Cryptocurrency Regulation in the EU AML Regime: the path towards effective harmonization?

Eduardo Silva de Freitas[1]

Abstract

The harmonisation of Anti-Money Laundering (AML) law, at EU level, has been motivated by the need to disrupt transnational organised crime. Cryptocurrencies present a complex challenge to AML policies, given the networked and cross-border nature of the transactions through which they are exchanged. Since the creation of Bitcoin in 2008, scholarly discussions contended the applicability of both the Third and the Fourth AML Directives to Cryptocurrency transactions. In 2018, an attempt was made by the EU to harmonise AML law targeting Cryptocurrencies through the enactment of the Fifth AML Directive. However, as it becomes evident from the current legal scholarship on this matter, the Fifth AML Directive has several shortcomings which undermine its potential to effectively harmonise AML measures targeting Cryptocurrencies, thereby creating a gap between the national implementing legislations that causes asymmetrical harmonisation. Thus, this paper argues that a revision of the Fifth AML Directive is necessary to prevent further asymmetrical harmonisation of AML legislation targeting Cryptocurrencies. I untangle the constructions undertaken as attempts towards the legal characterisation of Cryptocurrencies under both the Third and the Fourth AML Directives, in an attempt to outline the context of the legal environment in which the enactment of Fifth AML Directive took place. Then, I outline the shortcomings in the Fifth AML Directive's effort to provide for the harmonisation of AML policies targeting Cryptocurrencies in the EU. The main issues raised are its ability to cover Initial Token Offerings, Initial Coin Offerings, crypto-to-crypto exchange services and Tumbler services. Afterwards, I analyse, from the perspective of Cryptocurrencies, the EU AML Regime's limitations when it comes to enforcement and jurisdictional matters between EU Member States. Finally, I compare specific implementing measures of five EU Member States to verify whether there is, in fact, asymmetrical harmonisation of AML measures targeting Cryptocurrencies: Bulgaria, France, Germany, Italy and the UK. I conclude that delegating to Member States the responsibility for

[1] LLM, Faculty of Law. KU Leuven. Belgium.
eduardosfadv@gmail.com

distributing AML compliance obligations among the relevant actors within the Cryptocurrency ecosystem reverses the goal of Directives to facilitate the law through harmonisation.

Topics: Cryptocurrencies; Legal and regulatory issues; Security and utility tokens; Forensics and monitoring

Introduction

At least since the Silk Road scandal, Cryptocurrencies (CCs) are known to pose a major threat to public goods (e.g., financial stability) so as to demand a counteraction by public authorities in order to mitigate the potential risks arising from transactions involving them[2]. In this context, a prominent source of concern is the potential of CCs to circumvent Anti-Money Laundering (AML) regulations[3] given their anonymity/pseudonymity feature, their decentralized essence and the limited data available in the underlying system for transactions' recording in the form of blockchains[4].

Given the complex and networked structure that crosses national borders in which CC transactions take place, attention to this issue has been brought by the Financial Action Task Force (FATF), which updated its Recommendations accordingly on grounds that clarification was necessary on how its Recommendation 15 on "new technologies" should be applied to CCs[5]. Thus, in addition to jurisdictions which already had put in place CC-related legal provisions pertaining to AML, like Canada[6], several jurisdictions around the world began enacting AML legislations targeting CC-related Money Laundering (ML), such as Australia[7],

[2] P. Filippi, 'Bitcoin: a regulatory nightmare to a libertarian dream' (2014) 3 Internet Policy Review 1-11.

[3] K. K. R. Choo, 'Cryptocurrency and virtual currency: Corruption and money laundering/terrorism financing risks?', *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data* (Academic Press 2015) 283-307.

[4] Edgar G. Sanchez, 'Crypto-Currencies: The 21st Century's Money Laundering and Tax Havens' (2017) 28 University of Florida Journal of Law and Public Policy 167-191.

[5] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' (2019) 6.

[6] Bill C-31, An Act to Implement Certain Provisions of the Budget Tabled in Parliament on February 11, 2014 and Other Measures, 2nd Session, 41st Parliament, 2014.

[7] Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017.

Brazil[8] and the European Union (EU), to name just a few. This paper will focus on the EU AML regulatory regime targeting CC-related ML.

The EU AML regulatory regime targeting CCs was enacted via a Directive, namely Directive (EU) 2018/843 – the Fifth AML Directive (AMLD5)[9]. Directives establish goals for Member States to pursue, allowing for a margin of discretion[10]. AMLD5, like the AML directives that came before it, was enacted on the basis of what, post-Lisbon, is Article 114 of the Treaty on the Functioning of the EU (TFEU), as part of the overall EU project to harmonize measures regarding the establishment of the internal market[11]. The two-fold goal of such harmonization was well outlined by Advocate General (AG) Saggio in the Opinion issued for Case C-290/98 *Commission v Austria* – in which the improper implementation of provisions of the First AML Directive (Council Directive 91/308 – AMLD1) by Austria was discussed: both to avoid the (then) European Community from becoming "a field of activity for organised crime" and to establish "a privileged arena for the economic activity of those operators who, by exercising their right of establishment in a manner compatible with Community interests, enjoy the advantages of an internal market *founded on clear-cut and transparent rules*"[12].

Therefore, the possibility of reliance on clear and predictable rules is a cornerstone of the EU harmonisation efforts in AML matters. Nevertheless, as reported by the media, EU Member States are adopting "tougher crypto rules than [AMLD5] requires"[13]. Thus, this paper will, in two main steps, attempt to verify this assertion by exploring the degree to which AMLD5 contributes to the attaining the goal of establishing clear and predictable rules regarding the prevention of CC-related ML. For that purpose, I will first explore the way the

---

[8] BRASIL. Instrução Normativa da Receita Federal do Brasil nº 1.888, de 03 de maio de 2019. Institui e disciplina a obrigatoriedade de prestação de informações relativas às operações realizadas com criptoativos à Secretaria Especial da Receita Federal do Brasil (RFB). Diário Oficial da União. Brasília, DF, 07 maio 2019. Seção 1, p. 14.

[9] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU OJ L 156, 19.6.2018.

[10] Lorna Woods, Philippa Watson and Marios Costa, *Steiner & Woods EU Law* (13th edn, Oxford University Press 2017) 70.

[11] Valsamis Mitsilegas and Bill Gilmore, 'The EU legislative framework against money laundering and terrorist finance: a critical analysis in the light of evolving global standards' (2007) 56 International and Comparative Law Quarterly 119-141.

[12] Case C-290/98 *Commission v Austria* [2000] ECR I-7835, Opinion of AG Saggio, para 57 (emphasis added).

[13] 'EU Members Adopt Tougher Crypto Rules Than AML Directive Requires' (*Financial Accountant*, 2019) <https://www.financialaccountant.co.uk/news/eu-members-adopt-tougher-crypto-rules-than-aml-directive-requires> accessed 4 May 2020.

EU attempted to do so by outlining the scope of AMLD5's provisions regarding CCs. Here, it is important to highlight that AMLD5 focuses on the intermediaries involved in the process of CC transactions[14]. Then, I will explore what ML issues posed by CCs, involving such intermediaries as well as those which were not addressed by AMLD5, are being targeted by Member States' national implementing legislations, thereby causing asymmetrical harmonisation. I will also analyse how the jurisdiction rules established in the EU AML regulatory regime affect its potential to tackle CC-related ML. In this sense, the goal of this paper is to address the following question: What are the shortcomings of AMLD5 in promoting effective harmonization of AML policies targeting CC transactions across the EU?

Effective harmonisation is understood here as one which contributes towards the goals of the EU AML regulatory regime. Accordingly, the hypothesis formulated for this paper is that, leaving it to Member States to distribute the responsibility for AML compliance among the relevant actors within the CC ecosystem is reversing the goal of Directives within the EU AML regulatory regime to facilitate the law through harmonization.

As for the methodology, this paper will take a doctrinal approach to legal research, whereby I will indicate, through inductive reasoning, the incoherencies in law with reference to the abovementioned overall goals[15] of the EU AML regulatory regime stated by AG Saggio in *Commission v Austria*. I will also perform comparative analysis, based on a functional approach, again considering those same goals and objectives[16]. I compare the French, Italian, Bulgarian, German and United Kingdom (UK) national legislations implementing AMLD5. This comparative analysis will attempt to ascertain which issues regarding CC-related ML are being targeted by asymmetrical harmonisation.

This study has two limitations. The first is that it will not discuss how the EU AML criminal framework targets CCs, since this would involve a highly complex dogmatic analysis of legal concepts pertaining to EU criminal law, which is out of the scope of this paper. The second is that it will not discuss how the new technology called "atomic swap" – which allows users to directly engage in crypto-to-crypto transactions between them, without the need of an

[14] Nikola Paunović, 'Terrorist Financing as The Associated Predicate Offence of Money Laundering in The Context of The New EU Criminal Law Framework for The Protection of The Financial System' [2019] EU and Member States – Legal and Economic Issues 659-683.

[15] M. Siems, 'A World without Law Professors', *Methodologies of Legal Research: Which Kind of Method for What Kind of Discipline?* (Hart 2011) 79-82.

[16] Ralf Michaels, 'The Functional Method of Comparative Law', *The Oxford Handbook of Comparative Law* (Oxford University Press 2006) 361.

exchange service acting as intermediary[17] – should be brought under the EU AML regulatory regime, given the lack of evidence of concrete policy propositions for AML regulations targeting such mechanism in the EU.

This paper is structured as follows. Firstly, I describe what CCs are, how they work, and what are the ML risks posed by them. Secondly, I describe how the coverage of CCs under the EU AML regulatory regime evolved until the enactment of AMLD5. Thirdly, I outline the shortcomings in AMLD5's effort to provide the harmonization of AML policies targeting CCs in the EU. The main issues raised are its ability to cover Initial Token Offerings (ITOs), Initial Coin Offerings (ICOs), crypto-to-crypto exchange services and Tumbler services. Afterwards, I analyse, from the perspective of CCs, the EU AML regulatory regime's limitations when it comes to enforcement and jurisdictional matters between EU Member States. Finally, there will be a conclusion where I express my final remarks on the subject and give my opinion on some of the issues explored during this paper.

Cryptocurrencies, Virtual Currencies and Tokens

The European Central Bank's (ECB) report on Virtual Currency (VC) Schemes (ECB report) classifies VCs in three categories: "[c]losed [VC] schemes", "[VC] schemes with unidirectional flow" and "[VC] schemes with bidirectional flow". Closed VC schemes are usually linked to online games. The amount of virtual money earned is correspondent to the players' performance in the game. One example is World of Warcraft gold, which is then used to buy in-game goods and services (e.g., armor and transport). Players are not allowed to sell this type of virtual money for real-life cash. VC schemes with unidirectional flow are those which are bought using fiat currency for a pre-established purpose, but which cannot be switched back into fiat currency later. One example is the, now extinct, Facebook Credit, which was used to buy virtual goods on the Facebook platform. VC schemes with bidirectional flow are the focus of this paper. This type of VC can be exchanged back and forth from and to fiat currency at the exchange rate value and be used to buy any type of virtual of real-life assets[18]. The most popularly famous VC scheme with bidirectional flow is Bitcoin (BTC), the first known CC.

[17] Lindsay X. Lin, 'Deconstructing Decentralized Exchanges' [2019] Stanford Journal of Blockchain Law & Policy.

[18] European Central Bank, 'Virtual Currency Schemes' (2012) 44.

CCs are bought mainly from exchange service providers. There are two main types of exchange service providers: centralized and decentralized. Centralized exchange service providers are the most common form to acquire CCs: the prospective buyer simply needs to access them and perform the purchase. Decentralized exchange service providers are platforms in which users that communicate through the interface provided seek to match their needs with that of the other users, so as they can then trade[19].

CCs are exchanged on a peer-to-peer basis, meaning the users do not depend on any financial institution or clearing facilities to complete the necessary steps for performing CC-related transactions[20]. CCs' owners have two keys, a private and a public key. The public key is the one used to receive CCs from other owners, resembling a bank account number. The private key is used by the owners themselves to perform transactions, transferring CCs to other users, resembling a bank account password[21].

The private keys of CC users are stored in digital wallets. These digital wallets, when offered via software, provide the user with an interface to both perform transactions with and receive CCs from other users[22]. There are two types of wallet providers: custodian and non-custodian. Custodian wallet providers not only store the user's private key but also control it. Non-custodian wallet providers let the users themselves control their private keys. This latter service can be provided by offering a hardware which stores the key or a software where the user manually enters the key[23].

These transactions are recorded on a blockchain "that allows verification and recording of each transaction within the system in a publicly-distributed ledger"[24] – the Distributed Ledger Technology. However, the identity of the parties to the transaction is kept secret. Thus, CCs such as Bitcoin provide their users with "pseudonymity"[25]. On the other hand, another type of CCs, the so-called "privacy coins" – such as Monero (XMR) – are completely

[19] Garrick Hileman and Michel Rauchs, *Global Cryptocurrency Benchmarking Study* (Cambridge Centre for Alternative Finance 2017) 28.

[20] European Central Bank (n 18) 21.

[21] Paul Vigna and Michael Casey, *The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order* (Macmillan 2015) 124-126.

[22] Garrick Hileman and Michel Rauchs (n 19) 48.

[23] Garrick Hileman and Michel Rauchs (n 19) 48.

[24] Robert Hockett and Saule Omarova, 'The Finance Franchise' (2017) 102 Cornell Law Review 1143-1218.

[25] Malte Möser, 'Anonymity of Bitcoin Transactions: An Analysis of Mixing Services', *Münster Bitcoin Conference* (2013).

anonymous. The respective transactions recorded on the blockchain use a different public key for each transaction[26].

The blockchain technology also gave rise to the process of "tokenization". "Tokens" are units of value. There are three types of tokens: currency tokens, utility tokens and investment tokens. Utility tokens are purpose-specific, their respective value is claimed upon the fulfilment, by the issuer, of the obligation to which they are attached. Investment tokens play the role of a fundraising facility. The issuer publicly offers such tokens and, in exchange, the acquirer of receives a return on this investment, such as dividends, resembling the function of securities in the stock markets. Currency tokens (CCs) are tokens which are used as means of payment for "anyone who is willing to accept them". As CCs do not have the support of a central authority, their value comes from the design of the hack-proof underlying technology[27]. Fitting it in the classification of VCs outlined by the ECB report, currency tokens (CCs) would fall under the category of VC schemes with bidirectional flow. Since the focus of this paper is on CCs, from here onwards I will refer to mostly to CCs, but I will still use the term "VCs" when it is not possible circumscribe the idea or source referred to CCs. I will use the term "tokens" when I want to refer to more than one of the purposes which these units of value can have.

Legally, CCs can be characterized from diverse perspectives. To give a few examples, the Court of Justice of the European Union (CJEU), for tax purposes, decided in Case C-264/14 *Skatteverket v David Hedqvist* that CCs are equal to legal tender and, therefore, its respective exchanges were exempt from the corresponding value-added tax[28]. In doing so, the CJEU stated that "it is common ground that the 'bitcoin' virtual currency has no other purpose than to be a means of payment and that it is accepted for that purpose by certain operators"[29]. The High Court of Justice of England and Wales granted an injunction in *AA v Persons Unknown & Ors, Re Bitcoin* on grounds that CCs are property and, as a consequence, recoverable assets, given that its characteristics meet those necessary for being legally defined as such under the English

[26] 'Guide on Privacy Coins: Comparison of Anonymous Cryptocurrencies' (*Master the Crypto: Cryptocurrency Investment Trading Guides*) <https://masterthecrypto.com/privacy-coins-anonymous-cryptocurrencies/> accessed 3 May 2020.

[27] Philipp Maume and Mathias Fromberger, 'Regulation of Initial Coin Offerings: Reconciling U.S. and E.U. Securities Laws' (2019) 19 Chicago Journal of International Law 548-585.

[28] Case C-264/14 *Skatteverket v David Hedqvist* [2015] ECR I-718.

[29] Ibid.

common law of property[30]. The Tribunal Supremo de España, on the other hand, defined CCs as being intangible assets which thus could not themselves be reclaimed, only compensated for[31]. In France, the Tribunal de Commerce de Nanterre decided in the same vein, adding that CCs are not only intangible assets, but also fungible[32].

However, although CCs are operated through electronic means and can be used as media of exchange, they do not legally qualify as electronic money (e-money), for two reasons. The e-money Directive (EMD) requires that e-money be issued only upon transfer of equivalent funds, as stated in Article 2(2) EMD[33], and be redeemable, in any moment, at par value, in compliance with Article 11(2) EMD[34]. Thus, since CCs can be bought with any asset and are usually sold at the exchange rate value, they do not qualify as e-money under the EMD[35].

Money Laundering risks posed by Cryptocurrencies

The FATF ascertained the ML process in three steps – placement, layering and integration. The first step (integration) is when the criminal places the proceeds of crime within the financial "upperworld" (e.g., banks). Such placement can be performed, for example, by splitting a large amount of cash into several small deposits. The second step (layering) is when the money is moved away from its unlawful source. For this purpose, illicit funds are, e.g., continuously, and randomly transferred across different bank accounts for the purpose of further concealment. The third and final step (integration) is the one by which the criminal invests the laundered funds in the "real economy", for example through the purchase of property[36].

ML is just one type of crime associated with CCs. Another crime associated with CCs, for example, is ransomware. Ransomware occurs when criminals lock access to a computer or

[30] *AA v Persons Unknown & Ors, Re Bitcoin* [2019] EWHC 3556 (Comm).

[31] Sentencia del Tribunal Supremo (Sala 2ª, Sección 2ª) nº 326/2019 (recurso nº 998/2018) de 20 de Junio de 2019.

[32] Comm. Nanterre (6e ch.), 26 février 2020.

[33] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC OJ L 267, 10.10.2009, p. 7–17, Article 2(2).

[34] Directive 2009/110/EC (n 33), Article 11(2).

[35] Noah Vardi, 'Bit by Bit: Assessing the Legal Nature of Virtual Currencies', *Bitcoin and Mobile Payments: Constructing a European Union Framework* (Palgrave Macmillan 2016) 55-71.

[36] 'Money Laundering' (*Financial Action Task Force*, 2011) <https://www.fatf-gafi.org/faq/moneylaundering/> accessed 9 March 2020.

data until the target pays for getting access back[37]. This payment is often demanded in CCs[38]. However, this paper will focus on ML, and this section in the main ML risks posed by CCs, which are those that AMLD5 sought to address, namely anonymity/pseudonymity as well as the cross-border flexibility of CC transactions. Other, more intermediary-specific risks and/or blind spots will be discussed below together with the criticisms towards AMLD5 regarding the failure to address them. Table 1 demonstrates how the three stages of ML described above take place within the context of CC-related ML.

General risk factors	**Potential exploitation of vulnerabilities at each stage**		
	Placement	Layering	Integration
Anonymity/ pseudonymity	CCs can be used by criminals and associations	Suspicious names	Allowing cashing out of proceeds of crime to be passed on anonymously to individuals that cannot be traced
Real-time transactions	Proceeds of crime can be transferred to another CC in another country	Transactions occur in real-time, allowing little time to stop them if suspected of money laundering	Proceeds of crime can be moved rapidly through the global financial system and withdrawn in another country

Table 2. Money laundering risks posed by CCs. Adapted from Malcolm Campbell-Verduyn, 'Bitcoin, Crypto-Coins, And Global Anti-Money Laundering Governance' (2018) 69 Crime, Law and Social Change 283–305.

In the context of ML, the anonymity/pseudonymity feature of CCs challenges the traditional AML Customer Due Diligence (CDD) compliance landscape from "'parties known-transactions unknown' to 'transactions known-parties unknown'"[39]. As explained above, although CC transactions are recorded on a blockchain, the identity of the parties to the transaction is kept secret. The only information available is the amount traded and the public

[37] 'Ransomware' (*Department of Homeland Security*) <https://www.us-cert.gov/Ransomware> accessed 5 May 2020.

[38] European Union Agency for Law Enforcement Cooperation, 'Internet Organised Crime Threat Assessment' (2019) 54.

[39] Malcolm Campbell-Verduyn, 'Bitcoin, Crypto-Coins, And Global Anti-Money Laundering Governance' (2018) 69 Crime, Law and Social Change 283–305.

keys of the owners of the CCs. Moreover, since public keys are easily available, criminals can make use of a different public key for each transaction[40].

The threat posed by the cross-border flexibility of CC transactions stems from the fact that, differently from traditional money remittance means, CC users do not need any professional intermediary to intervene. As soon as the user is in possession of her private key, she can immediately transfer the CCs to the holder of a public key located anywhere in the planet. And here is where traditional AML policies and the blockchain technology that underlies CCs collide. Most of the AML efforts developed so far focus on intermediaries, who seek to identity suspicious transactions through CDD[41]. CC transactions *necessarily* involve an intermediary only when the user wants to convert them back into fiat currency. But for that matter, not only a whole range of tactics can be used to add extra layers of untraceability, as I will demonstrate below, but also CCs can be exchanged for any type of good or service due to their bidirectional character.

Cryptocurrencies under the Third Anti-Money Laundering Directive

The Third AML Directive (Directive 2005/60 – AMLD3) did not expressly cover CCs since it was enacted three years before they were created. However, it still constituted the regime in force for several years after the creation of CCs in 2008 up until the enactment of the Fourth AML Directive (Directive (EU) 2015/849 – AMLD4) in 2015. And even though, as mentioned, AMLD3 did not expressly cover CCs, Kaiser argues that they could come under its scope[42]. The reasons for this are as follows.

In terms of its material scope, AMLD3 covered a wide range of forms by which ML could take place[43]. The term used to refer to the assets being laundered was "property" and not "money"[44]. "Property" under AMLD3 meant "assets of every kind, whether corporeal or

[40] Robert Stokes, 'Virtual Money Laundering: The Case of Bitcoin and The Linden Dollar' (2012) 21 Information & Communications Technology Law 221-236.

[41] Pierpaolo Fratangelo, 'The CDD Obligations Following a Risk-Based Approach', *The New Anti-Money Laundering Law: First Perspectives on the 4th European Union Directive* (Palgrave Macmillan 2016) 14-15.

[42] Carolin Kaiser, 'The Classification of Virtual Currencies and Mobile Payments in Terms of The Old and New European Anti-Money Laundering Frameworks', *Bitcoin and Mobile Payments: Constructing a European Union Framework* (Palgrave Macmillan 2016) 212-215.

[43] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing OJ L 309, 25.11.2005, p. 15–36, Article 1(2).

[44] Carolin Kaiser (n 42) 212-215.

incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such assets"[45]. According to Kaiser, CCs would thus be covered by AMLD3 in the notions of "assets of every kind", "incorporeal" and "intangible assets"[46]. In my view, considering the examples of legal characterization of CCs under Spanish, English and French private law provided above, the material scope of AMLD3 would entail all three, irrespective of how the respective legal system defined CCs.

In terms of its personal scope, AMLD3 applied, among other actors, to financial institutions. "Financial institutions", under AMLD3, included "activities of currency exchange offices (bureaux de change) and of money transmission or remittance offices"[47]. Kaiser shows that fiat currency exchange offices' work is analogous to those of CCs exchange providers with the slight difference that the latter operate exclusively online. Thus, given the incoherence that, in her view, would result in interpreting such legislation as excluding CCs exchange providers from its scope given the similarity of its activity with that of fiat currency exchange offices, Kaiser argues that CCs exchange providers did fall under the scope of AMLD3[48]. Miners and wallet providers were out of the scope of AMLD3 since, as Egan explains, "it was evident that neither role involved the provisions of credit services which would entail receiving deposits from the public or granting credit. Nor was the work of wallet providers and miners characterised by attributes of financial institutions"[49].

However, in my view, Kaiser's opinion regarding CCs exchange providers is wrong. When the FATF and the Council of Europe published their joint report on ML through Money Remittance and Currency Exchange Providers (in which they referred to the coverage of fiat currency exchange offices by AMLD3), they expressly excluded New Payment Methods (NPM) from the report's scope, explaining that such methods had already been object of the 2006 FATF report on NPMs[50]. And the latter report entailed ML concerns regarding "digital

[45] Directive 2005/60/EC (n 43), Article 3(3).

[46] Carolin Kaiser (n 42) 212-215.

[47] Directive 2005/60/EC (n 43), Article 3(2)(a).

[48] Carolin Kaiser (n 42) 212-215.

[49] Mo Egan, 'A Bit(Coin) Of A Problem for The EU AML Framework', *The Palgrave Handbook of Criminal and Terrorism Financing Law* (Palgrave Macmillan 2018) 189.

[50] Financial Action Task Force and Council of Europe, 'Money Laundering Through Money Remittance and Currency Exchange Providers' (2010) 9.

currencies" such as e-gold[51]. Thus, considering one of AMLD3's objectives was to bring the EU AML regulatory regime in line with the FATF standards[52], I understand it is not possible to depart from conceptual delineation constructed by the FATF itself in order to include CCs exchange providers in the AMLD3 notion of "currency exchange offices".

Cryptocurrencies under the Fourth Anti-Money Laundering Directive

While the legislative process leading up to the adoption of AMLD4 was taking place, the European Banking Authority (EBA) issued its "[o]pinion on 'virtual currencies'" (EBA opinion). In this opinion, the EBA recommended the inclusion of CCs under the material scope of the EU AML framework and the inclusion of CCs exchange providers under the personal scope. The reasons the EBA gave for such recommendation consist of the risk posed to AML policies by CCs explained above[53]. Following the EBA opinion, the European Commission's Payment Systems Market Expert Group acknowledged it and stated that would consider including CCs in the material scope of AMLD4, taking into account their anonymity feature and facing the challenge of balancing "fundamental rights [with] AML needs"[54].

Moreover, both the ECB report[55] and the EBA opinion[56] stated that CCs present a risk for the prevention of terrorism financing for the same reasons that they do so regarding ML. In the aftermath of the terrorist attacks perpetrated in French territory in early 2015, the Council of the EU urged for the enhancement of AML standards and specifically stated the need to target CCs[57]. However, further positions did not expressly mention CCs. The latter were supported by the European Parliament and agreed upon by the European Commission, resulting in the final text of AMLD4, which did not refer to CCs[58]. Furthermore, "the inclusion of VCs

[51] Financial Action Task Force, 'Report on New Payment Methods' (2006) 16.

[52] Directive 2005/60/EC (n 43), Recital 5.

[53] European Banking Authority, 'Opinion On 'Virtual Currencies'' (2014) 32-35.

[54] Commission, Directorate-General for Financial Stability, Financial Services and Capital Markets Union, 'Minutes of The Meeting, Payment Systems Market Expert Group' (2014) 2-3.

[55] European Central Bank (n 18) 44.

[56] European Banking Authority (n 53) 32-35.

[57] General Secretariat of the Council of the European Union, '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' (2015) 1-3.

[58] Niels Vandezande, 'Virtual Currencies Under EU Anti-Money Laundering Law' (2017) 33 Computer Law & Security Review 341-353.

in 5AMLD was not in response to actual indication of their use in Europe for [terrorism financing] purposes, but rather general concern about the potential for [terrorism financing] risks to emerge"[59]. The European Union Agency for Law Enforcement Cooperation also stated in its report on "[c]hanges in the [modus operandi] of Islamic State terrorist attacks" that there is no evidence confirming the actual use of CCs to finance Islamic State terrorist attacks[60]. Finally, the European Commission's Supranational Risk Assessment of ML and Terrorist Financing Risks considered the level of terrorism financing threat posed by CCs to be "moderately significant". The reason given is that, although law enforcement authorities had collected some evidence of the use of CCs for terrorism financing purposes, the hurdle of the technical complexity involving the use of CCs outweighs the benefit of anonymity[61].

Nevertheless, even before the amendments brought by AMLD5, AMLD4 contained provisions which could bring CCs under its scope. Although the Directive did not mention CCs, it also did not exclude them from being scrutinized. Therefore, Member States could include CCs under their own national AML frameworks[62]. Regarding AMLD4's material scope, the rationale is the same as for AMLD3, as the notion of "property" under AMLD4 also entails "incorporeal" assets[63].

In terms of its personal scope, AMLD4 also applies to "Financial institutions" which, under such Directive, means, among others, "an undertaking other than a credit institution, which carries out one or more of the activities listed in points (2) to (12), (14) and (15) of Annex I to Directive 2013/36/EU of the European Parliament and of the Council"[64]. Annex I to Directive 2013/36/EU (Capital Requirements Directive IV) includes the activity of

---

[59] European Parliament, 'Virtual currencies and terrorist financing: assessing the risks and evaluating responses' (2018) 24.

[60] European Union Agency for Law Enforcement Cooperation, 'Changes in modus operandi of Islamic State terrorist attacks' (2016) 7.

[61] Commission, 'Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border situations' COM (2017) 340 final.

[62] Peggy Valcke, Niels Vandezande and Nathan Van de Velde, 'The Evolution of Third-Party Payment Providers and Cryptocurrencies Under the EU's Upcoming PSD2 and AMLD4', SWIFT Institute Working Paper No. 2015-001 56.

[63] Niels Vandezande (n 58) 341-353.

[64] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC OJ L 141, 5.6.2015, p. 73–117, Article 3(2)(a).

"[i]ssuing and administering other means of payment (e.g. travellers' cheques and bankers' drafts) insofar as such activity is not covered by point 4"[65]. "[P]oint 4" refers to "[p]ayment services"[66]. From this perspective, a court in Estonia decided that CC exchange providers were covered by its national AML legislation, given the latter's extension to services which deal with financial obligations involving resources that have a function like money[67]. Moreover, the AMLD4 framework could be extended to CC exchange providers given the general rule of Article 4(1), according to which Member States should include ML-prone undertakings under their national AML legislations[68].

Cryptocurrencies under the Fifth Anti-Money Laundering Directive

The legal framework outlined above shows that CCs were never expressly included in the EU legislative framework on AML. In this context, AMLD5 was enacted having as one of its main objectives to fill this gap[69] by amending AMLD4. AMLD5 refers to VCs which, as explained above, is a broader concept that includes CCs. The concept was framed as follows:

> "'virtual currencies' means a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically"[70].

Recital 11 AMLD5 explains that VCs which are essentially local or dealt with by a limited number of users fall out of its scope[71]. Recital 10 clarifies that VCs should not be confused with (a) in-game money; (b) e-money – differences which were explained above – nor with the broader notion "funds" entailing e-money under Article 4(25) Payment Services

---

[65] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC, Annex I, point 5.

[66] Directive 2013/36/EU (n 65), Annex I, point 4.

[67] Kaido Künnapas, 'From Bitcoin to Smart Contracts: Legal Revolution or Evolution from The Perspective Of *De Lege Ferenda*?', *The Future of Law and eTechnologies* (Springer 2016) 111-131.

[68] Niels Vandezande (n 58) 341-353.

[69] Thomas A. Frick, 'Virtual and Cryptocurrencies – Regulatory and Anti-Money Laundering Approaches in The European Union and In Switzerland' (2019) 20 ERA Forum 99-112.

[70] Directive (EU) 2018/843 (n 9), Article 1(2)(d).

[71] Directive (EU) 2018/843 (n 9), Recital 11.

Directive 2 (PSD2")[72]. It should also not be confused with "services based on specific payment instruments that can be used only in a limited way", i.e. accepted by its own issuer solely, as defined in Article 3(1)(k) PSD2[73]. Recital 10 also mentions potential uses of VCs other than as "means of payment". This part of Recital 10 and its implications will be further discussed below.

Therefore, when it comes to the three types of VCs outlined in the ECB report and explained above, we can say that AMLD5 focuses on VCs with bidirectional flow, since both closed VC schemes (which the Directive refers to as "in-game money") and VC schemes with unidirectional flow (which the Directive refers to as those which "can be used only in a limited way") are out of its scope.

Despite the possibilities of CCs falling under the scope of both AMLD3 and AMLD4 as mentioned above, AMLD5 delineates that, before its enactment, exchange and custodian wallet providers were not covered by the EU AML regulatory regime. This gap could allow criminals to take advantage of the anonymity/pseudonymity feature of CCs and transfer illicit resources to the EU via such platforms (nevertheless, it should be noted that, although CCs can provide anonymity/pseudonymity for their users, their use for concealing the illicit origin of resources is still marginal if compared to ordinary cash[74]). Thus, both exchange and custodian wallet providers were brought under the scope of the EU AML regulatory regime. Under Recital 8 AMLD5, competent authorities should be able to, through such platforms, scrutinize the flow of CCs[75].

Recital 9 states:

> "The inclusion of providers engaged in exchange services between virtual currencies and fiat currencies and custodian wallet providers will not entirely address the issue of anonymity attached to virtual currency transactions, as a large part of the virtual currency environment will remain anonymous because users can also transact without such providers"[76].

---

[72] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC OJ L 337, 23.12.2015, p. 35-127, Article 4(25).

[73] Directive (EU) 2015/2366 (n 72), Article 3(1)(k); Directive (EU) 2018/843 (n 9), Recital 10.

[74] Simon Butler, 'Criminal Use of Cryptocurrencies: A Great New Threat or Is Cash Still King?' (2019) 4 Journal of Cyber Policy 326-345.

[75] Directive (EU) 2018/843 (n 9), Recital 8.

[76] Directive (EU) 2018/843 (n 9), Recital 9.

One can infer from Recitals 8 and 9 that – besides the overall goal of the EU AML regulatory regime stated by AG Saggio in *Commission v Austria*[77] – the reason why the harmonization of AML policies targeting CC transactions across the is EU necessary is that, as just mentioned, remedying this gap was necessary to prevent, to the extent possible, criminals from taking advantage of the anonymity/pseudonymity feature of CCs to transfer illicit resources to the EU via custodian wallet and exchange service providers. This approach, taken by the EU, which consists in focusing in the intermediaries between the "virtual" and the "real" world regarding the flow of CCs is known as the "gatekeeper approach"[78], in line with the traditional method of AML policies to focus on intermediaries. However, this is only fruitful when there is an identifiable intermediary involved in the transaction. Nevertheless, when this is not the case, a blind spot in the fight against ML emerges, as will be explained below.

Two intermediaries in the CCs ecosystem are defined in AMLD5. The Directive brings "custodian wallet providers" and "providers engaged in exchange services between virtual currencies and fiat currencies" under the heading of "obliged entities"[79]. It defines "custodian wallet providers" as "an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies"[80]. Member States must ensure that both intermediaries are registered[81].

Initial Token/Coin Offering

As explained above, "CCs" is a term that refers to currency tokens. Tokens, however, can also have the function of investment[82] (investment tokens). ITOs and, as a part of them, ICOs, are the act whereby entrepreneurs looking for investors and CCs issuers, respectively,

[77] *Commission v Austria* (n 12), Opinion of AG Saggio, para 57.

[78] Thomas A. Frick (n 69) 99-112.

[79] Directive (EU) 2018/843 (n 9), Article 1(1).

[80] Directive (EU) 2018/843 (n 9), Article 1(2).

[81] Directive (EU) 2018/843 (n 9), Article 1(29).

[82] European Central Bank, 'Opinion of the European Central Bank of 12 October 2016 on a proposal for a directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC' (2016) 3.

publicly offer these tokens[83]. ITO transactions take place through smart contracts[84]. Smart contracts record the terms of the agreement reached by the parties, in the form of a code, in the blockchain. The performance of the contract is then automatically carried out by the code, without the need of intervention by the parties[85]. An analogy often made to illustrate the functioning of a smart contract is to compare it with that of a vending machine. The anonymity/pseudonymity issue of CCs is equally present in the context of ICOs, leaving them also prone to ML risks[86].

There are two parameters in AMLD5 against which its coverage of these public offers can be ascertained: the definition of VCs enacted in AMLD5 and the definition of obliged exchange services as those operating fiat-to-crypto trade[87]. The latter approach was taken by the European Securities and Markets Authority (hereafter "ESMA") regarding ICOs. According to ESMA, under such definition, ICO issuers are not obliged entities under the EU AML regulatory regime[88]. The reason for this view is that the consideration for ICOs can be any asset, especially other CCs, and not just fiat currencies[89]. Therefore, ESMA recommends the explicit inclusion of ICOs under the EU AML regulatory regime not only for the risks they present but also to align the regime with the updated FATF Recommendations[90].

Haffke, Fromberger and Zimmermann argue that, given the plural "services" found in Article 2(1)(g) AMLD4, only ICOs that, besides accepting fiat currency as a means of payment, *are multi-staged* could fall under the scope of AMLD4, since such wording would indicate that one-time transactions are not covered by this provision[91]. I do not agree with this overly

---

[83] Jonathan Rohr and Aaron Wright, 'Blockchain-based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets' (2019) 70 Hastings Law Journal 463-524.

[84] Philipp Hacker and Chris Thomale, 'Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies Under EU Financial Law' (2018) 15 European Company and Financial Law Review 645–696.

[85] Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Harvard University Press 2018) 74.

[86] Alexander Snyers and Karl Pauwels, 'ICOs In Belgium: Down the Rabbit Hole into Legal No Man's Land? Part 1' (2018) 29 International Company and Commercial Law Review 483-510.

[87] Apolline Blandin and others, *Global Cryptoasset Regulatory Landscape Study* (Cambridge Centre for Alternative Finance 2019) 85.

[88] European Securities and Markets Authority, 'Advice: Initial Coin Offerings and Crypto-Assets' (2019) 36.

[89] Dirk A. Zetzsche and others, 'The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators' (2019) 60 Harvard International Law Journal 267-315.

[90] European Securities and Markets Authority (n 88) 36.

[91] Lars Haffke, Mathias Fromberger and Patrick Zimmermann, 'Cryptocurrencies and anti-money laundering: the shortcomings of the fifth AML Directive (EU) and how to address them' [2019] Journal of Banking Regulation.

simplistic and grammatical interpretation. Article 3(5) AMLD4 is very clear in stating that the restrictions to the transaction-based exemption granted by Article 3(3)(b) AMLD4 are applicable "whether the transaction is carried out in a single operation or in several operations which appear to be linked"[92]. Therefore, in my understanding, the remaining criteria of Article 3(3)(b) – and not whether the ICO is multi-staged or not – should be the parameter against which to scrutinize whether a particular ICO, and the respective transactions which it would involve, can fall out of the scope of AMLD4, namely: the amount of money concerned, the type of financial activity and the ML risks involved[93].

This uncertainty is clearly a problem for harmonization and the fight against CC-related ML. Nevertheless, national legislatures may address this issue by going beyond the minimum required by AMLD5. The UK did so by clarifying in the implementing legislation that the category of "cryptoasset exchange provider" includes the "creator or issuer of any of the cryptoassets involved"[94]. France[95] and Italy[96] also included issuers. On the other hand, Bulgaria did not make such inclusion[97].

Regarding the other approach – which is more relevant for investment tokens – based on the definition of VCs enacted in AMLD5, Bal argues, with reference to Recital 10 AMLD5, that such definition is broad enough to cover the use of investment tokens[98]. Under such Recital:

> "… virtual currencies can frequently be used as a means of payment, they could also be used for other purposes and find broader applications such as means of exchange, *investment*, store-of-value products or use in online casinos. The objective of this Directive is to cover all the potential uses of virtual currencies"[99].

---

[92] Directive (EU) 2015/849 (n 64), Article 3(5).

[93] Directive (EU) 2015/849 (n 64), Article 3(3)(b).

[94] The Money Laundering and Terrorist Financing (Amendment) Regulations 2019. At the time of writing, although the UK left the EU in on January 31, 2020, "Union law shall be applicable to and in the United Kingdom during the transition period", "which shall start on the date of entry into force of this Agreement and end on 31 December 2020", see Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community OJ C 384I, 12.11.2019, p. 1–177, Articles 126 and 127(1).

[95] Décret n° 2019-1213 du 21 novembre 2019 relatif aux prestataires de services sur actifs numériques, JORF n° 0271 du 22 novembre 2019.

[96] Decreto Legislativo 21 novembre 2007, n. 231, GU n. 290 del 14-12-2007.

[97] Measures Against Money Laundering Act.

[98] Aleksandra Bal, *Taxation, Virtual Currency and Blockchain* (Wolters Kluwer 2018).

[99] Directive (EU) 2018/843 (n 9), Recital 10 (emphasis added).

However, a further issue is that, as explained above, the definition of VCs enacted in AMLD5 requires that, to fall under such definition, a VC must be usable as a "means of exchange". Considering this aspect, Haffke, Fromberger and Zimmermann argue that a broad interpretation such as that advanced by Bal cannot be accepted, pointing two main reasons[100].

The first reason is that Recital 10 itself uses the introducing transition "such as" before mentioning the applications of, e.g., means of exchange and investment, and Article 3(18) did not repeat such examples when defining VCs. Thus, it would be inconsistent to interpret the Recital as being more far-reaching than the legislation itself. I add to that the CJEU's understanding regarding the (absence of) legal force in Recitals[101]. The second reason is that a "means of exchange", in economic terms, is an "intermediary object" with the primary aim to make trade possible without having to recur to the practice of trading goods themselves. Since such a function is only a characteristic of currency tokens (CCs) and not investment tokens, the latter cannot be deemed to fall under the definition of VCs enacted in AMLD5[102].

This is another uncertainty that can create problems for harmonization. For example, in this matter, Bulgaria's legislation implements the minimum required by AMLD5, the former's definition of VCs being identical to that of the latter[103]. However, also here there are examples of national legislatures taking a step further in avoiding this definitional backsliding. Italy[104] and Germany[105] both include the possibility of the instruments concerned to be used for investment purposes in their definitions equivalent to that of VCs under AMLD5. The UK enacted an even more technologically neutral definition, giving to "cryptoassets" the meaning of "cryptographically secured digital representation of value or contractual rights that uses a form of distributed ledger technology and can be transferred, stored or traded electronically"[106]. In my view, this latter definition is not function-driven and therefore able to, in the future, cover

[100] Lars Haffke, Mathias Fromberger and Patrick Zimmermann (n 91).

[101] Case C-162/97 *Nilsson v Angličtině* [1998] ECR I-7477.

[102] Lars Haffke, Mathias Fromberger and Patrick Zimmermann (n 91).

[103] Measures Against Money Laundering Act.

[104] Decreto Legislativo 21 novembre 2007, n. 231, GU n. 290 del 14-12-2007.

[105] Gesetz zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie, Vom 12. Dezember 2019 (BGBl. I S. 2623).

[106] The Money Laundering and Terrorist Financing (Amendment) Regulations 2019.

tokens used for other purposes than those outlined above, which gives it an advantage in terms of fitness to regulate[107].

Crypto-to-crypto exchanges and Tumblers

As AMLD5 only targets exchange services as far as those provide fiat-to-crypto exchanges, crypto-to-crypto exchange services are out of its scope[108]. This curbs the combat on ML, given that users engaging in criminal activities can simply receive illicit resources in CCs and later convert them to another CC, thereby avoiding supervision based on AMLD5. Inclusion of exchange services operating crypto-to-crypto trade under the heading of obliged entities would extend to them the CDD obligations to which those entities currently regulated under AMLD5 are already bound, thereby enhancing Financial Intelligence Units' (FIU) ability to investigate possibly correlated offences[109]. Such amendment would also include some CC miners under the AML radar, given that part of them sell the mined CCs for other CCs[110].

This limitation is a major shortcoming of AMLD5. Even though Article 1(18) AMLD4 does not use the word "investment", including this term in the provision would only bring ICOs that receive fiat currency as consideration under the scope of AMLD4. Or, in other words, just changing AMLD5's definition of VCs is insufficient for bringing ICOs under its scope – a broader definition of exchange service providers beyond only those operating fiat-to-crypto trade is also necessary. Most ICOs receive CCs as consideration. Thus, such ICOs would fall out of the scope of AMLD5, since there is no fiat-to-crypto exchange involved[111]. On the other hand, Snyers and Pauwels argue:

> "One could argue that the European legislator has not gone far enough as platforms that exchange virtual currency for other virtual currency do not fall within the scope of AMLD5 and most ITOs ask for a contribution in virtual currency. However, unless they

[107] Eugenia Macchiavello, 'FinTech Regulation from A Cross-Sectoral Perspective', *European Financial Regulation: Levelling the Cross-Sectoral Playing Field* (Hart 2019) 84.

[108] Christopher P. Buttigieg and others, 'Anti-money laundering regulation of crypto assets in Europe's smallest member state' (2019) 13 Law and Financial Markets Review 211-227.

[109] David Connell, 'Do EU Regulations Combating Money Laundering and the Financing of Terrorism adequately tackle Cryptocurrencies? The case of Ireland' (2018) 21 Irish Journal of European Law 68-90.

[110] European Parliament, 'Cryptocurrencies and Blockchain: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion' (2018) 76.

[111] Valentina Covolo, 'The EU Response to Criminal Misuse of Cryptocurrencies: The Young, Already Outdated 5th Anti-Money Laundering Directive', University of Luxembourg Law Working Paper No. 2019-015 15.

> have mined their virtual currency (which is becoming increasingly difficult), one cannot deny that even illicit investors must have acquired virtual currency at some point in time. If they have done so via a provider of exchange services or a custodian wallet provider, they will have been identified pursuant to AMLD5"[112].

However, such argument, in my view, ignores two important aspects. The first is that some CCs are easier to mine than others and these more easily mined CCs can thus equally be converted to another CC[113]. The second is that, alternatively, even if at some point a mainstream CC had to be acquired at an exchange service, it could have been bought at a foreign (non-EU) jurisdiction with more lax AML standards and later converted to another mainstream CC by transferring them to the public key of an EU-based crypto-to-crypto exchange service[114]. This issue is aggravated considering how easier it is for CCs to be used on a cross-border basis in comparison with fiat currencies[115].

Finally, including crypto-to-crypto transactions in the scope of AMLD5 would be a step further, although not the only one necessary, to entail the work of Tumbler services. Tumbler services are entities that collect CCs from their costumers and distribute them among diverse keys they own. They charge a fee for this service and return the CCs back to their original owners. This process adds extra layers to the anonymity/pseudonymity of the CC and further curbs traceability. As Haffke, Fromberger and Zimmermann explain, Tumbler services "exchange" a CC token "for" the same CC token. Thus, they recommend the inclusion, in AMLD5, of a complement to the definition of exchange providers to include "providers of services that exchange one virtual currency into the same virtual currency"[116].

Also, here the definitional backsliding of AMLD5 may undermine harmonization, as this is another issue on which some national legislatures are working around to address and go beyond the minimum required by AMLD5. Italy[117], France[118], and the UK[119] all have included

---

[112] Alexander Snyers and Karl Pauwels (n 86) 483-510.

[113] European Parliament (n 110) 76.

[114] Lars Haffke, Mathias Fromberger and Patrick Zimmermann (n 91).

[115] David Carlisle and Kayla Izenman, 'Closing the Crypto Gap: Guidance for Countering North Korean Cryptocurrency Activity in Southeast Asia', Royal United Services Institute for Defence and Security Studies Occasional Paper, April 2019 38.

[116] Lars Haffke, Mathias Fromberger and Patrick Zimmermann (n 91).

[117] Decreto Legislativo 21 novembre 2007, n. 231, GU n. 290 del 14-12-2007.

[118] Décret n° 2019-1213 du 21 novembre 2019 relatif aux prestataires de services sur actifs numériques, JORF n° 0271 du 22 novembre 2019.

[119] The Money Laundering and Terrorist Financing (Amendment) Regulations 2019.

exchange services operating crypto-to-crypto trade in their respective national AML legislations when implementing AMLD5. Bulgaria for example, however, did not[120].

Enforcement

In the view of the ECB, AMLD5 does not cover decentralized exchanges. As explained above, exchange platforms can be both centralized and decentralized, the latter being known as "peer-to-peer trading platforms". These platforms perform a merely technical, neutral, and passive role of attempting to meet the demand and supply of CCs owners. Therefore, the ECB understands that, since they do not involve the role of an "identifiable intermediary", they currently fall out of the scope of AMLD5[121]. Like crypto-to-crypto exchange service providers, this is a blind spot in the fight against CC-related ML[122]. Thus, the ECB recommends that decentralized exchanges should be submitted to a number of principles, amongst which is "technological integrity, meaning, inter alia, no back doors/loopholes or hidden functionalities, no white listing of malware, no fraudulent collusion, responsible cryptographic key management, and the pursuit of the state of the art"[123].

Anonymity and pseudonymity have been described above as one of the main sources of ML risks posed by CCs. As explained then, CCs vary in their degree of anonymity/pseudonymity. AMLD5 is "technologically neutral" on this point: both CCs which provide anonymity – i.e., privacy coins – and CCs which provide pseudonymity for their users are covered. Covolo suggests that the CDD obligations imposed by AMLD4 make it illegal for obliged entities to operate with privacy coins[124]. In my view, this is precisely the case considering Article 14(4) AMLD4, which provides that Member States shall prevent obliged entities from either carrying out a transaction and/or establishing a business relationship if they cannot perform the relevant CDD[125]. Again, according to the aforementioned study conducted for the European Parliament, referring to how ALMD5 treats privacy coins, exchanging them "will no longer be possible to the fullest extent: the [CCs] users that want to convert their [CCs]

[120] Measures Against Money Laundering Act.

[121] European Central Bank Crypto-Assets Task Force, 'Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures', ECB Occasional Paper Series No 223/May 2019 29.

[122] European Parliament (n 110) 77.

[123] European Central Bank Crypto-Assets Task Force (n 121) 29-30.

[124] Valentina Covolo (n 111) 19-20.

[125] Directive (EU) 2015/849 (n 64), Article 14(4).

into fiat currency via a virtual currency exchange or hold their portfolio via a custodian wallet provider, will be subject to [CDD]"[126].

Jurisdiction

The system for cooperation between FIUs of EU Member States for exchange of information is set up by Council Decision 2000/642[127]. The designation of the competent FIU to receive and process the Suspicious Transaction Reports (STR) submitted by obliged entities (whether CC-related or not) is provided by Article 33(2) AMLD4 as being "the FIU of the Member State in whose territory the obliged entity transmitting the information is established"[128]. The reach of the corresponding provision in AMLD3 (Article 22(2)), in light of the right to free provision of services provided for by Articles 56 and 57 TFEU[129], was interpreted by the CJEU in Case C-212/11 *Jyske Bank Gibraltar Ltd v Administración del Estado*[130].

This case concerned whether Member States were allowed to bindingly require that credit institutions providing services in their territory submitted STRs directly to their own FIUs when requested or if, on the other hand, such request should be directed to the FIU of the home Member State[131]. Although the case concerns credit institutions specifically, in my view it applied to all obliged entities, given the scope of application of Article 22(2) AMLD3, according to its own wording[132], was defined by Article 34 AMLD3, which did not discriminate between the types of obliged entities regulated by AMLD3[133]. The same can be said about the definition of the scope of application of Article 33(2) AMLD4 by Article 8(4) AMLD4[134].

---

[126] European Parliament (n 110) 80.

[127] Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information OJ L 271, 24.10.2000, p. 4–6.

[128] Directive (EU) 2015/849 (n 64), Article 33(2).

[129] Consolidated version of the Treaty on the Functioning of the European Union OJ C 326, 26.10.2012, p. 47–390, Articles 56 and 57.

[130] Case C-212/11 *Jyske Bank Gibraltar Ltd v Administración del Estado* [2013] ECR I-0000.

[131] Ibid [31].

[132] Directive 2005/60/EC (n 43), Article 22(2).

[133] Directive 2005/60/EC (n 43), Article 34.

[134] Directive (EU) 2015/849 (n 64), Articles 33(2) and 8(4).

On grounds that: (a) the wording of Article 22(2) AMLD3 did not "expressly prohibit such a possibility"; (b) although the enactment of AMLD3 (like that of AMLD1 and of the Second AML Directive – Directive 2001/97) was based on the internal market provision of Article 114 TFEU, its main aim was to tackle ML "*in an international context*" for the purpose of implementing the FATF Recommendations; (c) in light of the latter assessment, one of the goals of AMLD3 was to enhance the surveillance power of FIUs to effectively tackle ML; (d) AMLD3 did not prevent Member States from prosecuting ML-suspicious cases in their territory even if the respective activities were carried under the right to free provision of services, the CJEU decided that Member States were allowed to bindingly require that credit institutions providing services in their territory submitted STRs directly to their own FIUs when requested[135].

However, this judgement was made obsolete by AMLD4. Article 53(2) AMLD4, as amended by AMLD5, provides that "[w]hen an FIU seeks to obtain additional information from an obliged entity established in another Member State which operates on its territory, the request shall be addressed to the FIU of the Member State in whose territory the obliged entity is established"[136]. According to Incalza, such provision prevents the CJEU from applying the reasoning construed in *Jyske* to interpret Article 33(2) AMLD4[137].

The overriding of *Jyske* by AMLD4 has sensible consequences for the effectiveness AML measures in the EU, whether CCs-related or not. In *Jyske*, the CJEU pointed two major limitations to the system of exchange of information by FIUs in respect of obliged entities operating in another Member State under the right to free provision of services. Firstly, the FIU of the host Member State is more adequately placed to assess the elements potentially linked to ML activities in relation to both the obliged entities and its respective supervisory authorities[138]. Secondly:

> "… to be able to carry out a request for information through the mechanism for cooperation between the FIUs provided for by Decision 2000/642, the FIU must already be in possession of information indicating suspicion of money laundering or terrorist financing. Since disclosure relating to suspicious transactions is carried out, pursuant

[135] *Jyske* (n 130) [45]-[49] (emphasis added).

[136] Directive (EU) 2015/849 (n 64), Article 53(2).

[137] Thomas Incalza, 'National Anti-Money Laundering Legislation in A Unified Europe: *Jyske*' (2014) 51 Common Market Law Review 1829–1850.

[138] *Jyske* (n 130) [78].

> to Article 22(2) of Directive 2005/60, at the FIU of the Member State of origin and Decision 2000/642 does not provide for the requirement to forward them automatically to the FIU of the host Member State, the latter will only rarely have information corroborating the suspicions necessary so as to send a request for information to the FIU of the Member State of origin"[139].

Now I will reflect on the impact of the legal framework outlined above on (the absence of) AMLD5's coverage of crypto-to-crypto exchanges and Tumblers. Suppose a predicate offence is committed in the UK, which, as aforementioned, included crypto-to-crypto exchanges in its national AML legislation. The criminal agrees to receive BTC 2 as payment for the committed offence. The one who hires the criminal can buy the BTC 2 in an UK exchange service provider using fiat currencies and, through a device supplied by a non-custodian wallet provider, transfer the BTC 2 to the public key of a Bulgarian crypto-to-crypto exchange service operating in the UK under its right to free provision of services. The criminals then pay the respective fee to this crypto-to-crypto exchange service for converting the BTC 2 into XMR 300. The criminals also hire a Tumbler service to add extra layers of anonymity to the transaction. Finally, the XMR 300 can then be transferred to the person who was hired to commit the predicate offence. As said above, Bulgaria did not include crypto-to-crypto exchanges in its national AML legislation, but the UK did. The two latter intermediaries are not covered by Bulgarian AML measures, only UK measures. Under Article 53(2) AMLD4, if Incalza's understanding of its effects on the reasoning construed by the CJEU in *Jyske* to interpret Article 22(2) AMLD3 is correct, the UK could not request the Bulgarian crypto-to-crypto exchange service operating in its territory to submit STRs to its FIU. Moreover, even though the UK could, under Decision 2000/642, request information from the Bulgarian FIU, the latter would not be able – nor obliged – to provide the information requested, since both the Tumbler service and the crypto-to-crypto exchange service are not covered by Bulgarian AML measures. The wording of Article 53(2) itself confirms this by limiting the duties of the home Member States' FIUs to "the whole range of its *available powers* which it would normally use domestically for receiving and analysing information"[140]. This challenge is a great opportunity for arguing the necessity of further centralization of AML supervisory efforts at

[139] Ibid [79].

[140] Directive (EU) 2015/849 (n 64), Article 53(2) (emphasis added).

EU level[141] in addition to the EBA's mandate provided for by the European Supervisory Authorities Review Regulation, which so far only entails credit and financial institutions[142].

In view of the above, I believe this situation needs to be addressed for two reasons. The first reason is the ML risks posed by CCs described above. The second reason is that this provision is severely incoherent with the level of harmonisation aimed by AMLD4 itself – namely, minimum harmonisation – as evidenced by the right of Member States to adopt stricter measures than those prescribed by the Directive[143]. One could argue that the goal of Article 53(2) may be to ease the financial and administrative burden, on obliged entities operating abroad under their right to free provision of services, of having to comply with two reporting requirements simultaneously (that of the host Member State and that of the home Member State)[144]. However, combating ML is "amongst the overriding reasons in the public interest capable of justifying obstacles to the freedom to provide services"[145].

A possible way to address this issue would be to extend the possibility contained in Article 45(9) AMLD4 to CCs. Under Article 45(9) AMLD4 host Member States' FIUs can request that e-money issuers appoint a central contact point to forward STRs directly to them[146]. Although the AML regulatory approaches targeting CCs and e-money are very different (given that the latter – differently from CC intermediaries[147] – are only allowed to pursue their type of business upon meeting licensing requirements, are properly supervised and, therefore, more easily subject to AML rules[148]), in my view, for jurisdictional matters regarding supervision, such as these dealt with by Article 45(9) AMLD4, the extension of the regulatory approach taken regarding e-money could be extended to CCs. As evidenced by the Italian legislation

---

[141] Joshua Kirschenbaum and Nicolas Véron, 'A better European Union architecture to fight money laundering', Bruegel Policy Contribution Issue n° 19, October 2018 15.

[142] Regulation (EU) 2019/2175 of the European Parliament and of the Council of 18 December 2019 amending Regulation (EU) No 1093/2010 establishing a European Supervisory Authority (European Banking Authority), Regulation (EU) No 1094/2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority), Regulation (EU) No 1095/2010 establishing a European Supervisory Authority (European Securities and Markets Authority), Regulation (EU) No 600/2014 on markets in financial instruments, Regulation (EU) 2016/1011 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investment funds, and Regulation (EU) 2015/847 on information accompanying transfers of funds PE/75/2019/REV/1 OJ L 334, 27.12.2019, p. 1–145, Article 1.

[143] Directive (EU) 2015/849 (n 64), Article 5.

[144] Thomas Incalza (n 137) 1829–1850.

[145] Case C-212/08 *Zeturf Ltd v Premier ministre* [2011] ECR I-5633.

[146] Directive (EU) 2015/849 (n 64), Article 45(9).

[147] European Parliament (n 110) 81-82.

[148] Daniel Adeoyé Leslie, *Legal Principles for Combatting Cyberlaundering* (Springer 2014) 226.

implementing this provision[149], in such cases the FIU of the host Member State can request the central contact point to forward STRs directly to the former[150]. This would also, under the rationale construed by the CJEU in *Jyske*, contribute to the goals of the EU AML regulatory regime, as it would enhance the surveillance power of FIUs to effectively tackle ML. Consideration would also have to be given to the possibility of the hypothetical example provided above involving Bulgaria and the UK, where an undertaking would be an obliged entity in one Member State, but not in the other. Should the possibility contained in Article 45(9) AMLD4 be extended to CCs, would a Member State be able to require a central contact point to be appointed by an undertaking which would be an obliged entity under its national law, but is not an obliged entity under the national law of the home Member State? The *de lege ferenda* proposition hypothesized here would have to address this matter also, otherwise the shortcomings found in the current regime would not be superseded.

Conclusion

This paper attempted to inquire what are the shortcomings of the currently established EU AML regulatory regime in promoting effective harmonization of CC-related AML measures. The reasons why the EU harmonizes AML law are both the establishment of an internal market founded on legal certainty and crime prevention. The anonymity/pseudonymity feature of CCs provides them with the potential to be used for illicit transactions while disguising the identity of the parties involved. Therefore, the harmonization of AML measures targeting CC transactions across the EU – besides the core goals of harmonization of AML law in the EU stated by AG Saggio in *Commission v Austria* – is necessary to avoid, to the extent possible, that criminals take advantage of the anonymity/pseudonymity feature of CCs and transfer illicit resources to the EU via the relevant intermediaries involved in the transaction. However, not always clearly identifiable intermediaries will be involved in the transaction. Together, these two aspects of CCs (anonymity/pseudonymity and partial lack of identifiable intermediaries) pose a challenging obstacle to both the usual mean of scrutinizing suspicious transactions based on CDD as well the intermediary-driven governance structure of AML measures. Also, even in cases where there is a clearly identifiable intermediary, such as issuers,

[149] Decreto Legislativo 21 novembre 2007, n. 231, GU n. 290 del 14-12-2007.

[150] Domenico Siclari, 'Anti-Money Laundering EU Law and Network of Agents', *The New Anti-Money Laundering Law: First Perspectives on the 4th European Union Directive* (Palgrave Macmillan 2016) 45-56.

crypto-to-crypto exchange service providers and Tumbler services, the limitations of the reach of the provisions of AMLD5 that do not appropriately address these known ML risks posed by CCs cause Member States to (understandably) go beyond the minimum required by the Directive, thereby targeting different types of actors within CC ecosystem and reversing the goal of Directives within the EU AML regulatory regime to facilitate the law through harmonization. In this sense, the hypothesis formulated to address the main research question raised for this paper has been confirmed. Evidence collected from the national implementing legislations of Bulgaria, France, Germany, Italy and the UK demonstrates differences in the coverage of issuers and crypto-to-crypto exchange service providers in the personal scope of AMLD5 as well as in the coverage of investment tokens in the material scope of AMLD5.

How this situation translates in an obstacle towards effective harmonisation, considering its related goal of disruption of transnational organised crime, becomes salient when taking into account jurisdictional rules delineating the competence of FIUs to demand that obliged entities submit STRs, particularly after the legislative override of *Jyske* by Article 53(2) AMLD4. Currently, a criminal can easily circumvent AML laws by seeking the service of undertakings that are not obliged entities in the latter's home Member State to perform CC transactions the former does not want to be reported to FIUs, even if such undertakings are operating under their right to free provision of services in a Member State that imposes AML obligation on similar entities. Thus, I propose, *de lege ferenda*, that the possibility provided for host Member States' FIUs to request that e-money issuers appoint a central contact point to forward STRs directly to them be extended to custodian wallet and exchange service providers. Nevertheless as mentioned above, in my view, such proposition by itself would only marginally contribute to the effective harmonization of CC-related AML measures within the EU if the other shortcomings of AMLD5 regarding the limited reach of its provisions both in terms of its material as well of its personal scope are not addressed.

Table of Cases

AA v Persons Unknown & Ors, Re Bitcoin [2019] EWHC 3556 (Comm).

Case C-162/97 *Nilsson v Angličtině* [1998] ECR I-7477.

Case C-212/08 *Zeturf Ltd v Premier ministre* [2011] ECR I-5633.

Case C-212/11 *Jyske Bank Gibraltar Ltd v Administración del Estado* [2013] ECR I-0000.

Case C-264/14 *Skatteverket v David Hedqvist* [2015] ECR I-718.

Case C-290/98 *Commission v Austria* [2000] ECR I-7835.

Comm. Nanterre (6e ch.), 26 février 2020.

Sentencia del Tribunal Supremo (Sala 2ª, Sección 2ª) nº 326/2019 (recurso nº 998/2018) de 20 de Junio de 2019.

Table of Legislation

Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community OJ C 384I, 12.11.2019, p. 1–177.

Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017.

Bill C-31, An Act to Implement Certain Provisions of the Budget Tabled in Parliament on February 11, 2014 and Other Measures, 2nd Session, 41st Parliament, 2014.

BRASIL. Instrução Normativa da Receita Federal do Brasil nº 1.888, de 03 de maio de 2019. Institui e disciplina a obrigatoriedade de prestação de informações relativas às operações realizadas com criptoativos à Secretaria Especial da Receita Federal do Brasil (RFB). Diário Oficial da União. Brasília, DF, 07 maio 2019. Seção 1, p. 14.

Consolidated version of the Treaty on the Functioning of the European Union OJ C 326, 26.10.2012, p. 47–390.

Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information OJ L 271, 24.10.2000, p. 4–6.

Décret n° 2019-1213 du 21 novembre 2019 relatif aux prestataires de services sur actifs numériques, JORF n° 0271 du 22 novembre 2019.

Decreto Legislativo 21 novembre 2007, n. 231, GU n. 290 del 14-12-2007.

Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC OJ L 337, 23.12.2015, p. 35-127.

Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC OJ L 141, 5.6.2015, p. 73–117.

Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU OJ L 156, 19.6.2018.

Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing OJ L 309, 25.11.2005, p. 15–36.

Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC OJ L 267, 10.10.2009, p. 7–17.

Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC.

Gesetz zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie, Vom 12. Dezember 2019 (BGBl. I S. 2623).

Measures Against Money Laundering Act.

Regulation (EU) 2019/2175 of the European Parliament and of the Council of 18 December 2019 amending Regulation (EU) No 1093/2010 establishing a European Supervisory Authority (European Banking Authority), Regulation (EU) No 1094/2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority), Regulation (EU) No 1095/2010 establishing a European Supervisory Authority (European Securities and Markets Authority), Regulation (EU) No 600/2014 on markets in financial instruments, Regulation (EU) 2016/1011 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investment funds, and Regulation (EU)

2015/847 on information accompanying transfers of funds PE/75/2019/REV/1 OJ L 334, 27.12.2019, p. 1–145.

The Money Laundering and Terrorist Financing (Amendment) Regulations 2019.

References

Aleksandra Bal, *Taxation, Virtual Currency and Blockchain* (Wolters Kluwer 2018).

Alexander Snyers and Karl Pauwels, 'ICOs In Belgium: Down the Rabbit Hole into Legal No Man's Land? Part 1' (2018) 29 International Company and Commercial Law Review 483-510.

Apolline Blandin and others, *Global Cryptoasset Regulatory Landscape Study* (Cambridge Centre for Alternative Finance 2019).

Carolin Kaiser, 'The Classification of Virtual Currencies and Mobile Payments in Terms of The Old and New European Anti-Money Laundering Frameworks', *Bitcoin and Mobile Payments: Constructing a European Union Framework* (Palgrave Macmillan 2016).

Christopher P. Buttigieg and others, 'Anti-money laundering regulation of crypto assets in Europe's smallest member state' (2019) 13 Law and Financial Markets Review 211-227.

Commission, Directorate-General for Financial Stability, Financial Services and Capital Markets Union, 'Minutes of The Meeting, Payment Systems Market Expert Group' (2014).

Commission, 'Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border situations' COM (2017) 340 final.

Daniel Adeoyé Leslie, *Legal Principles for Combatting Cyberlaundering* (Springer 2014).

David Carlisle and Kayla Izenman, 'Closing the Crypto Gap: Guidance for Countering North Korean Cryptocurrency Activity in Southeast Asia', Royal United Services Institute for Defence and Security Studies Occasional Paper, April 2019.

David Connell, 'Do EU Regulations Combating Money Laundering and the Financing of Terrorism adequately tackle Cryptocurrencies? The case of Ireland' (2018) 21 Irish Journal of European Law 68-90.

Dirk A. Zetzsche and others, 'The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators' (2019) 60 Harvard International Law Journal 267-315.

Domenico Siclari, 'Anti-Money Laundering EU Law and Network of Agents', *The New Anti-Money Laundering Law: First Perspectives on the 4th European Union Directive* (Palgrave Macmillan 2016).

Edgar G. Sanchez, 'Crypto-Currencies: The 21st Century's Money Laundering and Tax Havens' (2017) 28 University of Florida Journal of Law and Public Policy 167-191.

'EU Members Adopt Tougher Crypto Rules Than AML Directive Requires' (*Financial Accountant*, 2019) <https://www.financialaccountant.co.uk/news/eu-members-adopt-tougher-crypto-rules-than-aml-directive-requires> accessed 4 May 2020.

Eugenia Macchiavello, 'FinTech Regulation from A Cross-Sectoral Perspective', *European Financial Regulation: Levelling the Cross-Sectoral Playing Field* (Hart 2019).

European Banking Authority, 'Opinion On ‘Virtual Currencies’' (2014).

European Central Bank Crypto-Assets Task Force, 'Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures', ECB Occasional Paper Series No 223/May 2019.

European Central Bank, 'Opinion of the European Central Bank of 12 October 2016 on a proposal for a directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC' (2016).

European Central Bank, 'Virtual Currency Schemes' (2012).

European Parliament, 'Cryptocurrencies and Blockchain: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion' (2018).

European Parliament, 'Virtual currencies and terrorist financing: assessing the risks and evaluating responses' (2018).

European Securities and Markets Authority, 'Advice: Initial Coin Offerings and Crypto-Assets' (2019).

European Union Agency for Law Enforcement Cooperation, 'Changes in modus operandi of Islamic State terrorist attacks' (2016).

European Union Agency for Law Enforcement Cooperation, 'Internet Organised Crime Threat Assessment' (2019).

Financial Action Task Force and Council of Europe, 'Money Laundering Through Money Remittance and Currency Exchange Providers' (2010).

Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' (2019).

Financial Action Task Force, 'Report on New Payment Methods' (2006).

Garrick Hileman and Michel Rauchs, *Global Cryptocurrency Benchmarking Study* (Cambridge Centre for Alternative Finance 2017).

General Secretariat of the Council of the European Union, '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' (2015).

'Guide on Privacy Coins: Comparison of Anonymous Cryptocurrencies' (*Master the Crypto: Cryptocurrency Investment Trading Guides*) <https://masterthecrypto.com/privacy-coins-anonymous-cryptocurrencies/> accessed 3 May 2020.

Jonathan Rohr and Aaron Wright, 'Blockchain-based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets' (2019) 70 Hastings Law Journal 463-524.

Joshua Kirschenbaum and Nicolas Véron, 'A better European Union architecture to fight money laundering', Bruegel Policy Contribution Issue n˚ 19, October 2018.

K. K. R. Choo, 'Cryptocurrency and virtual currency: Corruption and money laundering/terrorism financing risks?', *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data* (Academic Press 2015).

Kaido Künnapas, 'From Bitcoin to Smart Contracts: Legal Revolution or Evolution from The Perspective Of *De Lege Ferenda*?', *The Future of Law and eTechnologies* (Springer 2016).

Lars Haffke, Mathias Fromberger and Patrick Zimmermann, 'Cryptocurrencies and anti-money laundering: the shortcomings of the fifth AML Directive (EU) and how to address them' [2019] Journal of Banking Regulation.

Lindsay X. Lin, 'Deconstructing Decentralized Exchanges' [2019] Stanford Journal of Blockchain Law & Policy.

Lorna Woods, Philippa Watson and Marios Costa, *Steiner & Woods EU Law* (13th edn, Oxford University Press 2017).

M. Siems, 'A World without Law Professors', *Methodologies of Legal Research: Which Kind of Method for What Kind of Discipline?* (Hart 2011).

Malcolm Campbell-Verduyn, 'Bitcoin, Crypto-Coins, And Global Anti-Money Laundering Governance' (2018) 69 Crime, Law and Social Change 283–305.

Malte Möser, 'Anonymity of Bitcoin Transactions: An Analysis of Mixing Services', *Münster Bitcoin Conference* (2013).

Mo Egan, 'A Bit(Coin) Of A Problem for The EU AML Framework', *The Palgrave Handbook of Criminal and Terrorism Financing Law* (Palgrave Macmillan 2018).

'Money Laundering' (*Financial Action Task Force*, 2011) <https://www.fatf-gafi.org/faq/moneylaundering/> accessed 9 March 2020.

Niels Vandezande, 'Virtual Currencies Under EU Anti-Money Laundering Law' (2017) 33 Computer Law & Security Review 341-353.

Nikola Paunović, 'Terrorist Financing as The Associated Predicate Offence of Money Laundering in The Context of The New EU Criminal Law Framework for The Protection of The Financial System' [2019] EU and Member States – Legal and Economic Issues 659-683.

Noah Vardi, 'Bit by Bit: Assessing the Legal Nature of Virtual Currencies', *Bitcoin and Mobile Payments: Constructing a European Union Framework* (Palgrave Macmillan 2016).

P. Filippi, 'Bitcoin: a regulatory nightmare to a libertarian dream' (2014) 3 Internet Policy Review 1-11.

Paul Vigna and Michael Casey, *The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order* (Macmillan 2015).

Peggy Valcke, Niels Vandezande and Nathan Van de Velde, 'The Evolution of Third-Party Payment Providers and Cryptocurrencies Under the EU's Upcoming PSD2 and AMLD4', SWIFT Institute Working Paper No. 2015-001.

Philipp Hacker and Chris Thomale, 'Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies Under EU Financial Law' (2018) 15 European Company and Financial Law Review 645–696.

Philipp Maume and Mathias Fromberger, 'Regulation of Initial Coin Offerings: Reconciling U.S. and E.U. Securities Laws' (2019) 19 Chicago Journal of International Law 548-585.

Pierpaolo Fratangelo, 'The CDD Obligations Following a Risk-Based Approach', *The New Anti-Money Laundering Law: First Perspectives on the 4th European Union Directive* (Palgrave Macmillan 2016).

Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Harvard University Press 2018).

Ralf Michaels, 'The Functional Method of Comparative Law', *The Oxford Handbook of Comparative Law* (Oxford University Press 2006).

'Ransomware' (*Department of Homeland Security*) <https://www.us-cert.gov/Ransomware> accessed 5 May 2020.

Robert Hockett and Saule Omarova, 'The Finance Franchise' (2017) 102 Cornell Law Review 1143-1218.

Robert Stokes, 'Virtual Money Laundering: The Case of Bitcoin and The Linden Dollar' (2012) 21 Information & Communications Technology Law 221-236.

Simon Butler, 'Criminal Use of Cryptocurrencies: A Great New Threat or Is Cash Still King?' (2019) 4 Journal of Cyber Policy 326-345.

Thomas A. Frick, 'Virtual and Cryptocurrencies – Regulatory and Anti-Money Laundering Approaches in The European Union and In Switzerland' (2019) 20 ERA Forum 99-112.

Thomas Incalza, 'National Anti-Money Laundering Legislation in A Unified Europe: *Jyske*' (2014) 51 Common Market Law Review 1829–1850.

Valentina Covolo, 'The EU Response to Criminal Misuse of Cryptocurrencies: The Young, Already Outdated 5th Anti-Money Laundering Directive', University of Luxembourg Law Working Paper No. 2019-015.

Valsamis Mitsilegas and Bill Gilmore, 'The EU legislative framework against money laundering and terrorist finance: a critical analysis in the light of evolving global standards' (2007) 56 International and Comparative Law Quarterly 119-141.