into its scope; and the vagueness inherent to its concepts and methods to achieve the desired outcomes. The following diagram provides an overview on CSPs' regulation both in the EU and according to FATF's standards:

Figure 4 - CSPs regulation overview.



Non-regulation of crypto-to-crypto exchanges was identified as a potential threat as CC users are provided with many venues to obtain goods and services which include, dangerously, Dark Web. It was also concluded that where platforms merely match supply and demand, it will not constitute a regulated exchange service. Many CSPs are not willing to take the risk of having AECs on their portfolio, which might

hinder these items' sustainability in the future and stifle innovation[51]. The existence of AECs which provide for user information opt-in might be a solution to consider if one has privacy concerns on personal information exhibited on public blockchain. However, if looking for totally shielding identity from public authorities' intrusion, it will not be possible considering the 5AMLD provisions.

The absence of a stance on non-custodian wallet providers is problematic. Where two non-custodian wallets holders conduct CC transfers, such transactions will not be regulated despite a value is being transferred. It is a natural consequence of a gatekeeper approach; yet its risks cannot be disregarded. Should the use of disintermediated methods exponentially grow – which is already foreseen, mostly on the part of criminals (Chainalysis, 2020) – the current regulatory framework's viability might be called into question. In addition, there are many services claiming on its terms of service that they do not take custody of customers' funds. FATF's step back on using the expression *a certain level of control* might indicate that custody service providers must exert fully control over a customer's funds, *ie* be the only in possession of private keys. Thus, the term "custodianship" requires further conceptualization and guidance on the CC setting and those CSPs' claims must be scrutinized.

Debile interplay between sectoral legislation was identified. As CCs do not constitute "funds" under Regulation (EU) 2015/847, no counterparty customer's data will be collected on cross-border transactions. Despite some MSs are taking a more stringent approach, practical problems impend on CSPs collecting data of non-custodian wallet holders wanting to infiltrate the regulated ecosystem.

In addition to (1) lack of clear and consistent rules, the EC (2021[a]) identifies two other main problems: (2) inconsistent supervision across the internal market; and (3) insufficient coordination and exchange of information among FIUs. I consider that problem (1) is the main driver to problems (2) and (3). Such drawbacks call into question the necessity to clarify, provide guidance, harmonise and facilitate MSs' AML/CTF bastions roles. It is understandable that EU legislation must consider MSs sovereignty; however, the success of the AML/CTF rules is dependent on a

[51] OKEx, Upbit and ShapeShift exchanges delisted zcash, dash and monero. South Korea declared its intention to implement stricter CDD policies and ban "dark coins" (CipherTrace, 2021).

concerted practice across the EU which is inconsistent with regulatory gaps on critical issues. Lack of the necessary resources was identified as a structural obstacle to properly conduct AML/CTF operations (EC, 2021[a]). The RBA was also criticized as an ambiguous standard which mandates further guidance for its effective implementation (Durner *et al*, 2018) to avoid inequal treatment of both CSPs and customers, innovation hampering and financial exclusion (EC, 2021[a]). Regulatory vagueness presents even more challenges for a new sector, such as the one under analysis, to adapt, resulting in doubts and divergent application by CSPs (EC, 2021[a]). The 5AMLD vagueness is dangerous on data protection issues as well as it can lead to unlawful intrusions on CC users' privacy (cf. Subsection 5.5). Hence, only through regulatory clarity coupled with sufficient resources, effective cooperation, information exchange and, thus, TF tackling, will be granted.

TF is intrinsically global and incoherent approaches, either due to vagueness or states regulatory competition, will have EU and worldwide horizontal impacts. Regulatory gaps will be exploited by terrorists as they will swiftly shift to poorly or non-regulated environments. According to Paesano (2019), regulation should be carefully implemented to create a level playing field and reduce compliance costs. Imposing fruitless costs on CSPs will end up reflected on customers' fees which may produce a shift to P2P environments; or even to more relaxed jurisdictions (CipherTrace, 2021). Nonetheless, one should not disregard that the CC sector should be treated, at least, on the same grounds as the banking sector. CCs are becoming more and more intertwined with the incumbent financial system. As such, to contribute to the soundness of such system, the sieve on CCs should be correspondently raised (Meijer, 2021; Mersch, 2018). As such, EU legislation needs to get more stringent towards the crypto sector.

All considered, 5AMLD's shortcomings must be addressed through a more consistent, granular, and multilateral approach for all the stakeholders at stake to better implement EU rules.

V. THE INESCAPABLE NEED FOR A MULTILATERAL RESPONSE

Terrorists progressively acknowledge new ways to remain anonymous and "make the job of the antiterrorism analyst harder" (Brill *et al*, 2014, p. 25). Thus, it is of key importance to counteract terrorists' evolving skills on CC abuse. Therefore, a proper response to the problems presented in the previous chapters entails a coordinated and cohesive multilateral approach.

5.1. Bringing (other) entities into the EU regulatory framework scope?

It is, first, important to ensure that entities that fall into the 5AMLD's scope apply for registration. Entities should be specifically created to identify unregistered CSPs to ensure that they comply with their legal obligations. Useful tools to uncover CSPs operating in violation of the registration requirement include publicly available information such as web-scraping and monitoring, as well as industry, intelligence, and reporting information (FATF, 2019). Additional relevant criteria to assess whether a CSP serves customers within a jurisdiction while not complying with registration requirements include offices and servers' location (e.g., call centers), promotions or marketing directed to certain countries, CSP' website/application language, the presence of a distributed network in a country such as visiting customers at domicile, and type of asked information to customers which might reveal the targeted state (FATF, 2021[a]).

The EC (2020[a]) recognized the importance of assessing the need to broaden the EU regulatory scope to encompass other entities, and was urged to expand such list (Council of the EU, 2020). Loopholes left by the 5AMLD led some MSs to adopt a more stringent approach. France and Portugal widened the legislative scope to include crypto-to-crypto exchanges (Le Maire, 2020; Art. 2[mm][ii], Law No. 58/2020). In addition, the Portuguese legislator, through Art. 2(mm)(iii) of Law No. 58/2020, which transposed the 5AMLD, is bringing into the legislative scope "[s]ervices whereby a virtual asset is moved from one address or wallet to another (virtual asset transfer)". As such, non-custodian wallets, *ie* transfer-only services, are covered by the Portuguese Law No. 58/2020. The latter refers to custodian wallet providers by allying safekeeping and transfer by referring to "*[s]afekeeping* or safekeeping and administration services for virtual assets or *of instruments that*

allow the control, holding, storage or *transfer of such assets*, including private cryptographic keys" (Art. 2[(mm)][(iv)]; added emphasis).

Outside the EU, despite not directly regulating non-custodian wallets, the US FinCen is somehow introducing obstacles to interactions with such players. It proposes the application of the "travel rule" to non-custodian wallets when transactions surpass $3,000. In addition, CSPs will have to file currency transaction reports when $10,000 or more are transferred through single or multiple transactions within a 24-hour period (Paesano, 2021). Indeed, FATF (2019) urges states to ensure that their customers provide the beneficiary information when transacting with non-obliged entities, including non-custodian wallet holders. The Swiss legislator adopted the most stringent approach: one can only send CCs to his/her own self-hosted wallet or another self-hosted wallet belonging to the same or other CSP, when it is registered and checked by the CSP (FINMA, 2019). In these cases, despite one has a non-custodial wallet, it will be necessary to provide identification data when wanting to infiltrate the regulated environment. If information is not provided, the wallet holder is denied the right to transact with a (hosted) wallet user that complies with regulation. Nonetheless, such stringent approaches towards CSPSs might be justified on the grounds that CCs are becoming widespread and intertwined with the financial and banking sector and, as such, should be treated, at least, on equal terms (Meijer, 2021; Mersch, 2018).

Houben *et al* (2021) consider that the 5AMLD's scope must be broadened to include (1) cryptoasset financial services providers, (2) issuers of cryptoassets, (3) cryptoasset creators, and (4) miners. Accordingly, financial services and crypto actors issuing or selling CCs (1, 2) should be regulated. Crypto asset creators, in turn, are considered to only grant technical tools, and as such, should not be regulated. The EC did not cover miners as those were considered mere technic service providers and due to enforceability challenges arising from extraterritoriality, as it considered miners to be mostly placed in China (Houben *et al*, 2021). Indeed, CCs might finance criminality, and particularly TF, through CC mining (Whyte, 2019). There are concerns regarding mining activities providing criminals access to laundered cash. Accordingly, those entities require deeper analysis in terms of regulation and a fiction might be created by imposing a middleman (Houben *et al*, 2021). However, miners fail to fulfill the "on behalf of their customers" sieve as they

are considered to solely operate a CC-related network (FATF, 2021[a]). Thus, what would be the criteria to impose regulation on miners, as CC generators, and not on a service that, despite being considered ancillary, as non-custodian wallets, allows transfers of value to occur? CC mining is a licit activity that rewards miners for their computational power; it is the destination of such proceeds that could be illicit. As such, only transfers of value, as in TF criminalisation, should be regulated. If minted CCs are then transferred or exchanged trough regulated CSPs, they will possibly capture criminality (namely though filtering methods presented on Subsection 5.2). At most, covering at least some extent of the mining activity can be thought of in tax terms with regard to the declaration of income, which might be useful if such CCs do not enter the regulated space through any of the gatekeepers – it will create at least a chokepoint.

5.2. Cryptocurrency sector approach

CDD and EDD to privacy-enhancing tools. CDD should be applied irrespective of the type of CC or privacy-enhancing service. CC users should be treated on equal terms. When it comes to AECs, zcash, for instance, besides privileging privacy-by-default, has an option "to reveal […] data for the purposes of auditing or regulatory compliance"[52]. If such features are available, despite detailed information on users is opaquer on blockchain, it might comply with regulation. Information will be available upon request. This kind of features might be the answer for CSPs to continue offering AECs and privacy-enhancing tools. However, if blockchain is an open source for public authorities to consult, in these cases, their investigative work will be much dependent on STRs filled by CSPs. Where regular CDD threshold amounts are not activated, and where a TF suspicion exists, applying EDD to privacy-oriented tools is possible on the grounds that it constitutes a product or transaction that might favour anonymity (Annex III[2][b] *ex vi* Art. 18[3]). When such suspicion does not exist, a safety valve is applicable to the cases not directly prescribed by the 5AMLD: when MSs or obliged entities identify "other cases of higher risk" (Art. 18[1]). In such scenarios, they should apply the general principle of the RBA. Therefore, as the perceived risk is higher, the "sieve" is tighter, and EDD is applied, as AECs allow completely anonymous transactions. One could argue that

[52] Available at https://coinmarketcap.com/currencies/zcash/, accessed on 08.12.2020.

such a solution would offend the equality principle between CC users. However, CC users should be treated on equal terms, irrespective of the underlying technology of the tool there are resorting to. Situations that pose similar risks should receive equal treatment (FATF, 2019). Privacy enhancing tools users pose a different risk, being it legitime to apply to them tighter criteria. FATF (2021ª) states that when such approach is not sufficient, CSPs should not engage in such activity. Yet, regulators must provide CSPs with detailed guidelines on how they should conduct CDD when confronted with users that enhance their anonymity levels (Keatinge *et al*, 2018). CSPs should collaborate with regulators to establish guidelines and tools to be used in investigations involving AECs (Chainalysis, 2020) – namely through risk categorization tools (cf. Subsection 5.3). It is worth to question whether such options will defraud users' privacy expectations. User information will continue to be obfuscated on blockchain. If one has privacy concerns, at least at blockchain-level, other participants and entities will not, at a first glance, have access to identification data – despite the concept of pseudonymity entails that crossed information might reveal a CC user data. A different topic is that this information will be available and might be delivered to public authorities upon request, putting legitimate users in a fragile position. In such a scenario, EDD might give space for the "underground" ecosystem to expand as privacy concerns will lead CC users to shift to unregulated services.

Capacity building: training, feedback, risk assessments and RegTech. Despite CSPs are in possession of customers' and transactions' data, framing a TF situation is always a complex task for such private actors, particularly as TF "does not always follow clearly recognizable guidelines" (Goméz, 2010, p. 25). As such, training assumes a pivotal aspect to enhance their capacity in this regard. Most importantly, the lack of feedback on STRs must be addressed as it is vital for CSPs to calibrate their knowledge on confirmed or unconfirmed suspicions.

As CSPs should implement model risk management practices, internal controls, manage their compliance and, where necessary, an independent audit function (Art. 8[4][a]), regulatory technology (RegTech) may allow apply technology such as AI, data analytics, and machine learning to meet regulatory requirements "in a more efficient and effective way" (Portuguese Securities Market Commission, s.d.). CSPs could benefit from RegTech by introducing built-in options such as geographic, CC

type, amounts, and P2P transactions limits (Salami, 2017). The FATF's (2020) red flag indicators could be the basis for CSPs to design their own RegTech tools. Engagement with other industry actors that are already offering such services will facilitate CSPs' adherence to RegTech. Industry actors provide: assistance in assessing whether they comply or violate AML/CTF rules, allowing real-time reaction (Chainalysis, s.d.); tools to identify when inbound monero may have criminal origins (CipherTrace, 2020[b]); secure protocols for CSPs to mutually authenticate each other and ensure data interoperability – the Virtual Assets Account Number (VAAN), in a similar manner to IBAN (Riegelnig, 2019); tools to securely transmit customers' data with the transaction without attaching it to the transaction itself, which is to be decrypted by the receiving CSP (Sygna Bridge, 2020); and tools which helps banks attributing scores to CSPs according to their CDD quality (CipherTrace, 2020[c]) and can be deployed by CSPs in their activities as well.

Wallet addresses' identification, red flags, and data hubs as information exchange enablers. Central registries should be created to "allow the identification, in a timely manner, of any natural or legal persons holding or controlling payment accounts and bank accounts identified by IBAN" (Art. 32a[1]). This legal provision does not capture CSPs. However, they should have received the same legal treatment as the financial institutions, being captured by such provision.

In the financial sector, central registries are often described by LEAs as an instrument to facilitate financial investigations, including TF related ones (EC, 2016[a]). In addition to identification, a system to flag suspicious addresses should be developed to facilitate investigations and prosecutions. A possible solution would be to create a filtering system.

Figure 5 - Wallet addresses filtering system.

This system should be accessible to CSPs and would facilitate the process of identifying TF-related addresses. In the case of, for instance, the AQB campaign, it was stated that although the identification of a wallet address does not automatically shut it down or block its transactions, it is a means to encourage CSPs to flag such addresses and report them. It is recognized, however, that where terrorist organisations are not recognized as such by third countries, CSPs will not be compelled to flag such transactions (Fanusie, 2019).

The use of Central CC User Databases and blockchain analysis tools, however, may violate the fundamental rights of data protection and privacy (Rueckert, 2019). The Article 29 Data Protection Working Party (29WP) (2011) expressed concerns on this matter – centralization of data should give place to local storage "within the EU or countries with adequate data protection", as centralization "contradicts several fundamental data protection principles". A national-level data sharing scheme would be an important starting point. If concerns still exist, it would be at least important for each CSP to create such a system. FATF (2019) supported the idea of CSPs having in place a swift wallets' identification system through blacklisted wallet addresses. CSPs would compare it with its' customers and their counterparties to conduct an onboarding scanning and an ongoing monitorization. The wallet addresses' identification system proposed could be built upon the red flag indicators designed by FATF (2020).

National or CSP level data hub efficiency would be, however, hampered, as no networking would be done and, as such, identification systems would not be as up-to-date as possible. As long as privacy-by-design and by-default principles are met – *ie* safeguarding data protection and privacy from the outset (EDPS, 2020) – these datasets should be privileged. For instance, Ma^{3}tch is a FIU.net analysis tool which matches national FIUs data and triggers a positive hit that involved FIUs might follow if cross information of interest is pinpointed. Tools of this kind do not provide access to any personal data until there is a match; personal data sharing only takes place if there is a hit and the FIUs choose to investigate it – ensuring a privacy by design solution. In addition to data matching, Ma^{3}tch can also be used to share know-how on risks and behaviour patterns (Mouzakiti, 2020).

A "translucent" ID blockchain system could be used. CC users' personal data such as driving license or ID would be built upon blockchain itself. Blockchain would serve as the record-keeping system for such personal data providing for the security and integrity of the information *in casu*. A third party would retain access to the necessary credentials to access such information, similar to an escrow service, which would only grant access to it on certain pre-defined conditions. This would allow a customer to remain anonymous to a CSP and public authorities, but it would also allow identification if and when necessary (FinTech Futures, 2016).

The use of the eID tool is also proposed by the EC (2021[b]). Allowing the EU citizens to share the data they want, it can help ensuring that only the legally required information is shared, hiding the remaining personal data. This digital identity can also introduce adequate security safeguards to protect data (EC, 2021[b]). Blacklisting for CCs themselves instead is also proposed, CCs being compared to stolen bank notes. CCs with an underlying criminal activity should, if technically feasible, be tainted or tagged. This would prevent criminals, and terrorists in particular, from using such CCs and render them less interesting (Houben *et al*, 2021).

Codes of conduct and self-regulation. CSPs are interested in the evolvement of the crypto market, so they have "an internal incentive to engage in self-regulation" to build a positive reputation (Kfir, 2020, p. 115). Through Blockchain and Virtual Currencies Working Group, the CC industry makes efforts towards compliance.

According to its ethical guidelines (s.d.), its members will only accept transactions originated from counterparties which appropriately mitigate risks. Its adherents might set common robust standards and goals, including CTF, to comply with in order to become a member and be allowed to interact with other players in the sector. Nonetheless, it can only be a complement to formal supervision (Keatinge et al, 2018). FATF (2019) considers that CSPs should, instead, be supervised by a competent authority. Keatinge *et al* (2018, p. 56) go even further, supporting the opinion that the EU "could pursue pan-European self-regulatory bodies, as well as other country-specific bodies". Such a structure would be relevant to MSs' regulators as well, as a venue for them to engage in and ensure that the crypto industry implements effective CTF controls (Keatinge *et al,* 2018).

5.3. Institutional approach

Capacity building and Enforcement. Legislation and investigative practices must be genuinely connected (Europol, 2020[a]). MSs should endeavor to develop LEAs and FIUs' capacity by constantly updating their knowledge on CC developments to disrupt TF (Keatinge *et al*, 2018). Supervisors also lack the necessary resources to conduct their tasks. As such, it is of utmost importance to guarantee that they are provided with the necessary tools to enlarge their capacity. Their personal need to be trained on blockchain analytic tools to understand how it operates as CSPs are resorting to these tools to conduct their own risk assessments (FATF, 2021[b]). Some of the 4th Global Conference on Criminal Finances and Cryptocurrencies' outcomes were, precisely, that capacity building is key and massive importance shall be given to the production of manuals, training projects, exchange programs and international conferences (Europol, 2020[b]). Training on basic topics such as types of wallets and CCs' seizure process is important – e.g., paying attention to hardware wallets to be confiscated or having readily available wallets to transfer the CCs during investigations (Keatinge *et al*, 2018). Indeed, not only imprisonment but also funds seizure is a disincentive tool. In the EU, confiscation rates are still very low (Ferber *et al*, 2020). Enforcement shall be achieved through standardization of freezing and confiscation of criminal proceeds (EC, 2020[a]), as well on the mutual recognition to facilitate cross-border recovery of criminal assets and legislation to facilitate administrative freezing by FIUs (Ferber

et al, 2020). Other mechanisms might contribute for the enforcement of EU rules: the US Financial Technology Task Force introduced a reward scheme for valuable information provided on the terrorist use of CC (Barone, 2018[a]). Therefore, enforcement is inevitably dependent on several factors.

Evidence shows that even AECs can be traced and that LEAs must enhance their knowledge and explore these CCs vulnerabilities (Koerhuis *et al*, 2020). There are several projects and partnerships demonstrating an effort at EU, MS, and international level to enhance knowledge on CCs: (1) at EU-level, the TITANIUM project allows LEAs to monitor CC and Dark Web ecosystems, transactions occurred on different blockchains and to generate court-proof evidence reports[53]; Basel Institute on Governance, in cooperation with the Egmont Group of Financial Intelligence Units, provides FIUs with free eLearning courses on suspicious transactions analysis and CC-related TF threats[54]; Europol and the Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research (CENTRIC) formalized a partnership that resulted in CRYPTOPOL, a game which simulates CC investigations (Europol, 2020f); in August 2020, Europol conducted the first international survey to understand how cooperation with CC exchanges will take place (Europol, 2020[a]); (2) at MS-level*:* VIRTCRIME, an Austrian research project, is intended to develop tools for the analysis of *inter alia* AECs (Keatinge *et al*, 2018); (3) at international level, Interpol developed a group of tools such as GraphSense, a tracing tool which allows investigators to search addresses and transactions by tag and to create clusters of related addresses; the creation of a CC taxonomy to define and aggregate the kind of suspicion-related data that should be collected; CapaCT, conducted by Interpol and The Netherlands, which will consist in guidelines and training manuals for ASEAN Countries' authorities to analyse CC misuse on the Dark Web and by terrorists; the Darknet and Cryptocurrencies Task Force, a working group established in combination with the Bavarian State and global experts, as an international hub to exchange information on crime-related wallets, methodologies, best practices, investigative standards and forensic tools for LEAs[55].

[53] Available at https://www.titanium-project.eu, accessed on 15.02.2021.
[54] Available at https://baselgovernance.org/basel-learn, accessed on 09.01.2021.
[55] Available at https://www.interpol.int/How-we-work/Innovation/Darknet-and-Cryptocurrencies, accessed on 12.02.2021.

Despite the divergencies in the resources and methods applied, FIUs exchange of know-how is limited, and they sometimes resort to private actors when other FIU would be best placed to provide them with expertise (EC, 2021ª). Indeed, the public sector shall innovate its investigative techniques and invest in CC-specific technology when reliance in the private sector is not the only, nor the optimal, solution. Conflicts of interest, governance, liability, and ethical issues might arise (Lannoo *et al*, 2021). When not accompanied by political commitment and an appropriate legal framework, public-private partnerships (PPPs) turn into complex and time-consuming structures. Sometimes risks are better managed by public entities. As to emerging markets, PPPs might not provide the adequate level of competence and quality as expected and, furthermore, create obstacles to find a suitable substitute. Such a novel market to procure PPPs might also lead to increasing costs to the public sector and even collusive behaviors (European PPP Expertise Centre, 2015). In addition, privacy and data protection might be impacted by PPPs (cf. Subsection 5.5).

When it comes to FIUs lack of cross-border coordination, the EC (2020ª) argued that an EU-level coordinator and support mechanism could assist FIUs in identifying and jointly analysing cross-border cases. The EP welcomed that proposal, adding that the EU FIUs coordinator should be a hub to propose common standards for cooperation, promote training, capacity building and know-how exchange between FIUs. Furthermore, such an entity should be empowered to access relevant information in different MSs (Ferber *et al*, 2020). The EU legislator provided for new measures on this topic (cf. Subsection 5.6).

(EU-level) Supervision and SupTech. For supervisors to consolidate their positions at domestic level, they need strong legal basis to exercise their mandates and powers, as well as political and organisational support (FATF, 2021ª). When it comes to anticipate the imminent regulated population, resorting to relevant (inter)national organisations, to open-source data and to workshops addressed to CSPs might constitute useful tools. Supervisors should undertake sectoral and granular risk assessments and provide feedback and guidance on CSPs' own risk assessments results. They should put in place channels to communicate national risk assessments or conduct a more educational role while explaining such

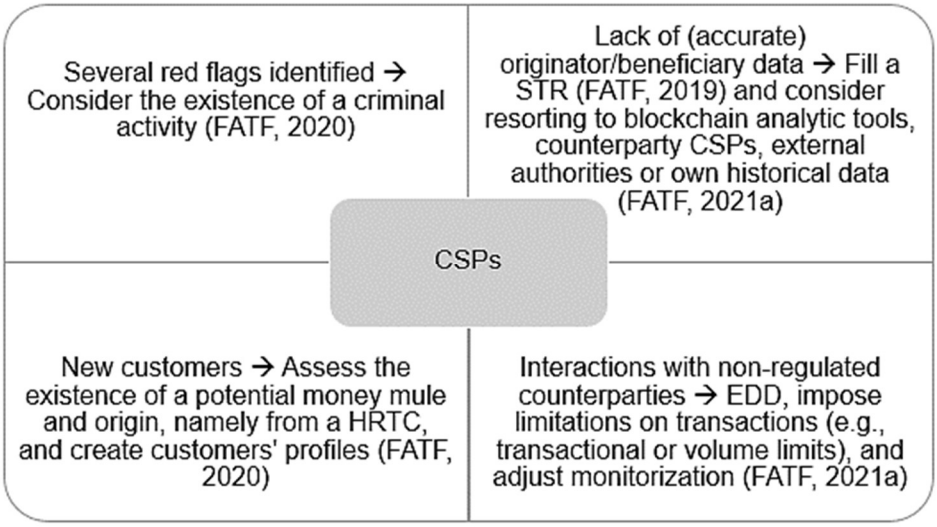
outcomes, and consider drafting templates for CSPs to resort to when conducting their own risk assessments (FATF 2021[b]).

The next step will involve "a change in the supervisory culture" (FATF, 2021[b], p. 5). RegTech gained space among supervisors – as Supervisory Technology (SupTech). Needs for efficiency and effectiveness in detecting and mitigating TF risks lead several supervisors to resort to it. SupTech's benefits include *inter alia* sharing information with other entities, strengthening surveillance capabilities, entity-focused supervision, targeting novel risks more effectively, machine-assisted analyses of large datasets, and real-time monitoring (FATF, 2021[b]). Nevertheless, efficiency does not come without costs and might bring cyber-related threats – such as data loss leading to interruption of supervisory activities (Broeders *et al*, 2018) – which must be properly foreseen. Singapore, United Kingdom, Brazil and Mexico are examples of jurisdictions resorting to SupTech to conduct risk rating, risk surveillance and prepare on-site inspections (FATF, 2021[b]).

As registration on incorporation and host jurisdiction signify that a CSP might be subject to dual or multiple supervision, sound and effective cross-border cooperation is required (Pavlidis, 2020). As such, fragmentation of action across MSs demonstrates that not only national supervision, but also EU-level supervision is of utmost importance. The Council of the EU (2020) warned the EC on the dangerous of riskier sectors such as the one pertaining to CCs and advised the EU institution to focus on the creation of an EU-level supervisor. The EC (2020[a]) pointed that EBA, or otherwise an *ex-novo* entity, should be attributed with such task to complement national supervision. Houben *et al* (2021) consider that, in addition, it would constitute a pool for information and expertise sharing and would deliver a more objective approach to AML/CTF cases. Therefore, whilst supervisors must individually prepare themselves, an EU-level supervisor should exist to combat fragmentation. The EU legislator provided for new developments on this topic as well (cf. Subsection 5.6).

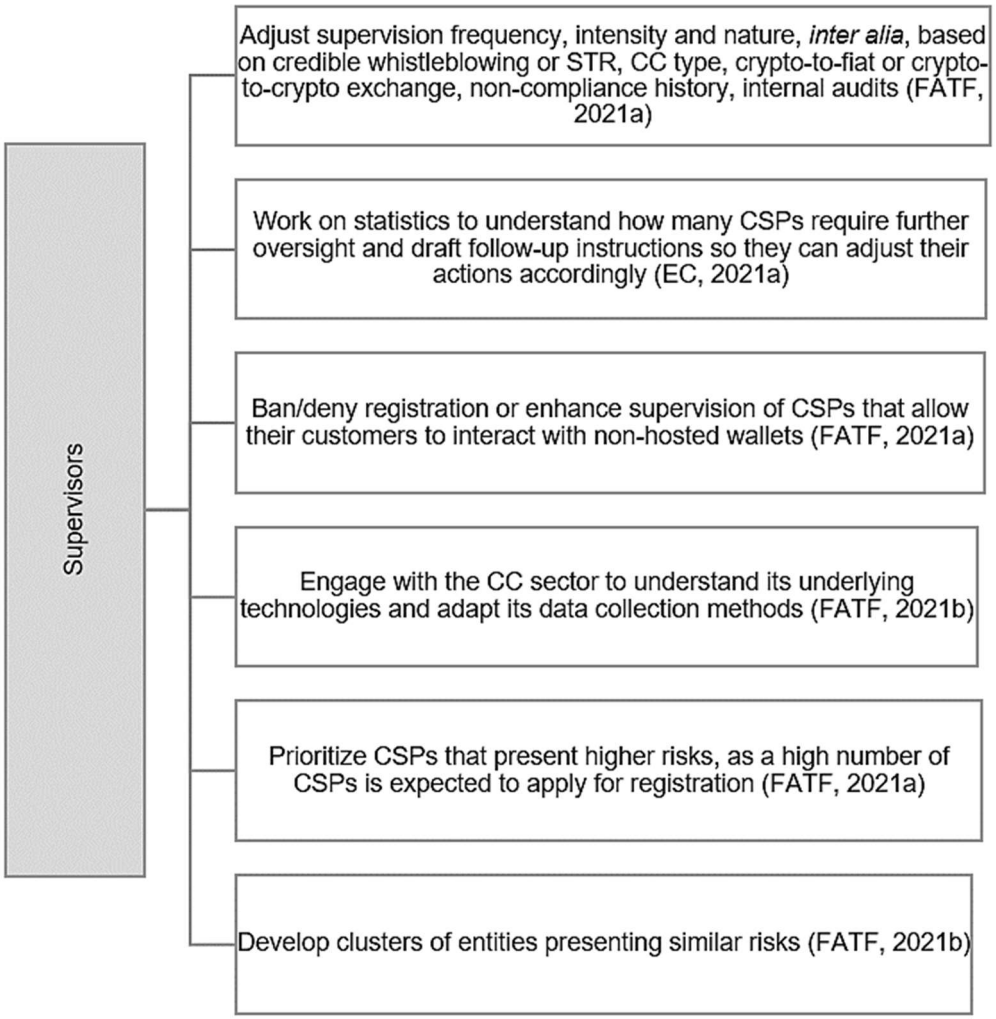
Risk categorization tools. Densifying risk indicators and how to tackle them will provide granular guidance to CSPs and NCAs. The following figure bundles risk identification and mitigation orientations to CSPs:

Figure 6 - CSPs risk identification and reaction mechanisms.



In turn, whilst shifting from a rules-based to a risk-based supervision (FATF, 2021[b]), supervisors should implement the following measures:

Figure 7 - Supervision management.



How to address HRTCs? What level of interplay should states engage in and at which level? The EU legislator acknowledged that the weak points generated by MSs' different approaches must be tackled by improving the effectiveness of the list of HRTCs and coordinate as much as possible the treatment towards those jurisdictions (Recital 12). However, the methodology and approach adopted by the EC in 2019 was criticized by the EP as a gold-plating of the FATF list and identified a lack of engagement with the detected problematic jurisdictions (EC, 2021[a]). In 2020, the EC presented a new methodology to identify and address HRTCs, but its inability to demarcate cooperative from non-cooperative jurisdictions was criticized (similar to what is achieved by FATF's "grey" and "black" lists), as well as the non-identification of specific EDD measures for MSs to apply, the disproportional nature of restrictions towards cooperative HRTCs, the difficulty to impose enhanced vigilance and deficiencies on publication of HRTCs that not allow public scrutinization (EC, 2021[a]). As such, those specific points should be re-thought. Nevertheless, the EU choice to impose stringent criteria to identify HRTCs in the context of the 5AMLD was welcomed by the EP (2020, p. 9) as it frees the EU from "geopolitical meddling".

When it comes to the necessary level of interplay between the MSs to build a robust framework to tackle CCs cross-border nature, harmonisation constitutes an important and achievable approach (even if not fully achieved yet) due to MSs' sovereignty and EU voting unanimity rules. Effective cooperation and coordination requires in-depth harmonisation (Council of the EU, 2019). However, the EU CTF policy will never be totally common at regional level due to "significant operational, functional and sovereignty hurdles to overcome" (Andreeva, 2019, pp. 363-364). Nevertheless, the EC (2020[a]) pinpointed the importance of incorporating specific topics into a Regulation: the definition of obliged entities, CDD, internal controls, STRs and provisions on BO and central bank account mechanisms. Hence, such topics should be addressed through a directly applicable regulation, and not a Directive, to fill existent gaps (cf. Subsection 5.6).

At global level, cooperation is even more complex. Setting a global standard for countries to comply with is a great challenge as there are financial and legal systems in different development stages; different commitment levels to tackle terrorism; and different attitudes as to the balancing exercise between security and freedom

(Salami, 2017) (cf. Subsection 5.5). Yet, Salami (2017, p. 5) calls for a "coordinated global regime", considering that the RBA fails precisely because AML/CTF rules are implemented at a micro-level. Therefore, the appropriate attitude towards CC-related TF risks is to maintain a coherent coordination scheme at international level. A more interconnected regulation at such level is a rather non-realistic ambition as what is difficult to achieve at micro level (e.g., in the case of the EU) becomes even more challenging at macro level. Therefore, no uniformisation, and not even harmonisation, are options to take at such level. It is important to ensure, nonetheless, coordination with regard to matters of central importance, namely, to ensure that states implement CC regulation where regulation is still absent (Keatinge *et al*, 2018). International cooperation must be strengthened in terms of mutual legal assistance, identification, freezing, seizing and confiscation proceeds, providing effective extradition assistance (FATF, 2019), and through channels such as Interpol, Europol, the Egmont Group and FIU.net (Europol, 2020[b]). Moreover, it is for the EU "to play a leadership role in advocating for a coordinated AML/CTF global regulatory framework" towards CCs, to ensure a minimum level of effectiveness to be in place and that no critical gaps exist in other states' legislation (Keatinge *et al*, 2018, p. 10).

Educating netizens[56] *and countering terrorist propaganda*. In 2019, EU-individuals' digital skills average was scored with around 57 points in 100, a considerable low level nowadays (Eurostat, 2021). It indicates that education for the safe use of the Internet is still required as a pre-step, as we are all (cyber)security agents. Netizens' education shall evolve for the development of CC-awareness and safe use, for them to be aware of whether their funds are being transferred to a façade humanitarian aid campaign or a terrorism-related address. Very simple recommendations such as googling wallet addresses is a useful resource. It gives access to online newspapers, CC community blogs, or websites connected to the address (Smith, 2019[b]). In a more advanced scenario, CC-related blogs provide useful information on tools which, when used in connection, provide netizens with an overall picture. The bitcoin BlockExplorer tool provides access to the bitcoin blockchain; BitcoinWhosWho provides user-reported data on addresses associated

[56] *Ie* Internet users (Polydor, 2020).

with illicit activities; and WalletExplorer shows the addresses linked to a same wallet and associated exchange. Such blogs provide (not so technical) guidance on how to use these tools (Smith, 2019[c]). Then, netizens may take on a more advanced research task, which involves programming. It combines Python programming language, BlockExplorer and Webhose.io., which performs secondary Dark Web searches to acknowledge the existence of hidden services referring to specific wallets (Seitz, 2017). Therefore, it is recognized that "in the near future, it may be simple for anyone- including friends, relatives, employers, and law enforcement, to track every BTC transaction" (Rebane, s.d.). However, education of netizens encompasses not only instructions on Internet safer use, but to implement a culture of crime reporting (Kfir, 2020). Consultation and cross-check information with the European Database of Terrorist Offenders is useful to that end.

In a study on a sample of 119 lone actor terrorists, almost all expressed their violence and extremist ideology through social media posts (Tierney, 2017). Indeed, globalization makes it possible to achieve the top-down effect, *ie* propaganda that reaches and radicalizes people around the world (Barone, 2018[a]). Europol (2020[g]) concluded that real-time coordination and engagement between MSs and Online Service Providers remains vital, and that such cooperation will facilitate investigations and contain potential threats. Akhbar al-Muslimin tried to counter the fact that its official website was continuously being shut down. Therefore, countering terrorist propaganda is critical to prevent, at first, radicalization from happening as terrorists reach a tremendous number of supporters without spending anything. It would permit to cut down donation links. Globalization also makes it possible for bottom-up effects, *ie* the fact that new and younger members bring with them new approaches and tools (Barone, 2018[a]). The current and next generation of technological savvy terrorists will push terrorist organisations more and more into the use of new technologies, namely CCs. Despite that, less experienced terrorists may still resort to advanced techniques through how-to guides available on the Dark Web (Keatinge *et al*, 2018) or contact skilled criminals to provide guidance on the use of CC or conduct the required act – crime-as-a-service[57]. Monitorization of Dark Web is thus pivotal to prevent not only terrorists from acquiring illicit goods with an

[57] Cf. "Europol Internet Organized Crime Threat Assessment", 2014, available at https://www.europol.europa.eu/iocta/2014/toc.html.

extra layer of anonymity provided by CCs, but also to prevent these entities from networking and obtaining more human and financial resources to their causes. Therefore, monitorization of money flows, social media and Dark Web is of great importance to better tackle TF (Barone, 2018[a]). Nevertheless, it inevitably raises freedom and privacy concerns (cf. Subsection 5.5).

5.4. The inevitable symbiosis

P2P interactions' dangers must be properly addressed. EU and MSs' institutions must meet its obligations whilst joining forces with the private sector to fill the gaps inevitably left by the EU regulatory framework. The alliance with the private sector lays on states' lack of capacity to cover "every corner of society" (Koh, 2006, p. 40). PPPs should be encouraged as the public sector cannot act alone (Keatinge *et al*, 2018). Taking into consideration that CSPs are already obliged to fill STRs, the EC (2020[a], pp. 30-31) refers that obliged entities should receive "information on typologies and trends by FIUs and law enforcement" and "operational information on intelligence suspects by law enforcement authorities". However, this information should not flow bidirectionally only on such instances, this partnership should be carried out horizontally. There are private companies providing blockchain forensic tools which are expected to complement the institutional approach (Keatinge *et al*, 2018). Blockchain analysis companies can contribute to the research on terrorists funding methods and to the potential identification of terror networks by tracking CC activity (Eisermann, 2020). Additionally, and despite the merit of PPPs discussed on Subsection 5.4, these private companies' efforts to make data analysis interactive and easy to understand is of utmost importance to fill the crypto-and-blockchain literacy gap existing in the public sector. There are several examples of the public-private sector's symbiosis: Chainalysis supporting Europol's European Cybercrime Centre investigations (Keatinge *et al*, 2018); Blockchain Alliance, which provides a channel for open dialogue between the industry, LEAs, regulators, Europol and Interpol[58]; CipherTrace supporting the US Government through traceability simulation

[58] Available at https://blockchainalliance.org/wp-content/uploads/2018/07/blockchain-alliance-infographic.jpg, accessed on 07.01.2021.

techniques (CipherTrace, 2020[b])[59]; Elliptic (s.d.) providing tools to assist in the identification of suspects, to secure convictions, and to train on blockchain analysis.

Another important topic to consider is the creation of a data hub to be shared between the public and private sectors, a PPP which would, in coordination with Europol, "facilitate these contacts and interactions" (Keatinge *et al*, 2018, p. 10). Risk assessments, how and why terrorists misuse the CC environment, feedback on STRs and suspicious indicators, and information on assets that should be frozen should be priority topics covered by PPPs. Nevertheless, confidentiality agreements should be in place when classified data is shared (FATF, 2019). Solutions presented on CSPs' data hubs could be applicable on this instance as well (cf. Subsection 5.2). However, such interactions raise privacy and data protection challenges (cf. Subsection 5.5). Existing PPPs at EU level are mere systems to share information with no cross-border dimension and involving a small number of actors (EDPS, 2020). Taking into consideration all the variables at stake, the EP urges the EC to draft a clear legal framework which establishes duties and profiles of participants of these tripartite platforms. LEAs, FIUs and private actors shall comply with exchange of information, privacy, data protection and data security rules, whilst respecting fundamental rights of data subjects (Ferber *et al*, 2020).

The symbiosis can also be achieved through expert working groups which can analyse the necessity of further EU level measures (Keatinge *et al*, 2018). In fact, continuous assessment of regulatory adequacy is important. MSs might resort to regulatory sandboxes – ecosystems that provide a "direct testing environment for innovative products, services or business models, pursuant to a specific testing plan, which usually includes some degree of regulatory lenience combined with certain safeguards" (Parenti, 2020, p. 9). Thus, it is a solution that might be put at the disposal of CSPs to test their compliance, whilst allowing regulators to assess the adequacy of regulation and anticipate risks. Indeed, such an EU working group agency can work on the results reported by MSs whilst implementing regulatory sandboxes. According to Goldman *et al* (2017), for the success of the CTF framework, policymakers shall, in addition, assess how other financial innovations with the same aspirations as CCs have successfully prevented TF. Hence,

[59] It filed two monero tracing patents which can assist financial investigations (CipherTrace, 2020b).

regulators should compare CCs with other technological developments and assess how those innovations are addressed by law and the efficiency of the rules at place.

5.5. The proper response: a balanced approach?

In the era of big data – *ie* data that is big in terms of volume, velocity, variety, veracity and value (Alwan *et al*, 2020) – innovation, digitization and economic growth benefits arise. Yet, there are also threats such as data manipulation, discrimination, oppression and individuals' rights and freedoms violation. Netizens are becoming aware of the economic, political, and social value of their personal data: activists in oppressive regimes (Möser *et al*, 2018); rich "bitcoiners" with physical integrity concerns (Eisermann, 2020); people distrusting states' systems (Kfir, 2020); Venezuelan citizens concerned with government seizure (Nguyen, 2020); impoverished communities financial inclusion through a system that is not prone to political influence (Whyte, 2019); people worried with the horizontal dimension of private interference (CoE *et al*, 2018) revealed by the Cambridge Analytica data-leak scandal (SIC, 2019). Against this backdrop, the security v. freedom conundrum is a question that still requires social and political discussion *inter alia* in the CC ecosystem.

There are several fundamental rights to consider in the CC environment. Rueckert (2019, p. 6) refers to the "cryptocurrency classics", namely personal data protection (Art. 8 Charter of Fundamental Rights of the European Union - EUCFR) and privacy (Art. 7 EUCFR)[60]. Those are analysed in turn against the fundamental right to security (Art. 6 EUCFR).

The privacy concept passed through several perceptions: (1) "private as opposed to public", (2) what concerns an individual; and (3) control upon one's personal information (Fuster, 2014, p. 22). Security, on the other hand, entails (1) an absence or unlikeliness of threat (Boemcken *et al*, 2016); (2) freedom from risks and dangers (Lieshout *et al*, 2012); (3) and addresses different entities – individual, national and international security (Afolabi, 2015). Security leads to the need for risk suppression measures (Lieshout *et al*, 2012) as privacy and data protection "are not absolute

[60] Freedom of telecommunication, right to property, to pursue a trade or profession are also CC classics. Other type of fundamental rights identified by the author in the CC landscape are the ones referring to P2P networks – freedom of assembly and association, for instance.

rights, [and] must be considered in relation to their function in society" (European Data Protection Board, 2020, p. 7). Limits to privacy and data protection must (1) be provided by law; (2) respect the essence of those rights; (3) respect the principle of proportionality; (4) be necessary; and (5) meet objectives of general interest recognised by the EU or be needed to protect the rights and freedoms of others (Art. 52[1] EUCFR).

Provided by law. Interferences with a fundamental right must be prescribed by law. Data processing is thus provided by law as the 5AMLD entered into force since June 19, 2018. In addition, the criterion of the quality of law must be met (EDPS, 2019): clear and precise rules, adequately accessible (public) and foreseeable laws must be at place for its addressees to regulate their conduct (Data Protection Commissioner/ Maximillian Schrems, §§174-175; Privacy International/ Secretariat of State for Foreign and Commonwealth and others, §64-65; Mengozzi, §193; Øe, §139). As already noted, the 5AMLD is a vague piece of legislation, despite it is clear on the thresholds (amounts) or timings (e.g., inaccurate or inadequate data) that activate data collection; however, further clarifications on the specific type of data collected from CSPs' customers are needed as data collection must be based on "objective criteria provided for in the national legislation" (La Quadrature du Net and others/ Prime Minister and others, §189). Data subjects are only able to properly consent data collection and processing when clear, precise and accessible rules are in place. It might not be clear for data subjects that their data might be shared with other MSs' FIUs on an intelligence-based approach rather than upon a STR. The EDPS (2020) recommended FIUs' right to access and to share information to be clarified.

CSPs-to-public authorities data share should occur upon very defined conditions, as private entities retaining and making available data to NCAs constitute (further) interferences with fundamental rights (Privacy International, §§60-61; Digital Rights Ireland/ Minister for Communications, Marine and Natural Resources, §35). STRs triggers are broadly defined in the 5AMLD. Hence, MSs must identify specific and defined conditions to that end (e.g., the risk categorization tools presented in Subsection 5.3).

Art. 41 did not solve doubts on the applicable data protection regime, which might be related with FIUs organisational status. The Directive (EU) 2016/679 (General Data Protection Regulation – GDPR) is applied by some FIUs, while the Directive (EU) 2016/680 (Police Data Protection Directive) is applied by others: law enforcement-type United Kingdom's FIU applies the GDPR whereas judicial-type Luxembourg's FIU applies the Police Data Protection Directive (Mouzakiti, 2020). Nevertheless, irrespective of FIUs organisational status, the nature of the tasks they conduct, *ie* AML/CTF tasks, result in the application of the Police Data Protection Directive (Mitsilegas *et al*, 2016; Art. 2[2][d] GDPR). However, such application leads to the watering down of data subjects' rights in terms of transparency, protection against further processing, data minimisation, and the necessity of data collecting and processing which, under such regulatory framework, is not limited to the necessary (Mouzakiti, 2020).

Respects the essence of the right. Limitations must not go so far that the right is adversely impacted through obstacles to its exercise (EDPS, 2017[a]). It is what Mitsilegas (2015, p. 52) defines as "procedural justice". While CJEU case-law is not abundant in this regard, it is settled that individuals must be provided with access to data and legal remedies to access, rectify or erase it (Maximillian Schrems v Data Protection…, §95). As to the prohibition of STR disclosure and access to personal data of the customer concerned (Arts. 39[1]; 41[4]), MSs will have to specify their options providing for *inter alia* maximum time limits as a data subject cannot be eternally refused access to his/her personal data. Indeed, a clear legal basis "must itself define the scope of the limitation on the exercise of the right concerned" whilst defining minimum safeguards (Data Protection Commissioner/ Maximillian…, §§175; 180) *inter alia* to avoid the risk of abuse and unlawful use and access to data (Digital Rights Ireland/ Minister…, §54). Guidelines on the necessity and proportionality of such restrictions of access should have been provided (Mitsilegas *et al*, 2016). Basic rights such as recourse to the national data protection authorities to verify access, corrections or erasure of data, as well as the right to lodge judicial procedures should be granted to data subjects (Kariņš et al, 2014). In fact, it is somehow odd that Arts. 30(5)(c) and 31(4)(c) provides the general public and to who demonstrates a legitimate interest, wide access to at least information on BO name, month and year of birth, residence country, nationality and nature of the

interest held; whilst at the same time the 5AMLD provides wide discretion to refuse data subjects access to their own data provided that such limitation is "necessary and proportionate", to avoid NCAs and CSPs' tasks and investigations obstructions (Art. 41[4]).

The CJEU considered that as long as the content of electronic communications was not uncovered, the right to privacy was not irreversibly violated (Digital Rights Ireland, §39) – in the sense that metadata, *ie* data about data, does not amount to actual content (EDPS, 2019). In financial transactions, however, content assumes another configuration. It might provide "unprecedented insight into human behaviour, private life and our societies" (EP, 2017, §C). It can reveal *inter alia* the sender's and recipient's racial or ethnic origin, religious beliefs or trade-union membership (Tzanou, 2017) as well as "location, social networks, gender, sexual orientation, political views or medical history" (Paesano, 2019, p. 5). Therefore, basic guarantees must be afforded to data subjects for their rights not to be fully emptied, namely access to actual content of data only being granted on a scheme similar to the one provided by Ma^{3}tch.

Necessity and proportionality. The necessity requirement establishes that a restrictive measure is needed when no other available and less intrusive measures exist to achieve the same result – a strictly necessary measure (Data Protection Commissioner/Facebook Ireland Ltd and Maximillian Schrems, §176). The objective of 5AMLD and its importance is clearly identified: data is accessed and shared for the purposes of tackling TF (as codified in the Directive (EU) 2017/541) in terms of a public interest (Arts. 1[1]; 43). The EU legislator identifies the urgency and the level of threat by referring to recent terrorist attacks in the EU and the anonymity opportunities presented to terrorists to finance their causes in the shadows of modern technology services which were not covered by law (Recital 2). New measures were necessary to address the CC environment.

Yet, CDD must be limited to the strictly necessary as "general and indiscriminate [data] transmission exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society" (Privacy International, §81). Worryingly, Art. 55(1) continues to fail on the necessity principle as it does not specify to which entities FIUs may transmit data, whilst Mitsilegas *et al* (2016)

consider the conditions for such transmission very broad. Indeed, data transmission "must rely on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data at issue" (Privacy International, §78). Despite Art. 53(1)(§2) provides that information requests must be accompanied by its underlying motives, an in-depth categorization of criteria on such exchange should have been granted. In fact, a relationship "between the data which is to be transmitted and a threat to national security" should be established (Privacy International, §80).

Traceability tools to address P2P interactions are deemed suitable due to the inexistence of measures "to attain with comparable effectiveness the public security objective pursued" (Mengozzi, §214). However, it might be considered that public authorities have other tools at their disposal, namely access to publicly available blockchain data. Such kind of tool might be deemed as a less intrusive measure and can surely be taken. Yet, the CJEU acknowledged the importance of modern investigation tools to enhance "the effectiveness of the fight against serious crime, in particular […] terrorism", provided that such instruments do not provide for "general and indiscriminate" data retention (Tele2 Sverige AB/ Post-och telestyrelsen, §103). New traceability technological tools were welcomed as well by the EDPS (2020), where it complies with data protection-by-design and by-default. Thus, such traceability tools are necessary, which does not mean that they are proportional.

The *stricto sensu* proportionality test entails that disadvantages do not surpass the advantages and that a balance between means and objectives exists (EDPS, 2019). Although the 5AMLD intended to observe that principle, as well as the respect for privacy and personal data protection (Recitals 5; 51; EC, 2016[a]), five main privacy and data protection issues were stressed: (1) PPPs providing private entities access to operational data; (2) private entities lack of independency to be tasked with both commercial and AML/CTF activities; (3) FIUs shift to an intelligence-based approach and feedback on STRs; (4) FIUs organisational distortions; and (5) the 5-year data retention period.

The EDPS considers PPPs for exchange of patterns and trends information as positive; yet, transmission of operational data on suspects in that context is a

concern as it is not consistent with the proportionality principle. Private entities should never be "entrusted with an enforcement role" (EDPS, 2020, §42) as it entails monitoring persons that at the same time are their customers. CSPs are considered not to enjoy the required independence and autonomy to monitor their own customers due to confidentiality duties that regulate their business relationship (EDPS, 2020).

"Personal data shall be processed […] only for the *purposes of the prevention of money laundering and terrorist financing*" and that personal data "*shall not be further processed in a way that is incompatible with those purposes*" (Art. 41[2]; added emphasis). Hence, the "function creep" problem must be avoided, *ie* data initially collected for commercial reasons cannot be subverted to pursue different objectives namely to combat terrorism, "just because they are readily available" (Tzanou, 2017, p. 227). Customers must receive information on the exact purposes of the collection before conducting an occasional transaction or entering a business relationship, *ie* that commercial purposes (identification) and non-commercial purposes (AML/CTF rules) are at stake (Art. 41[3]; EDPS, 2020).

The shift towards a FIUs intelligence-based analysis (instead of the former STR-based analysis) was considered detrimental for data subjects (EDPS, 2020). That approach is "[more] similar to data mining than to a targeted investigation, with obvious consequences in terms of personal data protection" – thus, FIUs should be legally configurated as "'investigation-based' rather than 'intelligence-based'". (EDPS, 2020, §36). Such a configuration is more consistent with proportionality and purpose limitations principles (EDPS, 2020). Even though preventing terrorism is a justified objective, it is not an end in itself. Intrusive measures must be applicable "only in respect of persons with respect to whom there is a valid reason to suspect that they are involved in one way or another in terrorist activities" (La Quadrature du Net and others, §188). Thus, it is vital not to engage in data mining by pinpointing a risk against a pre-defined suspicion. It is necessary to shift to social network analysis, *ie* to draw possible outcomes by relating existent data (Wesseling *et al*, 2012). This approach is consistent with FATF's (2020[b]) risk categorization recommendation according to which where several red flags are identified, the existence of a criminal activity might be considered.

In addition, the EDPS (2020) considered that private entities should not receive feedback on the STRs they fill as access to intelligence information might be detrimental to individuals. Despite the merit of such consideration, the inexistence of such feedback does not grant CSPs the level of understanding of risks they need – *ie* understanding which transactions are indeed suspicious and which are not (EC, 2021[a]). The absence of feedback also prevents CSPs from completing STRs accurately, which might lead to false positives overreporting and to a poor RBA. In fact, only circa 10% of STRs are of use (EC, 2021[a]).

The purpose limitation principle is affected by FIUs organisational status distortions, as information management and sharing are conducted by interacting entities with heterogenous powers. Thus, FIUs share of information must be accompanied by proper technical and organisational measures to tackle such differences and avoid destruction, loss, modification, or disclosure of personal data. Those measures include encryption and anonymization (EDPS, 2020).

The 29WP (2011) considered that the 5-year period should start when data is collected and not when the business relationship reaches its end. The extension mechanism should be as short as possible and only renewed by FIUs and on very specific conditions. Subjective (analysis) data should not be retained for more than 5 years, whereas objective (operational) data should only be retained for more than 5 years when data remains accurate (29WP, 2011). Furthermore, the extension mechanism should have been designed in a way that its activation would only be allowed "after a careful assessment on a case-by-case basis" or according to defined guidelines (Mitsilegas *et al*, 2016, p. 281). The CJEU considered a 12-day retention period for cellphones' IMEI data proportional (Ministerio Fiscal, §§59-60). In cellphone theft cases, thieves readily use the stolen good or quickly want to sell it to another person. Nonetheless, such period is not consistent with TF nature. In TF, fundraising campaigns last for months or even years. Thus, the 5-year period is an effective measure, although the 29WP thoughts on the starting moment are worthy to be considered. Yet, in the case of "Ministerio Fiscal", IMEI data was considered not capable of giving access to specific human behaviour. The serious nature of the restrictive measure and of the objective should also be considered (La Quadrature du Net, §131). Financial data can reveal a lot of information on a person's way of living. Despite financial data does not amount to the special

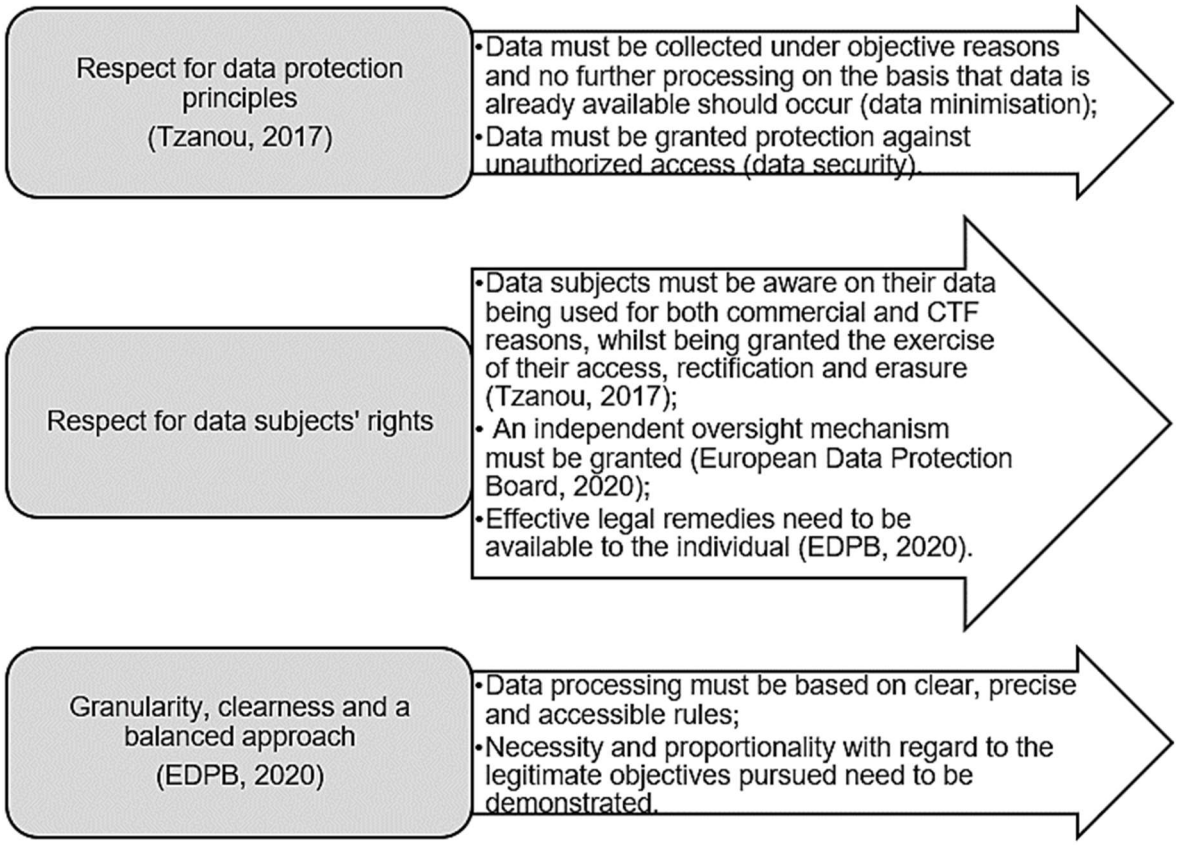
categories of personal data provided for in Art. 9(1) GDPR, the EDPS (2017[a]) argues that it can be considered as sensitive data. If one considers that data collection as a serious interference, it might be considered proportional, nonetheless, on the basis that its final objective is a serious one as well (La Quadrature du Net, §131; Tele2, §102). Even though a serious threat to national security is at stake, it is necessary to ensure that intrusive measures are not applied massively; where evidence suggests that a person might be linked to a terrorist activity, intrusion is allowed (La Quadrature du Net, §174). Additionally, safeguards must be granted to data subjects to exercise their rights. The CJEU noted that data retention measures must be accompanied by safeguards such as: geographical criteria to identify the public affected; notify data subjects after investigations opening, as soon as possible; and irreversibly destroy data after the 5-year retention period (Tele2, §§4-5, 120-122; La Quadrature du Net, §168).

AML/CTF measures were caught under other "heterogenous policy purposes". Whilst AML/CTF measures were deemed quite proportional, "measures that are acceptable to tackle the risk of terrorist attacks might result excessive when applied to prevent […] tax evasion" (EDPS, 2017[b], §49; §66, respectively). Therefore, CTF measures were, overall, appropriate. Certain conditions to access data would have been welcomed to guarantee proportionality; only LEAs should have been given the right to access data on BO; and processing should have been designed to occur according to defined, specific, and legitimate purposes (EDPS, 2017[b]). The RBA plays an important role on data protection issues. The more the risks to public security, the more intrusive procedures are justified (EDPS, 2020). Thus, the amount of data collected, stored and processed must be proportional to the risks (Finextra, 2016). The privacy-by-design principle is capable to balance the interests at stake. A balanced approach should be taken and "[s]ystematic data collection under CDD obligations should not be seen as a purpose in itself" (29WP, 2011, §4). Thus, the CDD should be adjusted to the risks posed, allowing for the optimisation of interferences.

Objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. It is important to assess whether the limitations on fundamental rights are justified considering the background against which the

measure is required. The EDPS (2017[a]) stressed that (1) privacy and data protection will give in before the general interest of fighting international terrorism and serious crime; and that (2) privacy and data protection rights will only be limited where general interest objectives are in place or where other persons' rights and freedoms are in danger. A strict connection between data and objective pursued must exist (La Quadrature du Net, §133). The EU legislator stressed in 5AMLD's Recitals 3, 5 and 7 that CTF rules are necessary to ensure internal security. The final aim of preventing, detecting and fighting TF is regarded as a serious goal (Ministerio Fiscal, §§56-57). However, an objective cannot be an end in itself; "legislation […] must also lay down the substantive and procedural conditions governing that use" (Privacy International, §77). More intrusive acts will be allowed where a serious threat to national security is "genuine and present or foreseeable", but such measures must be subject to court or independent administrative entity review (Privacy International, §192). Supervision on processing must in fact exist and be conducted by an independent entity (Tzanou, 2017).

Figure 8 - A three-fold approach to balance the security v. freedom clash.



Considering the analysis conducted on this subsection, and harvesting the EDPS (2017[b]) lessons, it can be concluded that, in general, the 5AMLD encompassed a balanced approach when it comes to the TF topic, considering the serious nature of the offense. Nevertheless, a core three-fold approach must be employed when this balance is hampered.

Final remarks. The EDPS (2017[b]) criticism is understandable as two different goals are at stake: on one hand, the EU CTF legislator favors transparency as much as possible due to security concerns; on the other hand, the EDPS is the privacy and data protection bastion, pushing into more and more anonymization (Quintais *et al*, 2019). TF prevention should not be confused with gathering proof of a crime; its legitimacy is completely different than the one which is found when investigating an actual offense (Nunes, 2018), as "[n]othing appears illegal except the future use of the money" (Tofangsaz, 2015, p. 122). The "genuine and present or foreseeable" criterion presented in the "La Quadrature du Net and others" case is a reminder that pre-emptive attitudes must be dealt with cautiously. It is pivotal to ensure that data collection, processing, and retention are not "undertaken pre-emptively in a probabilistic manner to uncover 'risky' individuals on the basis of algorithm processing and analysis of 'terrorist patterns'", but on "[actual] evidence of suspicion" (Tzanou, 2017, p. 252). The shift to a "forward-looking" attitude after the 9/11 events intends not only to fight terrorism, but to predict it (Mitsilegas, 2015, p. 36). Lack of data accuracy might lead to the base-rate fallacy, *ie* false positives, meaning that non-terrorists will be deemed as terror actors (29WP, 2011) – which contends with the presumption of innocence principle (Art. 48 EUCFR). It can also lead to a "suspect community" criterion, which may even fuel radicalization by a sense of discrimination. Nonetheless, the risk of negative positives, *ie* failing to safeguard that terrorists will be caught by data analysis, is a concern as well (29WP, 2011). As such, the EDPS (2019, p. 21) remarks that a fundamental rights approach should be pursued: the "privacy cost of the measure", namely discrimination, de-risking and financial exclusion, must be considered. Hence, such externalities must be addressed.

According to Weimann (s.d.), citizens must question themselves whether they give precedence to privacy over security from terrorist threats. It is in line with the old adage that says that "you can't have privacy without security, but you can have

security without privacy" (Bradley, 2019). However, combating TF should never be at expense of fundamental rights. What matters is not whether security or freedom should prevail, but how to strike a balance between them as "[e]very object can be used for good or evil, [which] merely depends on who is using it" (Chang *et al*, 2020, p. 5). Someone interested in protecting his financial life is not necessarily a criminal and public interest should not invalidate that right. A balanced approach is the one supporting security whilst not compromising EU values and freedoms, namely the principles laid down in Art. 3 TEU. Yet, the trade-off model, *ie* the systematic recourse to the notion of ''balancing'' wrongly suggests, according to Lieshout *et al* (2013), that privacy and security can only be enforced at each other's expense, while the obvious challenge is inventing a way to enforce both without loss on either side. The security/privacy clash must be replaced by a triangular relation where security, privacy and personal data protection coexist, whilst data protection plays a calibration role between security and privacy (EC, 2016[d]).

Terrorists' main goal is to threaten and shaken Western lifestyle. Nevertheless, it should not be permissible to create a culture of suspicion and fear when protecting the EU space from terror threats – as this would mean that terrorists succeed in demolishing fundamental values such as peace, human dignity, freedom and democracy. In fact, "[i]f privacy is regarded as a cornerstone of democracy, then scarifying privacy in the name of security undermines democracy itself" (Lieshout *et al*, 2013, p. 6). A new phenomenon emerges from large scale data collection and usage: "the disappearance of disappearance", *ie* it becomes more and more difficult for individuals to preserve their anonymity (Mitsilegas, 2015, p. 49). A clear general security interest exists, but CC adepts still raise the inevitable question: regulation is subtracting privacy from CC DNA, which is inevitably a paradox considering its creation purposes (Shubber, 2014). Wesseling *et al* (2012) stress that data anonymization must be considered – "'dots can be joined' in the absence of definitive named persons because link analysis and associated techniques *focus on the linking and not the dots*" (p. 62; added emphasis). Thus, EU citizens must live in a space that brings confidence in their future, freedom and security.

5.6. Next steps

Acknowledging the shortcomings present in the current AML/CTF framework, on July 20, 2021, the EU legislator proposed a new AML/CTF package comprised of four legislative proposals: (1) a Regulation establishing a new EU AML/CTF Authority; (2) a Regulation on AML/CTF; (3) a Directive on AML/CTF; and (4) a revised Regulation on transfers of funds[61]. The Regulation and a new minimum harmonisation Directive – which will repel and substitute the current one – were proposed to "carry out a structural reform of the rules with the aim to reduce the margins of interpretation that Member States have today" (EC, 2021ª, p. 29).

The Regulation will turn the list of obliged entities, CDD rules, reporting obligations, internal policies, controls and procedures and BO information directly applicable. A transposition process is not needed, which facilitates CSPs action across MSs by reducing compliance costs and creating a level playing field. The Directive will deal with FIUs and supervisors' tasks and cooperation (EC, 2021ª). The EC intends to impose time-limits on FIUs tasks and to clarify feedback obligations, in order enhance FIUs cooperation across the EU. The new proposal was drafted to better align the definitions of CCs and CSPs' activities with the FATF standards and to close the existing loopholes (EC, 2021ª). The proposed Regulation shall broaden the scope of CSPs covering: (1) custody and administration; (2) trading; (3) crypto-to-crypto and CC-to-fiat exchange; (4) execution of orders; (5) placing; (6) reception and transmission of orders; and (7) providing advice (EC, 2021ª). The Council (2020) urged the Commission to apply the travel rule to CSPs, to fully comply with FATF standards. The EC intends to address the lack of coherence between sectoral legislation by considering CCs as funds in the Regulation (EU) 2015/847. In addition, the EC intends to cover those activities and clarify its definitions, registration and licensing obligations. This will be achieved through an already proposed Regulation on Markets in Crypto-assets amending Directive (EU) 2019/193, a framework to be applied to AML/CTF rules using cross references (EC, 2021ª).

[61] Cf. COM(2021)420 final, COM(2021)421 final, COM(2021)422 final and COM(2021)423 final.

A proposed Regulation will create a new EU-level supervisor. The EU AML Authority (AMLA) will be responsible for defining technical standards on information exchange formats, explaining the characteristics of a proper RBA and setting the criteria to define the seriousness of risks and correspondent sanctions. It will coordinate MSs' supervisors to ensure that private actors apply EU rules in a correct and consistent manner. AMLA will also enhance FIUs coordination by establishing report and information exchange standards, supporting joint analysis and hosting FIU.net (EC, 2021[a]).

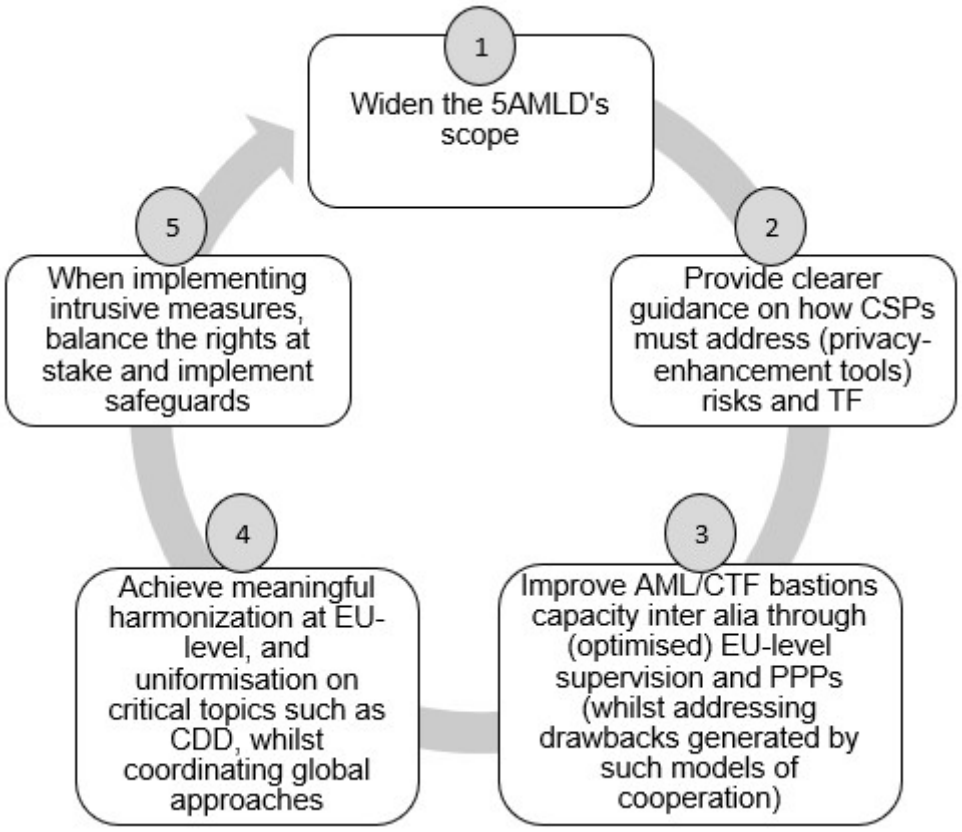
According to this new proposal, the anonymous wallets will be prohibited (EC, 2021[c]). However, the term "anonymous wallets" raises doubts. The EU legislator might be referring to non-custodian wallets, as it is not currently covered by the 5AMLD; but such designation might also refer to AECs holders or privacy wallets which provide for in-wallet mixing. Despite this blurriness, such prohibition will entail, in practice, an imposition of CDD on CC users. In addition, this approach calls for a deeper reflection: will CSPs and their customers only be allowed to conduct CSP-to-CSP operations as transactions will only be permitted with CSP account holders? This "would mean creating a system where only approved parties can interact" which happens in the traditional financial environment (Paesano, 2019, p. 4). Against this backdrop, the EU legislator intends this AML/CTF package to be future proof (EC, 2021[a]).

5.7. Intermediary conclusions

"Which approaches can complement the 5AMLD's loopholes?"

This Section demonstrated how 5AMLD's shortcomings can be tackled. It is thus necessary to look beyond the legislative approach and adopt a multi-level approach to achieve a holistic and comprehensive infrastructure capable of tackling CC-related TF:

Figure 9 – Multi-level approach.



Before even considering widening the 5AMLD's scope, it should be ensured that all CSPs meet their registration obligation. Only that way such entities will enter the supervisory radar. The stricter approaches adopted by some MSs and third countries demonstrate the importance that national legislators attributed to some entities that the EU legislator did not in 2018. The new proposed regulatory package is going to address crypto-to-crypto exchanges and to prohibit anonymous wallets. The EU legislator identified that a stringent option was needed, not only by extending the regulatory scope, but also by promoting the solution of a (uniform) EU approach by means of a Regulation on critical aspects. This shall ensure that all

MSs cover the same entities and exploitable points are removed, whilst simplifying CSPs' compliance with law.

As CC activity entails a transfer of value, same as financial transactions, according to the ECB, CC transactions should be treated, at least, on equal grounds according to the principle of equality (Mersch, 2018; Meijer, 2021). However, the goal is to treat the two realities on the same terms, the sieve should not be tighter for CCs when risks are not higher in order not to hinder innovation. *A contrario*, when risks are higher, the sieve should be raised and in-depth regulation should be considered.

It is important to enhance public authorities' capacity to respond to CC-related TF in the legal vacuum. FIUs role in unregulated venues will be of utmost importance to "link the dots" on transfer of values where zero user information is collected. Public authorities are improving their skills in CC-oriented investigations (Keatinge *et al*, 2018). Nevertheless, capacity building is of key importance as every criminal use of CC is different (Europol, 2020[b]) and it might have a deterrent effect on terrorism supporters (Brill *et al*, 2014; Kethineni *et al*, 2019). On the other hand, it is also expected that criminals will become more sophisticated (Chainalysis, 2020). Thus, public entities will be confronted with a never-ending learning process. PPPs are expected to play an important role whilst drawbacks generated by such models of cooperation must be addressed. Blockchain analysis companies are important to neutralize the tendency of illicit actors adapting "to these technologies faster than law enforcement can adjust" (Keatinge *et al*, 2018, p. 64). The 2020 dismantlement of CC-related TF demonstrates that allying blockchain analytics with diligent investigations by LEAs is the core of an efficient response to the phenomena (CipherTrace, 2021). Public authorities should also guide CSPs in the process of identifying TF by providing feedback on their STRs so they can produce more targeted reports, and drafting risk categorization tools for CSPs to adapt their approaches.

Modern terrorists rely on a global network. Thus, counteraction needs to attain a (coordinated) global reach (Barone, 2018[a]) to achieve group immunity (Norton *et al*, 2016). In the absence of such an approach, regulatory arbitrage will always be a very likely risk. In addition, HRTCs must be seen not only as a risk factor, but also as a means of cooperation, both in terms of providing guidance on how they can

improve their regulatory systems and practices and on ensuring exchange of information (Caiola, 2017).

EU citizens are also a central actor in the CC-TF scenario by using Internet in a diligent manner and reporting suspicious activity, as this can prevent CC from ending up in the hands of terrorists. Countering terrorist propaganda, monitorization of social media and Dark Web to prevent indoctrination and calls for funds was highlighted as well (Barone, 2018[a]; Europol, 2020[g]).

Inevitable privacy-security dilemmas are posed by the solutions presented above. The EDPS (2017[b]) criticized the 5AMLD's privacy and data protection tools, and particularly its proportionality design – stressing, though, at the same time its importance and suitability considering the serious nature of CTF. Yet, monitorization by private actors was considered to doubtfully comply with proportionality and necessity principles, less intrusive options to achieve the CTF goals being welcomed (EDPS, 2020). Nevertheless, identification and cross-check information systems on CC users are also important, even if its legal feasibility is achieved at CSP level only. As such, traceability mechanisms should be properly designed *inter alia* by means of legislation that provides for clear and sufficient legal grounds to interfere with fundamental rights (Rueckert, 2019) as well as GDPR hardcore principles of data minimisation, proportionality, privacy-by-design and by-default. It is crucial that CTF does not impinge upon human rights in impermissible ways; the proportionality principle is of prime importance; the EUCFR constitutes primary law, and as such the 5AMLD should fully comply with it (Caiola, 2017). Hence, the EU should be a bastion on international fora not only on AML/CTF topics, but also regarding the data protection and privacy (EC, 2016[a]).

CONCLUSION

Having discussed the CC use for terrorist purposes and critically analysed EU's approach to it in the light of the 5AMLD, the core question of the present thesis: *"Is the EU CTF legal framework able to tackle CC fundraising campaigns?"* is to be re-addressed.

Section III analysed CC-related TF empirical data. It was concluded that, albeit it is not clear how these methods to collect funds become effective, terrorists keep calling for CC and more organisations adhering to this *modus operandi* demonstrate that it is a convenient method to raise funds. CC might be deemed as a backup financial plan. "Cash might still be king", but it appears that the CC "could quickly become a kind of queen" (Smith, 2019ª). More terrorist organisations are expected to adopt CCs fundraising schemes and to employ even more privacy enhancement tools (Chainalysis, 2020). CCs' anonymity is a subterfuge for terrorists and renders the new mechanisms of prevention and detection obsolete (Europol, 2020ª). AQB fundraising stressed how terrorists are improving their skills on CC and engaging in more complex fundraising campaigns to escape detection (Keatinge *et al*, 2018). CTF is presented with more challenges when the so-called lone wolves and their attacks do not need major funding; such smaller amounts cannot be easily traced (Keatinge *et al*, 2018). Thus, CC fundraising campaigns existence should not be deemed as anecdotal evidence. Acknowledging the danger is necessary to ensure that public authorities' tasks are taken seriously and that they are afforded with the necessary tools to conduct their important role.

Limitations of the EU's gatekeeper approach to the CC ecosystem were identified in *Section IV*. Intermediaries' regulation is not an optimal solution; however, it is the only possible way to cover, at least, some of the CC ecosystem whilst not interfering extensively with financial freedom and privacy. However, leaving crypto-to-crypto exchanges and non-custodian wallets outside the scope of the 5AMLD leads to an inefficient application of CTF controls (EC, 2021ª). The EU legislator's choice created two different ecosystems: a regulated and a non-regulated one that overlap and create a lure for illicit actors (Fanusie, 2018). As the genesis of CC lays on P2P transaction models, it is not surprising that the present legislative framework might originate a chilling-effect to the unregulated perimeter.

The development of a sound regulatory regime is more difficult when there is definitional uncertainty (Kfir, 2020). The quality of the EU AML/CTF is questionable (Basel Institute on Governance, 2020). The 5AMLD brought more complexity to the transposition process as it demanded changes on legislations that were being, or have recently been transposed by MSs, which might result in inconsistent approaches (Silva, 2019). The 5AMLD lack of clarity and blurred lines pose difficulties for all the CTF stakeholders, leading to different attitudes and hampering proper cooperation. Adoption of CCs and anonymization techniques is expected to grow. Public authorities' analysis will be impacted as they will have to filtrate much more information to pinpoint suspicious transactions (Europol, 2021[b]). As such, public entities must have the proper legal and practical tools to conduct their assessments. Legal blurriness also prevents CSPs from properly fulfilling their legal obligations. Different approaches by MSs results in a regulatory puzzle across the EU that is difficult for CSPs to comply with. It chills innovation and, in addition, leads CSPs to establish themselves in jurisdictions where the quality of CTF controls is questionable, creating more threats to the EU. Although the aim is to unleash innovation, CCs are increasingly interacting with the real world. As such, the approach towards their nefarious effects should be addressed in terms of depth of regulation (Meijer, 2021; Mersch, 2018). The approach adopted by FATF is more conservative or at least more ambitious than that of the EU legislator, as it covers crypto-to-crypto exchange. It inevitably leads states and EU MSs to adopt its standards, creating further different approaches, this time at both international and regional level. Therefore, it was concluded that certain critical topics must be addressed by means of a regulation at EU level, while further coordination is needed globally. Ensuring a robust global effort towards CC-related TF is of key importance as CTF frameworks "would only be as strong as the weakest link of nations" (Salami, 2017, p. 12). Due to the "elasticity of the threat" (Andreeva, 2019, p. 364) it is recognized that "regulations are aiming at a moving target" (Paesano, 2019, p. 2). As highlighted, decentralized ecosystems and criminality are expected to grow. Building a robust internal market would make it possible for the EU to consolidate its position and, perhaps, become a system that other states, including HRTCs, could duplicate. It is important to acknowledge that failure to regulate or overregulation of technological innovation such as CCs will inevitably be exploited

by nefarious actors (Kfir, 2020). Therefore, EU's next steps should be carefully thought.

Following the identification of the 5AMD's limitations, *Section V* introduced the reader to a multilateral response to tackle their adverse impact. Every stakeholder involved in the use of CC is expected to play its role. CSPs will play an important assistance position. Blockchain analysis companies are expected to provide guidance on what is happening in the CC environment and to fill the vacuum observed in this field by public authorities when navigating "in waters" that are still somehow unknown. However, whilst AML/CTF rules demand for greater transparency, in a datafied-world, privacy concerns inevitably arise. Thus, it is necessary to provide for clear rules for the CTF success, which will collaterally enhance EU citizens confidence in the future. A study carried out in the EU, through the PRISMS project, revealed that trust in public authorities entails a "positive correlation with citizens' support for a security practice" (EC, 2016[d], p. 20). Thus, it is important for the EU legislator to deal with 5AMLD's abstractness and to provide data subjects with adequate safeguards. In this way, public and private entities will fulfill their tasks in a more informed and harmonised way and ensure transparency when employing security tools. EU citizens confidence in the future means, most importantly, that CTF measures must be as efficient as possible to prevent devastating effects. In fact, terrorism impacted the global economy in $26,4 billion in 2019 and 63 countries recorded at least one death from terrorism in the same year (Institute for Economics & Peace, 2020). Recognizing the need for in-depth regulation and a more consistent approach, the EC proposed a new AML/CTF package in July 2021. Its importance is indisputable to respond to current insufficiencies. However, it seems that the EU is "chasing the damage".

The advent of new technologies has brought unquestionable benefits to the society. However, it also posed challenges requiring a proper answer by law. Legal experts are called not only to understand the problems posed by new technologies, but also the technology itself, and to design the most suitable solution, *ie* a solution that responds to the problem *in casu* without curtailing innovation. Therefore, support must be granted to the projects developing taxonomies in the field. In fact, one of the problems experienced during the analysis on CCs undertaken in the context of this thesis was, precisely, the use of many different concepts to describe

the very same realities, both from a legal and from an industrial perspective. Moreover, the next decentralization wave will significantly impact on counterterrorism actors, making it an area worthy of analysis by scholars, practitioners, policymakers, and public authorities (Whyte, 2019).

BIBLIOGRAPHY

ADELSTEIN, Jake - **Japan's Financial Regulator Is Pushing Crypto Exchanges To Drop 'Altcoins' Favored By Criminals** [Online]. Jersey: Forbes. [Access. 26 Dec. 2020] Available at https://www.forbes.com/sites/adelsteinjake/2018/04/30/japans-financial-regulator-is-pushing-crypto-exchanges-to-drop-altcoins-favored-by-criminals/?sh=1c379b561b8a.

AFOLABI, Muyiwa – Concept of Security. In "Readings in Intelligence and Security Studies". [S.l.]: Intelligence and Security Studies Programme, ABUAD, 2015. p. 1–11.

ALEXANDER, Harriet - **New York woman charged with sending $85,000 in Bitcoin to support Isil** [Online]. London: The Telegraph. [Access. 26 Dec. 2020] Available at https://www.telegraph.co.uk/news/2017/12/14/new-york-woman-charged-sending-85000-bitcoin-support-isil/

AL-RAYA FOUNDATION FOR MEDIA PRODUCTION – **The voice of jihad and Mujahideen in Jerusalem** [Online]. [S.l]: Al-Raya Foundation for Media Production. [Access. 18 Dec. 2020] Available at https://alraia.net/en/bitcoin-digital-currency/

ALWAN, Hiba Basim; KU-MAHAMUD, Ku Ruhana – Big data: definition, characteristics, life cycle, applications, and challenges. IOP Conference Series: Materials Science and Engineering. ISSN 1757-899X. 769 (2020) 1-8.

ANDREEVA, Christine – "Europe wasn't ready'—'but it has proven that it's adaptable". ERA Forum. ISSN 1863-9038. 20:3 (2020) 343–370.

ARTICLE 29 DATA PROTECTION WORKING PARTY – Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing. Adopted on 13 Jun. 2011.

AP NEWS – **French arrest 29 in cryptocurrency scheme to finance jihadis** [Online]. New York: AP NEWS [Access. 21 Apr. 2021] Available at https://apnews.com/article/arrests-terrorism-archive-france-701371a367d1ae26ff057d6e3d082458

AZANI, Eitan [et al.] – Cyber-Terrorism Activities. Israel: International Institute for Counter Terrorism, 2013 (Report No. 6).

AZANI, Eitan; LIV, Nadine - Jihadists' Use of Virtual Currency. Israel: International Institute for Counter-Terrorism, 2018.

BANK FOR INTERNATIONAL SETTLEMENTS. BROEDERS, Dirk; PRENIO, Jeremy – "FSI Insights on policy implementation No 9: Innovative technology in financial supervision (suptech) - the experience of early users". 2018.

BARONE, Maria

_____(2018[a]) Jihadists' use of cryptocurrencies: undetectable ways to finance terrorism. Sicurezza, Terrorismo e Società. Nternational Journal Italian Team for Security, J Terroristic Issues & Managing Emergencies. ISSN 2533-0659. 8:2/2018 (2018) 17-59.

_____(2018[b]) - **Jihad as a Business Segment: the Malhama Tactical Team – by Daniele Maria Barone** [Online]. Milan: Itstime. [Access. 26 Dec. 2020] Available at https://www.itstime.it/w/jihad-as-a-business-segment-the-malhama-tactical-team-by-daniele-maria-barone/

_____(2019) - **Suspicious crowdfunding campaigns in bitcoin and their exploitation of exchange services – by Daniele Maria Barone** [Online]. Milan: Itstime. [Access. 19 Dec. 2020] Available at https://www.itstime.it/w/suspicious-crowdfunding-campaigns-in-bitcoin-and-their-exploitation-of-exchange-services-by-daniele-maria-barone/

_____(2020) - **US multiagency operation dismantled part of al-Qaeda's cryptocurrency network. What we learned so far and what to expect – by Daniele M. Barone** [Online]. Milan: Itstime. [Access. 22 Dec. 2020] Available at https://www.itstime.it/w/us-multiagency-operation-dismantled-part-of-al-qaedas-cryptocurrency-network-what-we-learned-so-far-and-what-to-expect-by-daniele-m-barone/

BASEL INSTITUTE ON GOVERNANCE

_____"Basel AML Index: 9th Public Edition - Ranking money laundering and terrorist financing risks around the world". 2020.

_____Basel learn [Online]. Switzerland: Basel Institute on Governance. [Access. 9 Jan. 2021] Available at https://baselgovernance.org/basel-learn

BBB NEWS – **World's first Bitcoin ATM opens – and other tech news** [Online]. London: BBC News. [Access. 14 Nov. 2020] Available at: https://www.bbc.com/news/av/technology-24756030

BENTLEY, Alden – **Bitcoin rallies above $30,000 for first time** [Online]. London: Reuters. [Access. 2 Jan. 2021]. Available at https://www.reuters.com/article/cryto-currency-idUSKBN2970FF

BERNARDI, Simone D. Casadei – **Terrorist Use of Cryptocurrencies : A Blockchain Compliance White Paper**. [Online]. United Kingdom: Blockchain Consultus. [Access.23 Jun. 2021]. Available at: https://www.blockchainconsultus.io/wp-content/uploads/2019/08/3191-BCU-Crypto-Terrorist.pdf

BINANCE ACADEMY - **Coin Mixing and CoinJoins Explained** [Online]. [S.l]: Binance Academy. [Access. 5 Jan. 2021]. Available at https://academy.binance.com/en/articles/coin-mixing-and-coinjoins-explained

BITPAY

_____**Accept cryptocurrency payments from all over the world** [Online] Atlanta: Bitpay [Access. 17 Feb. 2021] Available at https://bitpay.com/online-payments/

_____ **Merchant Terms of Use** [Online] Atlanta: Bitpay [Access. 17 Feb. 2021] Available at https://bitpay.com/legal/terms-of-use/

BLOCKCHAIN AND VIRTUAL CURRENCIES WORKING GROUP - **Blockchain and virtual currencies Working Group Ethical Guidelines** [Online]. [S.l]: Blockchain and Virtual Currencies Working Group. [Access. 9 Jan. 2021]. Available at https://www.blockchainwg.eu/ethical-guidelines/

BLOCKCHAIN ALLIANCE – **Technology & Criminal Activity** [Online] New York: Blockchain Alliance [Access. 7 Jan. 2021] Available at https://blockchainalliance.org/wp-content/uploads/2018/07/blockchain-alliance-infographic.jpg

BLOCKONOMICS – **What is Blockonomics?** [Online] India: Blockonomics. [Access. 18 Dec. 2020] Available at https://www.blockonomics.co/docs/blockonomics-brochure.pdf

BOEMCKEN, Marc Von; SCHETTER, Conrad – **Security: What It Is? What Does It Do?** [Online]. Berlin: Friedrich Ebert Stiftung. [Access. 8 May. 2021]. Available at: http://library.fes.de/pdf-files/iez/12368.pdf

BOIN, Arjen; SCHMIDT, Susanne K. - The European Court of Justice: Guardian of European Integration. In “Guardians of Public Value: How Public

Organisations Become and Remain Institutions". [S.l.] : palgrave macmillan, 2021. ISBN 978-3-030-51700-7. p. 135–159.

BRADLEY, Tony – **Finding The Right Balance Between Security And Privacy** [Online]. Jersey: Forbes. [Access. 28 Jul. 2021] Available at https://www.forbes.com/sites/tonybradley/2019/03/22/finding-the-right-balance-between-security-and-privacy/?sh=55c64ddf3889

BRILL, Alan; KEENE, Lonnie – Cryptocurrencies: The Next Generation of Terrorist Financing? Defence Against Terrorism Review. 6:1 (2014) 7–30.

CAIOLA, Antonio – The European Parliament and the Directive on combating terrorism. ERA Forum. 18 (2017) 409-424.

CAMPBELL-VERDUYN, Malcolm – Bitcoin, crypto-coins, and global anti-money laundering governance. Crime, Law and Social Change. ISSN 1573-0751. 69:2 (2018) 283–305.

CHAINALYSIS

_____The 2020 state of crypto crime : Everything you need to know about darknet markets, exchange hacks, money laundering and more. 2020

_____**Empowering you to answer questions about blockchains** [Online]. New York: Chainalysis. [Access. 10 Jan. 2021] Available at https://demo.chainalysis.com/request-a-demo/

CHANG, Victor [et al.] – How Blockchain can impact financial services - The overview, challenges and recommendations from expert interviewees. Technological Forecasting and Social Change. ISSN 0040-1625. 158 (2020).

CIPHERTRACE

_____(2020[a]) CipherTrace Geographic Risk Report: VASP KYC by Jurisdiction. California: CipherTrace, 2020.

_____ (2020[b]) **CipherTrace Files Two Monero Cryptocurrency Tracing Patents** [Online]. California: CipherTrace. [Access. 2 Dec. 2020] Available at https://ciphertrace.com/ciphertrace-files-two-monero-cryptocurrency-tracing-patents

_____(2020[c]) **CipherTrace Armada: Cryptocurrency Risk Controls for Banks** [Online]. California: CipherTrace. [Access. 3 Dec. 2020] Available at https://ciphertrace.com/wp-content/uploads/2020/12/CIPHERTRACE_DS-ARMADA-INSPECTOR-20201203.pdf

_____(2021) Cryptocurrency Crime and Anti-Money Laundering Report. California: CipherTrace, 2021.

COIN ATM RADAR – **Crypto ATM Distribution by Continents and Countries** [Online]. [S.l.] [Access. 07 Jun. 2021] Available at https://coinatmradar.com/charts/geo-distribution/

COIN MARKET CAP

_____**Coin Market Cap** [Online]. Delaware: Coin Market Cap. [Access. 26 Nov. 2019; 10 Oct. 2020; 14 Nov. 2020; 9 Sep. 2021] Available at https://coinmarketcap.com/

_____**Crypto Glossary** [Online]. Delaware: Coin Market Cap. [Access. 14 Nov. 2020] Available at https://coinmarketcap.com/alexandria/glossary.

_____**Top Cryptocurrency Spot Exchanges** [Online]. Delaware: Coin Market Cap. [Access. 12 Nov. 2020; 06 Jun. 2021] Available at https://coinmarketcap.com/rankings/exchanges/

_____**Crypto Payments: Similarities and Differences** [Online]. Delaware: Coin Market Cap. [Access. 17 Feb. 2021] Available at https://coinmarketcap.com/headlines/news/crypto-payment-gateways-similarities-and-differences/

_____**Zcash** [Online]. Delaware: Coin Market Cap. [Access. 8 Dec. 2020] Available at https://coinmarketcap.com/currencies/zcash/

COIN SHUFFLE – **Crypto Aggregator. Swap 2000+ crypto pairs instantly and directly into your wallet** [Online]. [S.l.]: Coin Shuffle. [Access. 9 Apr. 2021] Available at: https://coinshuffle.io

COMMITTEE OF MINISTERS OF THE COUNCIL OF EUROPE – "Declaration of the Committee of Ministers of the Council of Europe "United around our principles against violent extremism and radicalisation leading to terrorism". 2015, CM[2015]74-final.

COUNCIL OF EUROPE

_____COUNCIL OF EUROPE. MONEYVAL Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism – Report. «De-risking» within Moneyval states and territories, 2015.

COUNCIL OF EUROPE; EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS – **Handbook on European data protection law: 2018 Edition**. 2018 ed. Luxembourg: Publications Office of the European Union, 2018. ISBN 978-92-871-9849-5.

COUNCIL OF THE EUROPEAN UNION

_____"Outcome of the Council Meeting. 3364th Council Meeting, Foreign Affairs". 2015, 5411/15.

_____"Council Conclusions on strategic priorities on anti-money laundering and countering the financing of terrorism". 2019, 14823/19.

_____"Council Conclusions on anti-money laundering and countering the financing of terrorism". 2020, 12608/20.

_____"Council Decision (CFSP) 2021/1192 of 19 July 2021 updating the list of persons, groups and entities subject to Articles 2, 3 and 4 of Common Position 2001/931/CFSP on the application of specific measures to combat terrorism, and repealing Decision (CFSP) 2021/142". 2021.

CUTHBERTSON, Anthony – **Bitcoin trader brutally tortured with drill in cryptocurrency robbery** [Online]. London: Independent. [Access. 22 Dec. 2020] Available at https://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-robbery-torture-cryptocurrency-netherlands-a8807986.html

DASKALAKIS, Nikos; GEORGITSEAS, Panagiotis – **An Introduction to Cryptocurrencies. The Crypto Market Ecosystem.** 1st ed. London: Routledge, 2020. ISBN 978-0-429-35258-4.

DEEN, Thalif - **UN: defining terrorism** [Online]. Doha: Aljazeera. [Access. 24 Nov. 2020] Available at https://www.aljazeera.com/features/2010/11/24/un-defining-terrorism

DIMITRAKOPOULOS, Ioannis – **Conflicts between EU law and National Constitutional Law in the Field of Fundamental Rights**. [Online]. Brussels: European Judicial Training Network. [Access. 22 Jul. 2021] Available at https://www.ejtn.eu/PageFiles/17318/DIMITRAKOPOULOS%20Conflicts%20between%20EU%20law%20and%20National%20Constitutional%20Law.pdf

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.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

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.

DURNER, Tracey; COTTER, Danielle – "Combating Money Laundering and Terrorism Financing : Good Practices for AML/CFT Capacity Development Programs. AML/CFT Landscape". 2018.

EISERMANN, Daniel – **Cryptocurrencies as Threats to Public Security and Counter Terrorism: Risk Analysis and Regulatory Challenges**. Frankfurt: Berlin Risk, 2020.

ELLIPTIC - **Actionable Blockchain Insights for FIUs** [Online]. London: Elliptic. [Access. 7 Jan. 2021] Available at https://www.elliptic.co/customers/regulators

EU FIU PLATFORM – "32nd Meeting of the EU FIU Platform Minutes". 2017.

EUROPEAN CENTRAL BANK – **Virtual Currency Schemes**. 1st ed. Germany: European Central Bank, 2012. ISBN 978-92-899-0862-7.

EUROPEAN COMMISSION

_____"Proposal for a Directive of the European Parliament and of the Council on combating terrorism and replacing Council Framework Decision 2020/475/JHA on combating terrorism". 2015, COM(2015) 625 final.

_____(2016ª) "Communication from the Commission to the European Parliament and the Council on an Action Plan for strengthening the fight against terrorist financing". 2016, COM(2016) 50 final.

_____(2016[b]) “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”. 2016, COM(2016) 450 final.

_____(2016[c]) “Proposal for a Directive of the European Parliament and of the Council on countering money laundering by criminal law”. 2016, COM(2016) 826 final.

_____(2016[d]) Final Report Summary - PRISMS (The PRIvacy and Security MirrorS: “Towards a European framework for integrated decision making)”. Brussels: European Commission, 2016.

_____(2019) Report from the Commission to the European Parliament and the Council assessing the framework for cooperation between Financial Intelligence Units. Brussels: European Commission, 2019. (COM(2019) 371 final)

_____(2020[a]) “Communication from the Commission on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing”. 2020, 2020/C 164/06.

_____(2020[b]) “Commission Staff Working Document. Methodology for identifying high-risk third countries under Directive (EU) 2015/849”. 2020, SWD(2020) 99 final.

_____(2020[c]) **February infringements package: key decisions** [Online]. Brussels: European Commission. [Access. 5 May. 2021] Available at https://ec.europa.eu/commission/presscorner/detail/en/inf_20_202

_____(2021[a]) “Commission Staff Working Document. Impact Assessment Accompanying the Anti-money laundering package”. 2021, SWD(2021) 190 final.

_____(2021[b]) **Commission proposes a trusted and secure Digital Identity for all Europeans** [Online]. Brussels: European Commission. [Access. 11 Jul. 2021] Available at https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663

_____(2021[c]) **Beating financial crime: Commission overhauls anti-money laundering and countering the financing of terrorism rules** [Online]. Brussels: European Commission. [Access. 12 Aug. 2021] Available at https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3690

_____**Anti-money laundering directive V (AMLD V) – transposition status** [Online] Brussels: European Commission. [Access. 5 May. 2021] Available at https://ec.europa.eu/info/publications/anti-money-laundering-directive-5-transposition-status_en

EUROPEAN DATA PROTECTION BOARD – "Recommendations 02/2020 on the European Essential Guarantees for surveillance measures: Adopted on 10 November 2020", 2020.

EUROPEAN DATA PROTECTION SUPERVISOR

_____(2017[a]) "Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit". 2017.

_____(2017[b]) "Opinion 1/2017: EDPS Opinion on a Commission Proposal amending Directive (EU) 2015/849 and Directive 2009/101/EC: Access to beneficial ownership information and data protection implications". 2017

_____"EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data". 2019.

_____"Opinion 5/2020 on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing". 2020.

EUROPEAN PARLIAMENT

_____"Fundamental rights implications of big data: European Parliament resolution of 14 March 2017 on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement (2016/2225(INI))". 2017, 2018/C 263/10.

_____EUROPEAN PARLIAMENT. Ferber [et. al] – "Motion for a Resolution to wind up the debate on the statements by the Council and the Commission pursuant to Rule 132(2) of the Rules of Procedure on a comprehensive Union policy on preventing money laundering and terrorist financing – the Commission's Action Plan and other recent developments". 2020, PE647.704v01-00.

EUROPEAN PARLIAMENT. KARIŅŠ, Krišjānis; SARGENTINI, Judith – Report on the proposal for a directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of

money laundering and terrorist financing. Brussels: European Parliament. 2014, PE523.003v02-00.

_____EUROPEAN PARLIAMENT. Policy Department for Citizens' Rights and Constitutional Affairs. KEATINGE, Tom; CARLISLE, David; KEEN, Florence – "Virtual Currencies and terrorist financing: assessing the risks and evaluating responses". 2018, PE 604.970.

_____EUROPEAN PARLIAMENT. PARENTI, Radostina – "Regulatory Sandboxes and Innovation Hubs for FinTech: Impact on innovation, financial stability and supervisory convergence". 2020, PE 652.752.

EUROPEAN PPP EXPERTISE CENTRE – "PPP Motivations and Challenges for the Public Sector: Why (not) and how". 2015.

EUROPOL

_____(2016) - **Money Laundering with Digital Currencies: Working group established** [Online]. Netherlands: Europol. [Access. 22 Out. 2020] Available at https://www.europol.europa.eu/newsroom/news/money-laundering-digital-currencies-working-group-established

_____Do criminals dream of electric sheep? How technology shapes the future of crime and law enforcement. The Netherlands: European Union Agency for Law Enforcement Cooperation, 2019.

_____(2020[a]) Internet Organised Crime Threat Assessment 2020. The Netherlands: European Union Agency for Law Enforcement Cooperation, 2020.

_____(2020[b]) "Recommendations: 4th Global Conference on Criminal Finances and Cryptocurrencies". 2020.

_____(2020[c]) European Union Terrorism Situation and Trend Report 2020. The Netherlands: European Union Agency for Law Enforcement Cooperation, 2020.

_____(2020[e]) **Two arrests in Spain for terrorist financing** [Online]. Netherlands: Europol. [Access. 22 Out. 2020] Available at https://www.europol.europa.eu/newsroom/news/two-arrests-in-spain-for-terrorist-financing

_____(2020[f]) **Game on for Europol and Centric** [Online]. Netherlands: Europol. [Access. 12 Feb. 2020] Available at

https://www.europol.europa.eu/newsroom/news/game-for-europol-and-centric

_____(2020[g]) **Virtual tabletop exercise coordinated by Europol: Disrupting terrorism and violent extremism online** [Online]. Netherlands: Europol. [Access. 22 Dec. 2020] Available at https://www.europol.europa.eu/newsroom/news/virtual-tabletop-exercise-coordinated-europol-disrupting-terrorism-and-violent-extremism-online

_____(2020[h]) **422 arrested and 4031 money mules identified in global crackdown on money laundering** [Online]. Netherlands: Europol. [Access. 22 Dec. 2020] Available at https://www.europol.europa.eu/newsroom/news/422-arrested-and-4%C2%A0031-money-mules-identified-in-global-crackdown-money-laundering

_____(2021[a]) European Union Terrorism Situation and Trend Report 2021. The Netherlands: European Union Agency for Law Enforcement Cooperation, 2021.

_____(2021[b]) European Union Serious and Organised Crime Threat Assessment. A corrupting influence: The infiltration and undermining of Europe's Economy and Society by Organised Crime. The Netherlands: European Union Agency for Law Enforcement Cooperation, 2021.

EUROSTAT - **Individuals' level of digital skills** [Online]. Luxembourg: Eurostat. [Access. 10 Jan. 2021] Available at https://ec.europa.eu/eurostat/databrowser/view/isoc_sk_dskl_i/default/bar?lang=eu

FADILPAŠIĆ, Sead; ŽEMAITIS, Eimantas - **ISIS Affiliated News Site Stops Accepting Bitcoin, Moves To Monero** [Online]. Vilnius: Cryptonews. [Access. 21 Dec. 2020] Available at https://cryptonews.com/news/isis-affiliated-news-site-stops-accepting-bitcoin-moves-to-m-6949.htm

FANUSIE, Yaya - **The New Frontier in Terror Fundraising: Bitcoin.** [Online]. Atlanta: The Cipher Brief. [Access. 7 Jan. 2021] Available at https://www.thecipherbrief.com/column_article/the-new-frontier-in-terror-fundraising-bitcoin

_____(2018) **Good Crypto, Bad Crypto: Blockchain Projects Gaining Legitimacy While Spawning An Underground** [Online]. Jersey: Forbes. [Access. 25 Jan. 2021] Available at

https://www.forbes.com/sites/yayafanusie/2018/07/12/good-crypto-bad-crypto-blockchain-projects-gaining-legitimacy-while-spawning-an-underground/?sh=6fe6c6981078

_____(2019) **Hamas Military Wing Crowdfunding Bitcoin** [Online]. Jersey: Forbes. [Access. 25 Jan. 2021] Available at https://www.forbes.com/sites/yayafanusie/2019/02/04/hamas-military-wing-crowdfunding-bitcoin/?sh=6f686dc24d7f

FIGUEIREDO, Guilherme – "Parecer da Ordem dos Advogados: Altera a Lei de Combate ao Terrorismo, transpondo a Diretiva (EU) 2017/541". 2018.

FINANCIAL ACTION TASK FORCE

_____FATF Report. Virtual currencies: Key Definitions and Potential AML/CFT Risks. France: Financial Action Task Force, 2014.

_____"Guidance for a Risk-Based Approach: Virtual Currencies". 2015.

_____"FATF Guidance: Criminalising Terrorist Financing (Recommendation 5)". 2016.

_____"Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers". 2019.

_____FATF Report: Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing**.** France: Financial Action Task Force, 2020.

_____(2021[a]) "Draft updated Guidance for a risk-based approach to virtual assets and VASPs". 2021.

_____(2021[b]) "Risk-Based Supervision". 2021.

_____(2021[c]) **Jurisdictions under Increased Monitoring - June 2021** [Online]. Paris: FAFT. [Access. 7 Sep. 2021] Available at https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-june-2021.html

_____(2021[d]) **High-Risk Jurisdictions subject to a Call for Action - June 2021** [Online]. Paris: FAFT. [Access. 7 Sep. 2021] Available at https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-june-2021.html

FINEXTRA - **Money Laundering, Bitcoin and Blockchain: Anonymity, Transparency and Privacy are not Incompatible** [Online]. London: Finextra. [Access. 12 Dec. 2020] Available at

https://www.finextra.com/blogposting/12663/money-laundering-bitcoin-and-blockchain-anonymity-transparency-and-privacy-are-not-incompatible

FINMA - **FINMA Guidance 02/2019: Payments on the blockchain** [Online]. Bern: FINMA. [Access. 26 Jan. 2021] Available at https://www.finma.ch/en/news/2019/08/20190826-mm-kryptogwg/

FINTECH FUTURES - **Will regulation be a blessing or a blow for Bitcoin?** [Online]. London: Fintech Futures. [Access. 24 Aug. 2021] Available at https://www.fintechfutures.com/2016/04/will-the-4th-aml-directive-be-a-blessing-or-a-blow-for-bitcoin/

FLOOD, John; ROBB, Lachlan – Trust, Anarcho-Capitalism, Blockchain and Initial Coin Offerings. SSRN Electronic Journal. (2017).

FREEMAN, Michael; RUEHSEN, Moyara – Terrorism Financing Methods: An Overview. Perspectives on Terrorism. 4:7 (2013) 5–26.

FRICK, Thomas A. – Virtual and cryptocurrencies - regulatory and anti-money laundering approaches in the European Union and in Switzerland. ERA Forum. 20 (2019). 99–112.

FUSTER, Gloria González - **The Emergence of Personal Data as a Fundamental Right of the EU**. 1st. ed. London: Springer, 2014. (Law, Governance and Technology Series). ISBN 978-3-319-05022-5.

GALAXY DIGITAL RESEARCH – Taproot & Schnorr: Scalability and Privacy Upgrades for Bitcoin [Online]. New York: Galaxy Digital Research. [Access. 5 Jan. 2021] Available at https://medium.com/galaxy-digital-research/taproot-schnorr-scalability-and-privacy-upgrades-for-bitcoin-e81b0df9101b.

GOLDMAN, Zachary K. [et al.] – Terrorist Use of Virtual Currencies: Containing the Potential Threat. Washington DC: Center for a New American Security, 2017.

GOMÉZ, Juan – A Financial Profile of the Terrorism of Al-Qaeda and its Affiliates. Perspectives on Terrorism. 4:4 (2010) 3–27.

GRAUER, Kim; UPDEGRAVE, Henry – The 2021 Crypto Crime Report. New York: Chainalysis, 2021.

HABIB, Ridlwan - **Indonesia Tracks Online Funding of Terror Groups** [Online]. Washington DC: BenarNews. [Access. 23 Nov. 2020] Available at

https://www.benarnews.org/english/news/indonesian/online-payments-01092017155456.html

HARSONO, Hugh – Prioritizing SOF Counter-Threat Financing Efforts in the Digital Domain. The Cyber Defense Review. 5:3 (2020) pp- 153-160.

HARVEY, Campbell R. - Bitcoin Myths and Facts. New York: Social Science Research Network, 2014 (Report No. 2479670).

HASBI, Ahmad Helmi; MAHZAM, Remy – Cryptocurrencies: Potential For Terror Financing?. S. Rajaratnam School of International Studies. 075 (2018).

HIGBEE, Aaron – The role of crypto-currency in cybercrime. Computer Fraud & Security. ISSN 1361-3723. 2018:7 (2018) 13–15.

HIGGINS, M. G. – **Cryptocurrency**. 1st ed. California: Saddleback Educational Publishing, 2018. ISBN 978-1-63078-475-1.

HOUBEN, Robby; SNYERS, Alexander – Cryptoassets and financial crime: a European Union perspective. In "The Routledge Handbook of FinTech". New York: Routledge, 2021. ISBN 978-1-00-037573-2.Chapter 11.

INSTITUTE FOR ECONOMICS & PEACE – Global Terrorism Index 2020: Measuring the Impact of Terrorism. Sydney: Institute for Economics & Peace, 2020.

INTERNATIONAL COMMISSION OF JURISTS. DUFFY, Helen; PILLAY, Róisín; BABICKÁ, Karolína – "Counter-Terrorism and Human Rights in the Courts : Guidance for Judges, Prosecutors and Lawyers on Application of EU Directive 2017/541 on Combatting Terrorism". 2020.

INTERNATIONAL INSTITUTE FOR COUNTER-TERRORISM – Cyber Report # 3: April – June 2019. Israel: International Institute for Counter-Terrorism, 2019 (Report No. 3).

INTERNATIONAL MONETARY FUND – **Financial Intelligence Units: An Overview**. 1st. ed. Washington DC: International Monetary Fund, 2004. ISBN 1-58906-349-X.

INTERNATIONAL MONETARY FUND. HE, Dong [et al.] – "Virtual Currencies and Beyond: Initial Considerations". 2016.

INTERPOL – Darknet and Cryptocurrencies [Online]. France: Interpol [Access. 12 Feb. 2021] Available at https://www.interpol.int/How-we-work/Innovation/Darknet-and-Cryptocurrencies

IRWIN, Angela S. M.; MILAD, George – The use of crypto-currencies in funding violent jihad. Journal of Money Laundering Control. ISSN 1368-5201. 19:4 (2016) 407–425.

Judgement of 16 July 2020, Data Protection Commissioner/Facebook Ireland Ltd and Maximillian Schrems, C-311/18, EU:C:2020:559.

Judgement of 8 April 2014, Digital Rights Ireland/Minister for Communications, Marine and Natural Resources and others., C-293/12, EU:C:2014:238.

Judgement of 10 September 2020, Hamas/Council of the European Union, C-386/19, P EU:C:2020:691.

Judgement of 6 October 2020, La Quadrature du Net and others/Prime Minister and others, C-511/18 and C-512/18, EU:C:2020:791.

Judgement of 6 October 2015, Maximillian Schrems/Data Protection Commissioner, C-362/14, EU:C:2015:650.

Judgement of 2 October 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788.

Judgement of 6 October 2020, Privacy International v Secretary of State for Foreign and Commonwealth Affairs and others, C-623/17, EU:C:2020:790.

Judgement of 21 December 206, Tele2 Sverige AB/Post-och telestyrelsen, C-203/15, EU:C:2016:970.

KARLSTRØM, Henrik – Do libertarians dream of electric coins? The material embeddedness of Bitcoin. Distinktion: Scandinavian Journal of Social Theory. ISSN 2159-9149. 15:1 (2014) 23–36.

KETHINENI, Sesha; CAO, Ying – The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. International Criminal Justice Review. ISSN 1057-5677. 30:3 (2020) 325–344.

KFIR, Isaac – Cryptocurrencies, national security, crime and terrorism. Comparative Strategy. ISSN 0149-5933. 39:2 (2020) 113–127.

KOERHUIS, Wiebe; KECHADI, Tahar; LE-KHAC, Nhien-An – Forensic analysis of privacy-oriented cryptocurrencies. Forensic Science International: Digital Investigation. ISSN 2666-2817. 33 (2020) 1-11.

KOH, Jae-Myong - **Suppressing Terrorist Financing and Money Laundering**. 1st ed. Berlin: Springer Science & Business Media, 2006. ISBN 978-3-540-32519-2.

KRPT3IA

_____**Bitcoin wa Sadaqat al-Jihad: Bitcoin and the Charity of Violent Physical Struggle** [Online] [S.l]: Krpt3ia. [Access. 30 Nov. 2020] Available at https://krypt3ia.files.wordpress.com/2014/07/btcedit-21.pdf

_____**SADAQACOINS** [Online] [S.l.]: Krpt3ia. [Access. 15 Dec. 2020] Available at https://krypt3ia.files.wordpress.com/2018/08/screenshot-from-2018-08-27-08-57-31.png

LANGRIDGE, Stuart - **Is Cryptocurrency Anonymous?** [Online]. Delaware: Coin Market Cap. [Access. 23 Nov. 2020] Available at https://coinmarketcap.com/alexandria/article/is-cryptocurrency-anonymous

LANNOO, Karel; PARLOUR, Richard – **Anti-Money Laundering in the EU: Time to get serious**. 1st ed. Brussels: Centre for European Policy Studies, 2021. ISBN 978-94-6138-782-0.

Law No. 58/2020, which transposes 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 purpose of money laundering or terrorist financing and Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by means of criminal law, amending several laws

LAWDER, David - **IMF's Lagarde says cooperation needed to keep crypto-assets safe** [Online]. London: Reuters. [Acces. 12 Aug. 2021]. Available at https://www.reuters.com/article/us-g20-imf-cryptocurrencies/imfs-lagarde-says-cooperation-needed-to-keep-crypto-assets-safe-idINKCN1GP1SX

LIELACHER, Alex - **Hot Wallets vs Cold Wallets: What's the Difference?** [Online]. Delaware: Coin Market Cap. [Access. 19 Nov. 2020] Available at https://coinmarketcap.com/alexandria/article/hot-wallets-vs-cold-wallets-whats-the-difference

LIESHOUT, Marc *et al.* – Reconciling privacy and security. Innovation: The European Journal of Social Science Research. ISSN 1469-8412. 26:1-2 (2013) 119–132.

LIV, Nadine - Jihadists' Use of Virtual Currency 2. Israel: International Institute for Counter-Terrorism, 2019.

MABUNDA, Sagwadi – Cryptocurrency: The New Face of Cyber Money Laundering. 2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD). (2018) 1-6.

MALIK, Nikita - **Terror in the Dark: How Terrorists use Encryption, the Darknet, and Cryptocurrencies**. 1st ed. London: The Henry Jackson Society, 2018. ISBN 978-1-909035-45-4.

MEIJER, Carlo R. W. De - **Cryptocurrencies and Regulation: Towards a Balanced and Coordinated Approach** [Online]. London: Finextra. [Access. 21 Feb. 2021] Available at https://www.finextra.com/blogposting/19822/cryptocurrencies-and-regulation-towards-a-balanced-and-coordinated-approach

MEIR AMIT INTELLIGENCE AND TERRORISM INFORMATION CENTER

_____(2017) **Drive for Bitcoin donations on an ISIS-affiliated website** [Online]. Israel: The Meir Amit Intelligence and Terrorism Information Center. [Access. 23 Jan. 2021] Available at https://www.terrorism-info.org.il/en/drive-bitcoin-donations-isis-affiliated-website/

_____(2019[a]) **Drive for donations using Bitcoin on an ISIS-affiliated website** [Online]. Israel: The Meir Amit Intelligence and Terrorism Information Center. [Access. 7 Jan. 2021] Available at https://www.terrorism-info.org.il/en/drive-donations-using-bitcoin-isis-affiliated-website/

_____(2019[b]) **Funding Terrorism: ISIS raises funds through an affiliated website, using bitcoins** [Online]. Israel: The Meir Amit Intelligence and Terrorism Information Center. [Access. 3 Jan. 2021] Available at https://www.terrorism-info.org.il/en/funding-terrorism-isis-raises-funds-affiliated-website-using-bitcoins/

_____(2019[c]) **Funding terrorism: ISIS-affiliated website raises funds using the virtual currency Bitcoin** [Online]. Israel: The Meir Amit Intelligence and Terrorism Information Center. [Access. 23 Jan. 2021] Available at https://www.terrorism-info.org.il/en/funding-terrorism-isis-affiliated-website-raises-funds-using-virtual-currency-bitcoin/

_____(2019[d]) **Hamas and the Popular Resistance Committees called on their supporters to donate money using the virtual currency Bitcoin** [Online].

Israel: The Meir Amit Intelligence and Terrorism Information Center. [Access. 5 Jan. 2021] Available at https://www.terrorism-info.org.il/en/hamas-popular-resistance-committees-called-supporters-donate-money-using-virtual-currency-bitcoin/

_____(2019[e]) **Funding Terrorism: campaign of a jihadi organization operating in the Gaza Strip to raise funds in Bitcoin** [Online]. Israel: The Meir Amit Intelligence and Terrorism Information Center. [Access. 15 Dec. 2021] Available at https://www.terrorism-info.org.il/en/funding-terrorism-campaign-jihadi-organization-operating-gaza-strip-raise-funds-bitcoin/

_____(2019[f]) **Hamas once again calls on its supporters to donate to its military wing in Bitcoin** [Online]. Israel: The Meir Amit Intelligence and Terrorism Information Center. [Access. 3 Jan. 2021] Available at https://www.terrorism-info.org.il/en/hamas-calls-supporters-donate-military-wing-bitcoin/

_____(2020[a]) **Funding Terrorism: The al-Qaeda-affiliated Salafi Army of the Nation in Jerusalem, which operates in the Gaza Strip, recently renewed its Bitcoin fund-raising campaign** [Online]. Israel: The Meir Amit Intelligence and Terrorism Information Center. [Access. 12 Jan. 2021] Available at https://www.terrorism-info.org.il/en/funding-terrorism-al-qaeda-affiliated-salafi-army-nation-jerusalem-operates-gaza-strip-recently-renewed-bitcoin-fund-raising-campaign/

_____(2020[b]) **New Hamas Fundraising Campaign: Hamas' military wing began a new fundraising campaign about a month after the United States thwarted digital coin campaigns of Hamas, al-Qaeda and ISIS** [Online]. Israel: The Meir Amit Intelligence and Terrorism Information Center. [Access. 3 Jan. 2021] Available at https://www.terrorism-info.org.il/en/new-hamas-fundraising-campaign-hamas-military-wing-began-a-new-fundraising-campaign-about-a-month-after-the-united-states-thwarted-digital-coin-campaigns-of-hamas-al-qaeda-and-isis/

MENGOZZI, Paolo – Opinion of Advocate General Paolo Mengozzi of 8 September 2016, Opinion 1/15, EU:C:2016:656.

MERSCH - **Speech by Yves Mersch, Member of the Executive Board of the ECB, at the 39th meeting of the Governor's Club Bodrum, Turkey,14 May 2018** [Online]. Frankfurt: European Central Bank. [Access. 8 Feb. 2021] Available at https://www.ecb.europa.eu/press/key/date/2018/html/ecb.sp180514.en.html

MIDDLE EAST MEDIA RESEARCH INSTITUTE

_____(2019) **Pro-Jihad NYC Imam Who Encouraged Hatred Of Non-Muslims Discusses Cryptocurrency On Salafi Telegram Channel, Raises Money On Patreon** [Online]. Washington DC: MEMRI - Cyber Terrorism & Jihad Lab. [Access. 26 Dec. 2020] Available at https://www.memri.org/cjlab/pro-jihad-nyc-imam-who-encouraged-hatred-of-non-muslims-discusses-cryptocurrency-on-salafi-telegram-channel-raises-money-on-patreon

_____(2020[a]) **On Telegram, Syrian Jihadi Group Seeks Poster Designers, Video Producers, And Nasheed Singers** [Online]. Washington DC: MEMRI - Cyber Terrorism & Jihad Lab. [Access. 26 Dec. 2020] Available at https://www.memri.org/cjlab/telegram-syrian-jihadi-group-seeks-poster-designers-video-producers-and-nasheed-singers

_____(2020[b]) **Pro-Jihadi News Network Solicits Cryptocurrency Donations** [Online]. Washington DC: MEMRI - Cyber Terrorism & Jihad Lab. [Access. 26 Dec. 2020] Available at https://www.memri.org/cjlab/pro-jihadi-news-network-solicits-cryptocurrency-donations

MITSILEGAS, Valsamis – The Transformation of Privacy in an Era of Pre-emptive Surveillance. Tilburg Law Review. 20 (2015) 35–57.

MITSILEGAS, Valsamis; VAVOULA, Niovi – The Evolving EU Anti-Money Laundering Regime: Challenges for Fundamental Rights and the Rule of Law. Maastricht Journal of European and Comparative Law. 23:2 (2016) 261-293.

MÖSER, Malte *et al.* – An Empirical Analysis of Traceability in the Monero Blockchain. Proceedings on Privacy Enhancing Technologies. 2018:3 (2018) 143–163.

MOUZAKITI, Foivi – Cooperation between Financial Intelligence Units in the European Union: Stuck in the middle between the General Data Protection Regulation and the Police Data Protection Directive. New Journal of European Criminal Law. ISSN 2032-2844. 11:3 (2020) 351–374.

NAKAMOTO, Satoshi – **Bitcoin: A Peer-to-Peer Electronic Cash System** [Online]. Washington DC: Bitcoin Foundation. [Access. 18 Oct. 2019] Available at: https://bitcoin.org/bitcoin.pdf

NANCE, Mark T. – The regime that FATF built: an introduction to the Financial Action Task Force. Crime, Law and Social Change. ISSN 1573-0751. 69:2 (2018) 109–129.

NGUYEN, Duy - **Venezuela's Bitcoin Story Puts It in a Category of One** [Online]. New York: Coindesk. [Access. 11 Jan. 2021] Available at https://www.coindesk.com/business/2020/11/11/venezuelas-bitcoin-story-puts-it-in-a-category-of-one/

NANYUN, Nankpan Moses; NASIRI, Alireza – Role of FATF on financial systems of countries: successes and challenges. Journal of Money Laundering Control. ISSN 1368-5201. 24:2 (2020) 234–245.

NORTON, Simon; CHADDERTON, Paula – Special Report: Detect, disrupt and deny: Optimising Australia's counterterrorism financing system, 2016.

NUNES, Carlos Casimiro – **O atual regime de prevenção e repressão do branqueamento de capitais e do financiamento do terrorismo: perspetiva prática** [Online]. Lisbon: Centro de Estudos Judiciários. [Access. 23 Jun. 2021] Available at https://educast.fccn.pt/vod/clips/jmi8czvis?locale=pt

ØE, Saugmandsgaard – Opinion of Advocate General Saugmandsgaard Øe of 19 July 2016, on joined cases C-203/15 and C-698/15, EU:C:2016:572.

Organisation for Economic Co-operation and Development – **Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditors**. 1st ed. Paris: Organisation for Economic Co-operation and Development, 2019.

PAESANO, Federico

_____Working Paper 28: Regulating cryptocurrencies: challenges & considerations. Basel Institute on Governance working papers series. ISSN 2624-9650. (2019).

_____**Will new FinCEN rules drive cryptocurrency users underground?** [Online]. Switzerland: Basel Institute on Governance. [Access. 14 Jan. 2021] Available at https://baselgovernance.org/blog/will-new-fincen-rules-drive-cryptocurrency-users-underground

PAVLIDIS, Georgios – International regulation of virtual assets under FATF's new standards. Journal of Investment Compliance. ISSN 1528-5812. 21:1 (2020) 1–8.

POE, Ted; SHERMAN, Brad – **House of representatives, congress of the United States, October 25, 2018 (Letter to Pavel Durov, Founder and CEO, Telegram Messenger LLP)** [Online]. Washington DC: MEMRI - Cyber Terrorism & Jihad Lab. [Access. 27 Dec. 2021] Available at https://www.memri.org/pdf/20181025_Telegram_sherman-Poe.pdf

POLYDOR, Sylvia – Blockchain Evidence in Court Proceedings in China – A Comparative Study of Admissible Evidence in the Digital Age (as of June 4, 2019). Stanford Journal of Blockchain Law & Policy. (2020).

POPPER, Nathaniel - **Terrorists Turn to Bitcoin for Funding, and They're Learning Fast** [Online]. New York: New York Times. [Access. 1 Feb. 2021] Available at https://www.nytimes.com/2019/08/18/technology/terrorists-bitcoin.html

PORTUGUESE SECURITIES MARKET COMMISSION – **FinTech: New technologies and business models** [Online]. Lisbon: CMVM. [Access. 12 Feb. 2021] Available at https://www.cmvm.pt/en/Investor_area/fintech/Pages/atividadades-fintech.aspx

QUINTAIS, João Pedro [et al.] – Blockchain and the Law: A Critical Evaluation. Stanford Journal of Blockchain Law & Policy. 2:1 (2019) 1-26.

REBANE - **What is a Bitcoin Mixer (Tumbler)?** [Online]. London: Cryptalker. [Access. 23 Dec. 2020] Available at https://cryptalker.com/bitcoin-mixer/

RÉBÉ, Nathalie – **Counter-Terrorism Financing: International Best Practices and the Law**. 1st ed. The Netherlands: BRILL, 2019. ISBN 978-90-04-40967-5.

RIEGELNIG, David – **OpenVASP: An Open Protocol to Implement FATF's Travel Rule for Virtual Assets** [Online]. OpenVASP. [Access. 15 Feb. 2020] Available at https://www.openvasp.org/wp-content/uploads/2019/11/OpenVasp_Whitepaper.pdf

ROSE, Gregory – Terrorism Financing in Foreign Conflict Zones. Counter Terrorist Trends and Analyses. ISSN 2382-6444. 10:2 (2018) 11–16.

ROTHSTEIN, Adam – **The End of Money: The story of bitcoin, cryptocurrencies and the blockchain revolution.** 1st ed. Boston: Nicholas Brealey, 2017. ISBN 978-1-909035-45-4.

RUECKERT, Christian – Cryptocurrencies and fundamental rights. Journal of Cybersecurity. ISSN 2057-2085. 5:1 (2019) 1-12.

SALAMI, Iwa – Terrorism Financing with Virtual Currencies – Can Regulatory Technology Solutions Combat this? Studies in Conflict & Terrorism. ISSN 1521-0731. 41:12 (2017) 969–989.

SAMOURAI – **a bitcoin wallet for the streets** [Online]. [S.l.]: Samourai [Access. 9 Apr. 2021] Available at https://samouraiwallet.com

SANDERS IV, Lewis – **Bitcoin: Islamic State's online currency venture** [Online]. Germany: Deutsche Welle. [Access. 15 Aug. 2021] Available at https://www.dw.com/en/bitcoin-islamic-states-online-currency-venture/a-18724856

SATZGER, Helmut – The Harmonisation of Criminal Sanctions in the European Union: A New Approach. The European Criminal Law Associations' Forum. ISSN 1862-6947. 2 (2019) 115–119.

SEITZ, Justin - **Follow the Bitcoin With Python, BlockExplorer and Webhose.io** [Online]. Netherlands: Bellingcat. [Access. 10 Jan. 2021] Available at https://www.bellingcat.com/resources/2017/09/15/follow-bitcoin-python-blockexplorer-webhose-io/

SHEA, Kevin - **N.J. man who posted online about bombing Trump Tower admits hiding support for terror group** [Online]. London: NJ Advance Media. [Access. 19 Aug. 2021] Available at https://www.nj.com/somerset/2020/09/nj-man-who-posted-online-about-bombing-trump-tower-admits-hiding-support-for-terror-group.html

SHIN, Laura - **Why The Travel Rule Is One Of The Most Significant Regulations In Crypto** [Online]. California: Unchained. [Access. 12 Dec. 2020] Available at https://unchainedpodcast.com/why-the-travel-rule-is-one-of-the-most-significant-regulations-in-crypto/

SHUBBER, Kadhim - Hyper-Anonymising Bitcoin Service 'Dark Wallet' Launches Today [Online]. New York: Coindesk. [Access. 11 Jan. 2021] Available at https://www.coindesk.com/markets/2014/05/01/hyper-anonymising-bitcoin-service-dark-wallet-launches-today/

SIC - **Facebook multado em 5 mil milhões de euros no caso Cambridge Analytica** [Online]. Lisbon: Sociedade Independente de Comunicação. [Access. 11 Jan. 2021] Available at

https://sicnoticias.pt/especiais/cambridge-analytica/2019-07-13-Facebook-multado-em-5-mil-milhoes-de-euros-no-caso-Cambridge-Analytica

SILVA, Patrícia Godinho – Recent developments in EU legislation on anti-money laundering and terrorist financing. New Journal of European Criminal Law. ISSN 2032-2844. 10:1 (2019) 57–67.

SMITH, Breena

_____(2019[a]) **The Evolution Of Bitcoin In Terrorist Financing** [Online]. Netherlands: Bellingcat. [Access. 23 Dec. 2020] Available at https://www.bellingcat.com/news/2019/08/09/the-evolution-of-bitcoin-in-terrorist-financing/

_____(2019[b]) **How To Track Illegal Funding Campaigns Via Cryptocurrency** [Online]. Netherlands: Bellingcat. [Access. 23 Dec. 2020] Available at https://www.bellingcat.com/resources/how-tos/2019/03/26/how-to-track-illegal-funding-campaigns-via-cryptocurrency/

_____(2019[c]) **Tracking Illicit Transactions With Blockchain: A Guide, Featuring Mueller** [Online]. Netherlands: Bellingcat. [Access. 10 Jan. 2021] Available at https://www.bellingcat.com/resources/how-tos/2019/02/01/tracking-illicit-transactions-with-blockchain-a-guide-featuring-mueller/

STALINSKY, Steven - **MEMRI Executive Director In 'Washington Post' Op-Ed: The Cryptocurrency-Terrorism Connection Is Too Big To Ignore** [Online]. Washington DC: MEMRI - Cyber Terrorism & Jihad Lab. [Access. 26 Dec. 2020] Available at https://www.memri.org/cjlab/memri-executive-director-in-washington-post-op-ed-the-cryptocurrency-terrorism-connection-is-too-big-to-ignore

SYGNA BRIDGE - **Signa Bridge Report: FATF Recommendation 16 Technical Solution for Virtual Asset Transactions** [Online]. Taiwan: Sygna. [Access. 12 Dec. 2020] Available at https://www.sygna.io/wp-content/uploads/2020/05/Sygna-Bridge-Report-April-2020-English-1.pdf

TEICHMANN, Fabian Maximilian Johannes – Financing terrorism through cryptocurrencies – a danger for Europe? Journal of Money Laundering Control. ISSN 1368-5201. 21:4 (2018) 513–519.

THE SOUFAN CENTER – **IntelBrief: Emerging Terrorist Financing Threats and Trends** [Online]. New York: The Soufan Center [Access. 16 Aug. 2021] Available at: https://thesoufancenter.org/intelbrief-2021-march-12/

TIERNEY, Michael – Spotting the lone actor: combating lone wolf terrorism through financial investigations Journal of Financial Crime. ISSN: 1359-0790. 24:4 (2017) 637-642.

TITANIUM PROJECT – **TITANIUM: Tools for the Investigation of Transactions in Underground Markets** [Online] European Union: Titanium Project. [Access. 15 Feb. 2021] Available at https://www.titanium-project.eu.

TOFANGSAZ, Hamed – Rethinking terrorist financing; where does all this lead? Journal of Money Laundering Control. ISSN 1368-5201. 18:1 (2015) 112–130.

TSIKHILOV, Alexander – **Blockchain Basics**. 1st ed. London: Clink Street Publishing, 2020. ISBN 978-1-913340-91-9.

TURNER, Nicholas W – The Financial Action Task Force : International Regulatory Convergence Through Soft Law. NYLS Law Review. 59:3 (2015) 547-559.

TZANOU, Maria – **The Fundamental Right to Data Protection. Normative Value in the Context of Counter-Terrorism Surveillance**. 1st ed. Oregon: Bloomsbury, 2017. ISBN 978-1-50990-167-8.

UNITED NATIONS – **United Nations Security Council Consolidated List** [Online] New York: United Nations. [Access. 23 Jul. 2021] Available at https://scsanctions.un.org/7kpuben-all.html

UNITED NATIONS OFFICE ON DRUGS AND CRIME – **Cryptocurrencies: Welcome to the UNODC Cryptocurrencies Course!** [Online] New York: United Nations. [Access. 26 Oct. 2020] Available at http://gpml-crypto.org/modules/Crypto%20English/launch.html

UNITED STATES DEPARTMENT OF JUSTICE

_____(2015) **Virginia Man Sentenced to More Than 11 Years for Providing Material Support to ISIL** [Online]. Washington DC: Department of Justice. [Access. 26 Dec. 2020] Available at https://www.justice.gov/opa/pr/virginia-man-sentenced-more-11-years-providing-material-support-isil

_____(2017) **Long Island Woman Indicted for Bank Fraud and Money Laundering to Support Terrorists** [Online]. Washington DC: Department of

Justice. [Access. 26 Dec. 2020] Available at https://www.justice.gov/usao-edny/pr/long-island-woman-indicted-bank-fraud-and-money-laundering-support-terrorists

_____(2019) **Somerset County Man Charged With Attempts To Provide Material Support To Hamas, Making False Statements, And Making Threat Against Pro-Israel Supporters** [Online]. Washington DC: Department of Justice. [Access. 1 Feb. 2021] Available at https://www.justice.gov/usao-nj/pr/somerset-county-man-charged-attempts-provide-material-support-hamas-making-false

_____(2020) **Global Disruption of Three Terror Finance Cyber-Enabled Campaigns** [Online]. Washington DC: Department of Justice. [Access. 12 Dec. 2020] Available at https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns

UNITED STATES IMMIGRATION AND CUSTOMS ENFORCEMENT – **Global disruption of 3 terror finance cyber-enabled campaigns** [Online]. Washington DC: US Immigration and Customs Enforcement. [Access. 26 Nov. 2020]. Available at: https://www.ice.gov/news/releases/global-disruption-3-terror-finance-cyber-enabled-campaigns

UNITED STATES OF AMERICA/ 155 VIRTUAL CURRENCY ASSETS, 13 August 2020, District Court for the District of Columbia, Civil Action No. 20-cv-2228.

WASABI WALLET – **reclaim your privacy now** [Online] . [S.l.]: Wasabi wallet. [Access. 9 Apr. 2021]. Available at: https://wasabiwallet.io

WEIMANN, Gabriel – **Going Darker? The Challenge of Dark Net Terrorism.**

WEIMANN, Gabriel – Terrorist Migration to the Dark Web. Perspectives on Terrorism. ISSN 2334-3745. 10:3 (2016) 40-44.

WEISS, Martin – "Terrorist Financing: The 9/11 Commission Recommendation", 2005.

WERBACH, Kevin – Trust, But Verify: Why the Blockchain Needs the Law. Berkeley Tech. L.J. 489 (2018).

WESSELING, Mara; GOEDE, Marieke DE; AMOORE, Louise – Data Wars Beyond Surveillance. Journal of Cultural Economy. ISSN 1753-0350. 5:1 (2012) 49–66.

WHYTE, Christopher – Cryptoterrorism: Assessing the Utility of Blockchain Technologies for Terrorist Enterprise. Studies in Conflict & Terrorism. ISSN: 1521-0731. (2019) 1–24.

WORLD BANK GROUP – "Distributed Ledger Technology (DLT) and Blockchain. FinTech Note No. 1". 2017.

ZENKO, Micah - **Bitcoin for Bombs** [Online]. New York: Council on Foreign Relations. [Access. 8 Dec. 2020] Available at https://www.cfr.org/blog/bitcoin-bombs

ZUCKERMAN, Molly Jane - **Tweeter Beware! Bitcoin Scam Snares Kanye West, Elon Musk, CZ and More** [Online]. Delaware: Coin Market Cap Blog. [Access. 8 Dec. 2020] Available at https://blog.coinmarketcap.com/2020/07/16/tweeter-beware-bitcoin-scam-snares-kanye-west-elon-musk-cz-and-more/

ANNEXES

Figure 10 - Muneer calling for and legitimizing bitcoin.

MEMRI, 2019

Figure 11 - Calling for support for weaponry purchase.

Fanusie, 2016

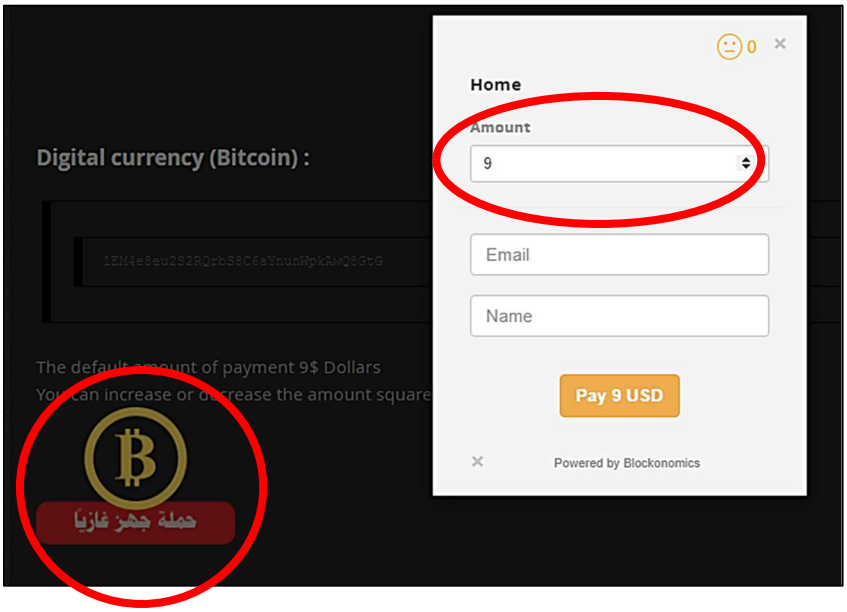
Figure 12 - Motives and reasons to contribute for the campaign presented in May 2020.

Available at https://alraia.net/en/motives-and-causes/, accessed on 18.12.2020.

Figure 13 - Intended weaponry purchase in May 2020.

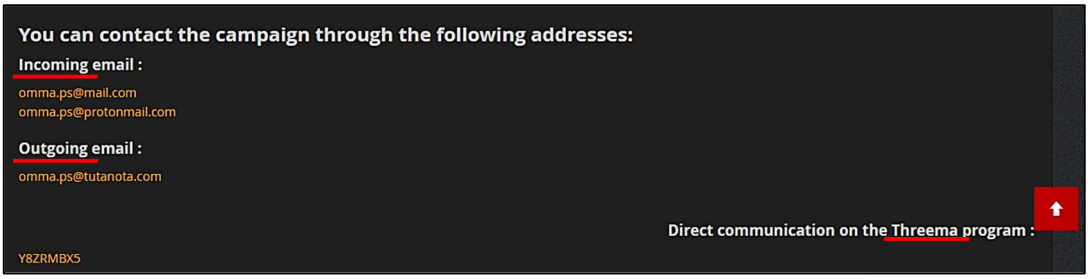
Available at https://alraia.net/en/anti-missile-and-anti-missile-prices/, accessed on 18.12.2020.

Figure 14 – Click-button to transfer funds and default amount.



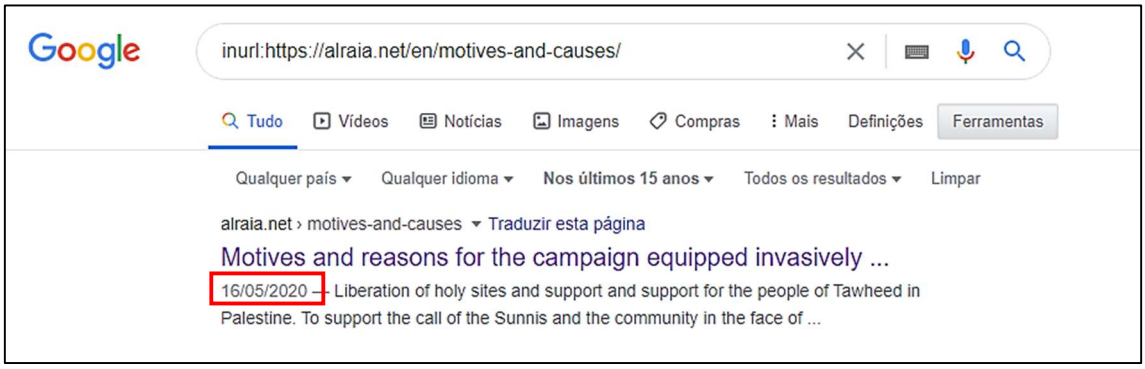
Available at https://alraia.net/en/motives-and-causes/, accessed on 18.12.2020.

Figure 15 - Providing points of contact.



Available at https://alraia.net/en/bitcoin-digital-currency/, accessed on 18.12.2020.

Figure 16 - Method used to discover a publication date.

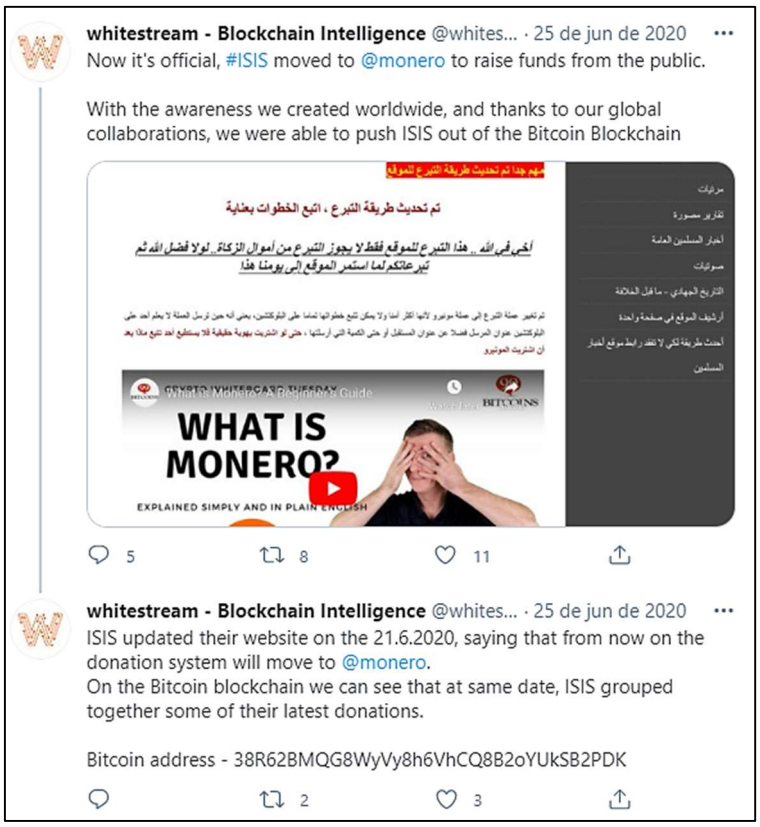


Google.com.

Figure 17 - June 2020 campaign for bitcoin.

Available at https://alraia.net/en/bitcoin-digital-currency/, accessed on 18.12.2020.

Figure 18 - Whitestream's tweet through which a print from Akhbar al-Muslimin's website is visible.



Available at: https://twitter.com/whitestream5/status/1276113021274898434?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1276113021274898434%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fcryptonews.com%2Fnews%2Fisis-affiliated-news-site-stops-accepting-bitcoin-moves-to-m-6949.htm, consulted on 21.12.2020.

Figure 19 - Comparing campaigns.

	Akhbar al-Muslimin	ITMC	AQB
Requested CC			
Communication channels			
Donation method	Hyperlink; QR code.	Cryto payment processor; QR code.	Hyperlink
Unique wallet generation scheme	✓	×	✓
Complementary layering techniques	×	×	✓
How-to videos	✓	×	✓
P2P interactions	-	2,1%	15,8%
Unregistered v Registered v HRTCs exchanges	-	17,5% v. 19,5% v. 10,2%	12,7% v. 58% v. 4,6%
Mixing services	-	50,3%	-
TF-related	-	-	3,9%
Donations size	-	$1,000 to $2,500 • At least 75% involved > $ 100 • Largest donation: $ 2, 495	$1 to $1,000 • Only three involved $ 1,000 and $ 2,500 • At least 75% involved < $ 70 • Largest donation: $ 2, 172
Total raised amount	$2,700	$16,680	Tens of thousands of dollars