IALS INSTITUTE OF ADVANCED LEGAL STUDIES | SCHOOL OF ADVANCED STUDY UNIVERSITY OF LONDON

Dissertation

Current Challenges and Possible Solutions for Anti-Money Laundering Regulation of Virtual Currencies in the EU and the UK.

Ekaterina Kashina
LLM in International Corporate Governance, Financial Regulation and Economic Law

Institute of Advanced Legal Studies
School of Advanced Study
University of London

2 September 2019

Table of Contents

Abstract

Cryptocurrency, a kind of a decentralised virtual currency intended to be used as a means of payment has appeared and gained momentum in recent years. It has been widely used as a speculative tool, but also for money laundering, terrorism financing and in the black market economy.

With the lack of any universal supervising authority, regulatory efforts to combat money laundering with cryptocurrency have been slow and inconsistent across jurisdictions. In the EU, it took almost ten years for it to be brought within the scope of the AML legislation. As yet untested, it is manifest that this legislation does not comprehensively address all the AML issues that cryptocurrencies create.

This dissertation provides an analysis of the AML challenges posed by cryptocurrencies, the regulatory responses to these challenges in the EU and the UK, and offers potential solutions, primarily a suggestion to incentivise AML-compliant cryptoassets through regulation.

Table of Abbreviations

AI	Artificial Intelligence
AML	Anti-Money Laundering
AMLD	EU Anti-Money Laundering Directive
ATM	Automatic Teller Machine
BCBS	Basel Committee on Banking Supervision
CDD	Customer Due Diligence
CTF / **CFT**	Counter Terrorism Financing / Counter Financing of Terrorism
DCE	Detection-Controlled Estimation
DLT	Distributed Ledger Technology
E-money	Electronic Money
EBA	European Banking Authority
ECB	European Central Bank
EMD	EU E-money Directive
ETF	Exchange Traded Funds
EU	European Union
FATF	Financial Action Task Force
FC	(Conventional) Fiat Currency
FCA	UK Financial Conduct Authority
FIU	Financial Intelligence Unit
FSB	Financial Stability Board
GDPR	EU General Data Protection Regulation
HM Treasury	Her Majesty's Treasury
ICO	Initial Coin Offering
IPO	Initial Public Offering
IMF	International Monetary Fund
ISIS	Islamic State of Iraq and Syria
KYC	Know Your Customer
MiFID	EU Markets in Financial Instruments Directive
ML	Money Laundering
MMORPG	Massively Multiplayer Online Role Playing Game
PSD	EU Payment Services Directive
SEC	US Securities and Exchange Commission
TOR	The Onion Router
UK	United Kingdom
UN	United Nations
US / **USA**	United States of America
USD	US Dollars
VAT	Value Added Tax
VC	Virtual Currency
WoW	World of Warcraft

1. Introduction.

1.1. Money Laundering from Bootlegging to Cybercrime: Legal and Historical Overview.

The offence of money laundering means secondary criminalisation of financial facilitation of criminal activities, in order to provide a disincentive to the primary crime.[1]

Although people have engaged in money laundering for a long time, the term 'money laundering' is believed to have first come into use in the 1930s to describe some of the activities of the mafia in the United States (US).[2] It is known that during prohibition, the notorious gangster Al Capone was using cash-intensive businesses, 'washing salons' (laundromats or laundrettes), to disguise and then re-introduce proceeds of the illegal alcohol trade into the legal money market, thus almost literally laundering money. In an official context, the term was used for the first time during the US Watergate scandal in the mid-1970s, and in a legal context in the United States Supreme Court decision in 1982.[3] Legislative efforts against money laundering really gained force and became international in the late 1980s, following the rapid increase in international drug trafficking.

The first convention aimed at combating money laundering was the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (adopted 20 December 1988, entered into force 11 November 1990 (Vienna Convention)), followed shortly after by the statement of the Basel Committee on 'Prevention of criminal use of the

[1] See, for example, Peter Alldridge, 'The Moral Limits of the Crime of Money Laundering' [2001] 5 Buffalo Criminal Law Review 279, 284.

[2] Friedrich Schneider and Ursula Windischbauer, 'Money Laundering: Some Facts' (2008) 26 European Journal of Law & Economics 387; Elizabeth Baker and Paul Napper, 'UK Part I: UK Money Laundering – Typological Considerations' in Arun Srivastava, Mark Simpson, and Richard Powell (eds), *International Guide to Money Laundering Law and Practice* (5th edn, Bloomsbury Professional 2019) 5; Brigitte Unger, 'Money Laundering Regulation: From Al Capone to Al Qaeda in Brigitte Unger and Daan van der Linde' (eds) *Research Handbook on Money Laundering* (Edward Elgar Publishing 2013) 19.

[3] Giannis Keramidas, 'The Legal Nature of Transnational Financial Crime' in Ilias Bantekas, Giannis Keramidas (eds), *International and European Financial Criminal Law* (LexisNexis Butterworths 2006) 22.

banking system for the purpose of money-laundering'.[4] The Financial Action Task Force (FATF) was subsequently established in 1989 and now is 'the single most important international body in terms of the formulation of AML policy and in the mobilisation of global awareness'.[5] Today, the term money laundering is widely used across all tiers of society, including academia, industry and the general public.[6]

Despite widespread use of the term, there exists no universal definition of money laundering (ML). Even more remarkable is the fact that the various definitions of money laundering keep expanding to incorporate new underlying offenses.[7] Money laundering has been intertwined with other forms of crime such as terrorism financing, drug dealing, human trafficking, theft, illegal art trading, tax evasion, counterfeiting, etc. The main characteristic of the traditional definitions of money laundering can be summed up as the legalisation of criminal proceeds.[8] FATF today defines money laundering as 'the processing of these criminal proceeds to disguise their illegal origin'.[9]

The generalised stages of a money laundering process are universally agreed upon. They are:

- placement, where the illegally obtained money is placed and mixed with legal funds;
- layering, the goal of which is the separation of the money from its illegal nature, usually through multiple transfers and other transactions;
- integration of the now 'laundered' funds into the legal economy, where it can be used on par with 'clean' money.[10]

[4] Basel Committee on Banking Supervision (BCBS), 'Prevention of Criminal Use of the Banking System for the Purpose of Money-Laundering' (28 December 1988) <https://www.bis.org/publ/bcbsc137.htm> accessed 30 July 2019.

[5] Mark Simpson and Sarah Williams, 'International Initiatives' in Arun Srivastava, Mark Simpson, and Richard Powell (eds), *International Guide to Money Laundering Law and Practice* (5th edn, Bloomsbury Professional 2019) 287.

[6] See, For example, Baker and Napper (n 2).

[7] David C. Hicks, 'Chapter 35 - Money Laundering' in Fiona Brookman et al, *Handbook on Crime* (Willan Publishing 2010) 712; Keramidas (n 3); Baker and Napper (n 2) 6.

[8] Keramidas (n 3) 23.

[9] FATF, 'Money Laundering - Financial Action Task Force (FATF)' <https://www.fatf-gafi.org/faq/moneylaundering/> accessed on 30 July 2019.

[10] Keramidas (n 3).

These traditional characteristics of money laundering, while they still exist, often appear to be challenged in the modern environment. Notably, 'the concept of money or cash is no longer a prerequisite of money laundering', which today is based on the far broader concepts of value and value transfer.[11] Similarly, the legalisation of criminal proceeds is no longer the only core process that is identified as money laundering. A large part of AML regulation now includes counter-terrorism financing, where the destination, and not the source of funds, must be illegal to constitute the offense.[12] With globalisation and the rapid rate of technological advancement, money laundering is also becoming more international and better organised than before.[13] As the reality of money laundering techniques have become ever more diverse, the traditional three-step money laundering model may not be an adequate reflection of the process in all cases.[14]

Money laundering legislation, in turn, is constantly evolving to reflect the changing environment and technological advances. In the European Union (EU), the first AML Directive entered into force in 1991, only a few years after the establishment of FATF and the first United Nations conventions against money laundering.[15] It was updated in 2001 to the 2nd AMLD.[16] The 3rd AMLD was introduced in 2003 following further changes to the FATF recommendations,[17] and in 2015 was repealed by the 4th AMLD, which was implemented into national laws in 2017.[18] However, this too was amended less than a year

[11] Baker and Napper (n 2) 6.
[12] Niels Vandezande, *Virtual Currencies: A Legal Framework* vol 1 (Intersentia 2018) 277.
[13] Keramidas (n 3) 20.
[14] Baker and Napper (n 2) 9.
[15] Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering [1991] OJ 166/77.
[16] Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering - Commission Declaration [2011] OJ L 344/76.
[17] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (Text with EEA relevance) [2005] OJ L309/15.
[18] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance) [2015] OJ L141/73 (4th AML Directive).

after the implementation by the 5th AMLD,[19] and only six months later supplemented by yet another Directive – the 6th AMLD, released in November 2018.[20]

This unusually haphazard legislative process was motivated, amongst other reasons, by the recognised need for AML regulation of virtual currencies.[21] The 5th AMLD not only includes virtual currencies within the scope of the AML regulation in the EU for the first time, but also highlights their regulation as one of the key changes.

Due to be implemented by the EU member states in January 2020, still a few months away at the time of writing, the new regulation of virtual currencies is as yet untested. Moreover, it appears to be dangerously limited in scope and not adequate for the issues that it aims to resolve.

1.2. Methodology and Terminology.

This paper will critically examine current EU and UK efforts against ML involving virtual currencies with the objective of identifying potential problems and offering possible solutions. Given the emerging nature and technical complexity of the field, it is important to start with offering sufficient explanation and background information on the phenomenon of virtual currencies and their current position in the wider economy. This will be provided in the next chapter. The following chapters will be dedicated to identifying known and possible methods of money laundering involving the use of virtual currencies and determining whether the 5th EU AMLD is capable of addressing all of them. This will be done by analyzing the ML risks and drivers and the legislative process in the EU and the UK and then reviewing the 5th AMLD and the proposed transposition guidance for the Directive in the UK. Finally, this work will propose and discuss possible solutions to the issues not addressed by the AML regulation.

[19] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance) [2018] OJ L156/43 (5th AML Directive).

[20] Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law [2018] OJ L284/22 (6th AML Directive).

[21] 5th AML Directive, recital (8).

To avoid any confusion going forward, it is worthwhile to note that there is no single set of accepted terms in the area of anti-money laundering in conjunction with the use of virtual currencies. Many notions lack canonical definitions, and a number of different names and spelling variations can be employed for the same notion. This is largely due to the innovative and hitherto dynamic nature of virtual currencies, but also to a number of other factors, such as differences in legal tradition in different jurisdictions. To start with, 'money laundering' can often refer to 'anti-money laundering' in legal literature. Commonly abbreviated as ML and AML respectively, the terms can be used interchangeably. Counter terrorism financing and counter financing of terrorism refer to exactly the same notion, and are abbreviated as either CTF or CFT.

The terms 'virtual currency', 'cryptocurrency' and 'cryptoasset' also can refer to the same concept and are often used interchangeably, although there are differences in meaning. Neither of these terms have a standardised definition, and spelling variations are also common. Even the name of the best known cryptocurrency, bitcoin, can be both capitalised and not. This paper will be using the spelling currently adopted by the Oxford Dictionary and/or UK regulators – 'cryptocurrency', 'cryptoasset' and 'bitcoin'.[22]

[22] 'cryptocurrency, n' (*Lexico.com)* <https://www.lexico.com/en/definition/cryptocurrency>; 'bitcoin, n' (*Lexico.com)* <https://www.lexico.com/en/definition/bitcoin> accessed 5 August 2019. 'Cryptoasset' is not included in the Oxford Dictionary at the time of writing, however this is the accepted spelling in the UK regulatory papers, for example, HM Treasury, 'Transposition of the Fifth Money Laundering Directive: consultation' (April 2019) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/795670/20190415_Consultation_on_the_Transposition_of_5MLD__web.pdf> accessed 12 May 2019.

2. The Phenomenon of Virtual Currencies.

2.1. Definitions and Typology.

The EU gave its very first, and possibly the best to date, legal definition of virtual currencies in the 5th AMLD in 2018:

> *'(18) "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.*[23]

This definition appears to stem from the earlier, 2014 definition by the European Banking Authority (EBA).[24] It is obvious that this definition is not comprehensive or precise, introducing multiple options such as 'currency *or* money' and broad characteristics such as 'not *necessarily* attached'. It also partly defines virtual currencies by negation, characterising them through what they are not. This is problematic, meaning that the definition will likely require revisions every time a new entity, similar to the others that are negated, appears. This is far from unlikely in a rapidly developing field. Yet this definition also serves as a good example of the difficulties in systematisation of this field in general.

It is important to point out that the classification of virtual currencies is undeveloped. There are no universal definitions, and each regulatory body or government tends to create, and often recreate, their own definitions.[25] These definitions can even become quite

[23] 5th AML Directive, art 1 (2)(d).

[24] EBA, 'EBA Opinion on 'virtual currencies' (4 July 2014) 5 <https://eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf> accessed 7 August 2019.

[25] For example, compare the ECB definition in 2012 and in 2015. In 2012, ECB defined virtual currencies as *'a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community'* – see ECB, 'Virtual Currency Schemes' (October 2012) 5 <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> accessed 3 August 2019. In 2015, the ECB definition was '*a digital representation of value, not issued by a central bank,*

contradictory. For example, the established view in the EU is that virtual currencies fall within a larger group of digital currencies, which also includes e-money. Conversely, the accepted US view is the opposite - 'digital currencies are considered a subset of virtual currencies that only exist in electronic form'.[26]

When defining virtual currencies, it is important to highlight that in the EU virtual currencies are not legally considered money. This includes electronic money (e-money), although there are views that some forms of cryptocurrencies can be classified as e-money.[27] Money, or fiat currency, must be a legal tender, issued and guaranteed by the state, and e-money is its digital representation, exchangeable for a fiat currency.[28] Since no public authority can issue and guarantee a virtual currency due to decentralized nature, it is explicitly distinguished from money.

Virtual currencies can be further classified based on their scheme of operation and issuer. There are multiple types of virtual currencies: some can be both purchased and exchanged for legal tender - notably cryptocurrencies, some can be purchased but not exchanged back for legal tender, such as Amazon Coins, and some can be neither purchased nor exchanged and operate within a wholly closed system, such as in-game currencies in Massively Multiplayer Online Role Playing Games (MMORPGs), for example 'Gold' in World of Warcraft (WoW).[29] Depending on the issuer, virtual currencies can be either centralized, where they are controlled by a single issuer, for example WoW Gold, issued and controlled by the developer of the game Blizzard Entertainment, or decentralized, such as bitcoin and most other cryptocurrencies.[30]

credit institution or e-money institution, which in some circumstances can be used as an alternative to money' – see ECB, 'Virtual Currency Schemes: A Further Analysis' (February 2015) 4 <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> accessed 3 August 2019.

[26] Vandezande (n 12) 32.

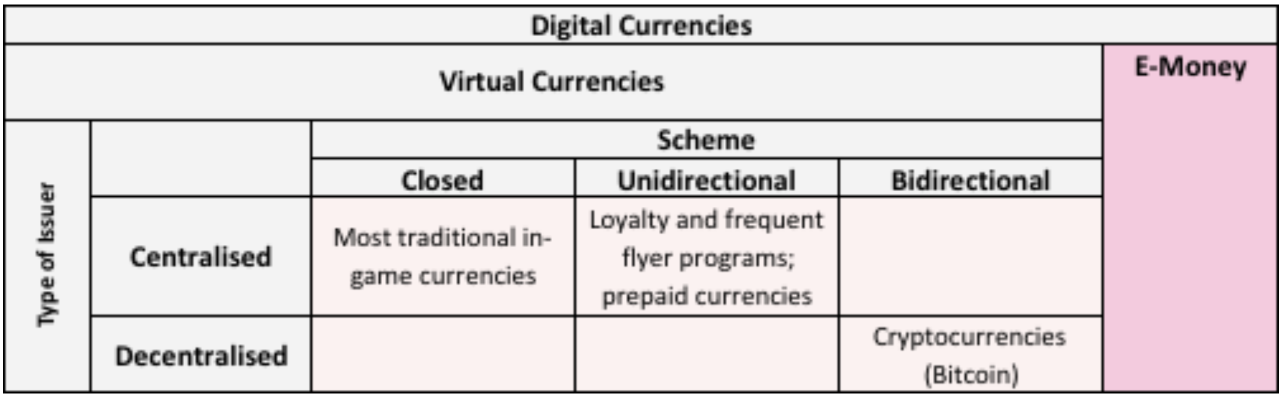
[27] EBA, 'Report with advice for the European Commission on crypto-assets' (9 January 2019) 12 <https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf> accessed 9 August 2019.

[28] Vandezande (n 12) and EBA (n 24).

[29] Niels Vandezande, 'Virtual Currencies under EU Anti-money Laundering Law' [2017] 33 Computer Law and Security Report 341; Vandezande (n 12) 42-43.

[30] Vandezande (n 12) 43 and 58; Viktor Dostov and Pavel Shust, 'Evolution of the Electronic Payment Industry: Problems of a Qualitative Transition' [Виктор Достов и Павел Шуст, 'Эволюция Отрасли Электронных Платежей: Проблемы Качественного Перехода'] (Working Paper, Russian Presidential Academy of National

Figure 1. The Typological Summary of Digital and Virtual Currencies in the EU.



Digital Currencies					
Virtual Currencies					E-Money
Type of Issuer		Scheme			
		Closed	Unidirectional	Bidirectional	
	Centralised	Most traditional in-game currencies	Loyalty and frequent flyer programs; prepaid currencies		
	Decentralised			Cryptocurrencies (Bitcoin)	

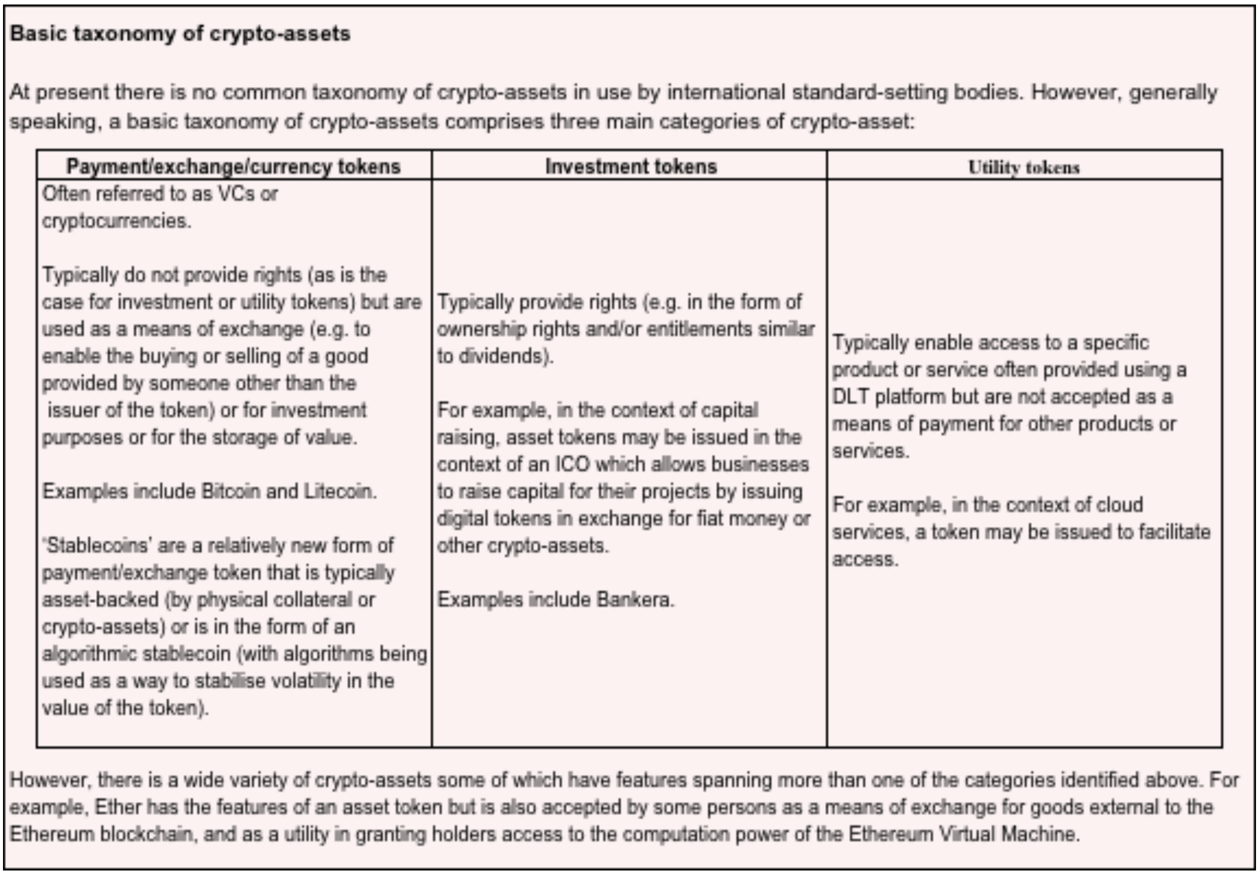
Going further, there is currently a growing view that the term cryptocurrencies may not be the most accurate description of the notion, since their application on par with traditional currencies is quite limited. Instead, they should be regarded as 'financial assets', and some researchers are operating with the term 'cryptoassets' as a result.[31] Additionally, recent developments have allowed the extension of the notion of 'cryptoassets' beyond just cryptocurrencies to include 'investment tokens' and 'utility tokens'.[32]

Economy and Public Administration, May 2017) 33 <ftp://w82.ranepa.ru/rnp/wpaper/051713.pdf> accessed 28 March 2019.

[31] For example, Vandezande (n 12) 34; Dr. Richard Alexander, 'Editorial – How to Regulate Bitcoin – the Debate Continues' [2018] 39 (3) Company Lawyer 65.

[32] EBA, 'Report with advice for the European Commission on crypto-assets' (n 27) 7.

Figure 2. EBA's 'Basic Taxonomy of Crypto-assets'.[33]



Basic taxonomy of crypto-assets

At present there is no common taxonomy of crypto-assets in use by international standard-setting bodies. However, generally speaking, a basic taxonomy of crypto-assets comprises three main categories of crypto-asset:

Payment/exchange/currency tokens	Investment tokens	Utility tokens
Often referred to as VCs or cryptocurrencies. Typically do not provide rights (as is the case for investment or utility tokens) but are used as a means of exchange (e.g. to enable the buying or selling of a good provided by someone other than the issuer of the token) or for investment purposes or for the storage of value. Examples include Bitcoin and Litecoin. 'Stablecoins' are a relatively new form of payment/exchange token that is typically asset-backed (by physical collateral or crypto-assets) or is in the form of an algorithmic stablecoin (with algorithms being used as a way to stabilise volatility in the value of the token).	Typically provide rights (e.g. in the form of ownership rights and/or entitlements similar to dividends). For example, in the context of capital raising, asset tokens may be issued in the context of an ICO which allows businesses to raise capital for their projects by issuing digital tokens in exchange for fiat money or other crypto-assets. Examples include Bankera.	Typically enable access to a specific product or service often provided using a DLT platform but are not accepted as a means of payment for other products or services. For example, in the context of cloud services, a token may be issued to facilitate access.

However, there is a wide variety of crypto-assets some of which have features spanning more than one of the categories identified above. For example, Ether has the features of an asset token but is also accepted by some persons as a means of exchange for goods external to the Ethereum blockchain, and as a utility in granting holders access to the computation power of the Ethereum Virtual Machine.

2.2. Cryptocurrency Market and Market Share.

At the time of writing, in August 2019, the total number of known cryptocurrencies is estimated at 2454,[34] thus representing a rapid growth from just one (bitcoin) in January 2009 and 584 in July 2015.[35] Their combined market share in wider economy is relatively small, with just over USD$273 bn in market capitalisation.[36]

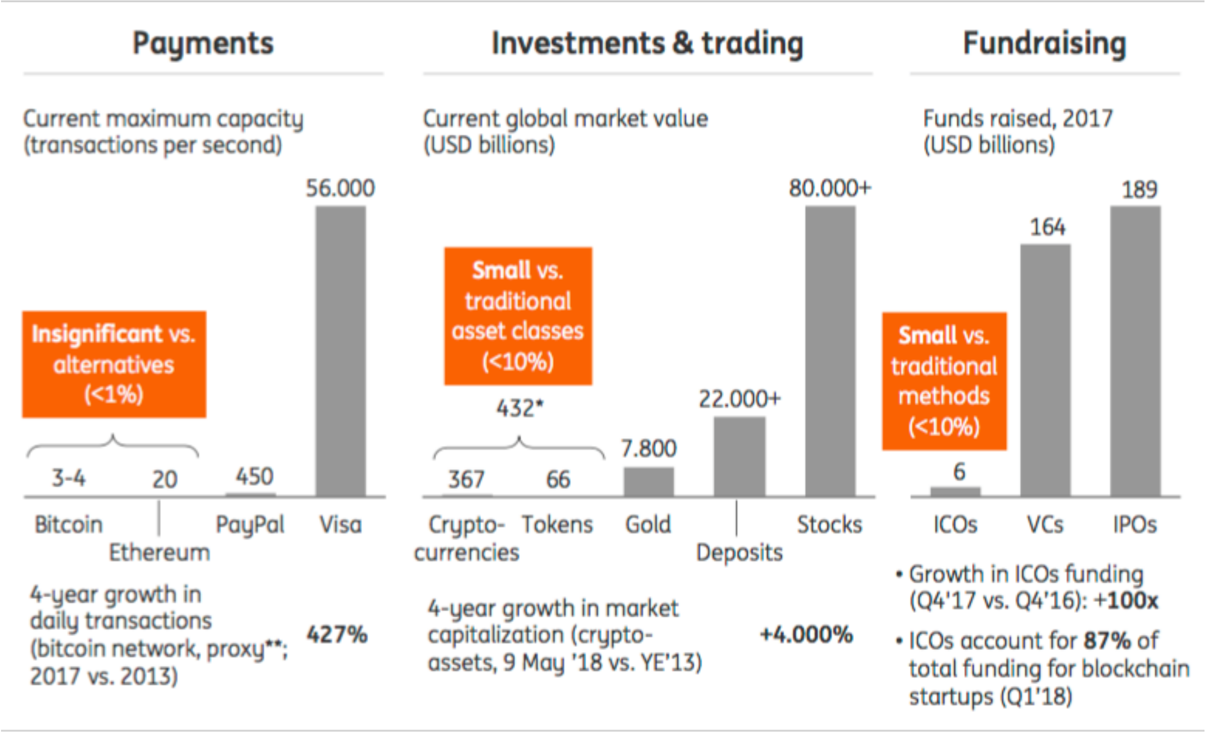
[33] Ibid.

[34] CoinMarketCap, 'Cryptocurrency Market Capitalizations' (Coinmarketcap.com 18 August 2019) <https://coinmarketcap.com/> accessed 18 August 2019.

[35] Angela S. M. Irwin and George Milad, 'The Use of Crypto-Currencies in Funding Violent Jihad' [2016] 19 Journal of Money Laundering Control 407, 412.

[36] CoinMarketCap (n 34).

Figure 3. ECB Summary of Crypto-Assets Market.[37]



Notably, only one cryptocurrency, bitcoin, makes up almost 70% of the cryptocurrency market share. While this largely depends on the value of bitcoin, which fluctuates wildly, historically the bitcoin market share also was very high, at around 50%.[38] This allows to conclude that while the cryptocurrencies' market is rapidly developing with new cryptocurrencies being created at an ever-accelerating rate, it is equally remaining relatively stable with one clearly dominant product.

2.3. Historical Background and the Emergence of Blockchain.

Virtual currencies, and cryptocurrencies in particular, came to prominence in the financial world after the birth of bitcoin, which was announced in 2008 and launched the next year.[39]

[37] European Central Bank (ECB), 'Cryptocurrencies and Tokens' (September 2018) 7 <https://www.ecb.europa.eu/paym/groups/pdf/fxcg/2018/20180906/Item_2a_-_Cryptocurrencies_and_tokens.pdf> accessed 30 July 2019.

[38] CoinMarketCap (n 34); Irwin and Milad (n 35) 412.

[39] Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (<www.bitcoin.org>, allegedly 31 October 2008) <https://bitcoin.org/bitcoin.pdf> accessed 30 July 2019. The paper is not dated, and believed to be first published online on the above date. (See, for example, Klint Finley, 'After 10 Years Bitcoin Changed

Bitcoin is an open source cryptocurrency network with a public design. This has allowed numerous other cryptocurrencies to follow in its wake. The growth of new cryptocurrencies became rapid from 2011, after bitcoin became better known.[40] Cryptocurrencies have been treated as a great invention and received a huge amount of attention. However, it would be a misconception to think that they appeared out of thin air. The underlying technology was largely pre-existing, as well as a number of somewhat similar, yet far less known currencies.[41]

Early predecessors of cryptocurrencies originated on the Internet and were attempts to bring 'existing schemes such as loyalty programs and prepaid cards online as a means of transferring money'.[42] There have been a number of cryptographic currencies before bitcoin, too. Notably, DigiCash, first proposed in 1982, was also used for 'real-life transactions'.[43] Additionally, cryptographic protection has been overwhelmingly used in payment technologies, and it is not uncommon for the funds to be stored in a decentralised manner, as opposed to a centralised storage.[44]

The one radically different aspect of bitcoin and the following cryptocurrencies is that they do not rely 'on trust'.[45] This means that they do not depend on third party intermediaries to police the double spend problem, but use the distributed ledger technology (DLT) in the form of a 'blockchain' instead. 'DLT enables the storage, update and validation of information in a decentralised way', and blockchain is one, although the best known, [i]example of DLT.[46] The transactional record system is therefore decentralised, meaning that the whole chain is stored on all computers participating in the network, as opposed to one central authority.

Everything and Nothing' (*Wired*, 31 October 2018) <https://www.wired.com/story/after-10-years-bitcoin-changed-everything-nothing/> accessed 30 July 2019.) Bitcoin was released on 9 January 2009, see email from Satoshi Nakamoto to the Cryptography Mailing List 'Bitcoin v0.1 released' (9 January 2009) <Mail-archive.com/cryptography@metzdowd.com/msg10142.html> accessed 7 August 2019.

[40] Vandezande (n 12) 53.

[41] Finley (n 39); Victor Dostov and Pavel Shust, 'Cryptocurrencies: An Unconventional Challenge to the AML/CFT Regulators?' [2014] 21 Journal of Financial Crime 249.

[42] Vandezande (n 12) 51.

[43] Dostov and Shust (n 30).

[44] Dostov and Shust (n 41) 249-250.

[45] Nakamoto (n 39) 8.

[46] EBA, 'Report with advice for the European Commission on crypto-assets' (n 27) 8.

In traditional payment methods, a new transaction cannot be completed before some verification that the money is there to be spent. Blockchain for the first time allowed for this verification to be done by the public actors (peers) 'without relying on the gatekeepers'.[47] This shift of trust from the gatekeepers to the network itself proved more than merely symbolic.

Unsurprisingly, there is no single and universally accepted definition of blockchain.[48] Blockchain can be described as an immutable sequence of blocks of data containing cryptographically encrypted information about each transaction in the cryptocurrency network. The verification of transactions is performed by the cryptographic calculation produced by nodes on the network. These nodes, typically called 'miners', corroborate each transaction and are rewarded for their work as each new block is defined to be a unique transaction which instantiates a new coin inherited by the creator of the block.[49] Thereby bitcoin and other similar cryptocurrencies utilising a DLT are a system which both enables peer-to-peer validation of transactions, and also 'by relying on computer science and economics...induces participation in the network and disincentives cheating'.[50] Any attempt at a fraudulent entry by one participant will be immediately disputed by other participants who did not record it.

Remarkably, even the main principle behind the DLT is not as ground-breaking as it may seem. The first known equivalent of a distributed ledger for monetary transactions was used on Yap Island in Micronesia. Money on the island was represented by large circular stones 13 feet in diameter, with a hole in the middle. With change of ownership, they were not transported but kept in the same place due to their size. 'The ownership rights were transferred virtually' and the information about each transaction was communicated to all

[47] Finley (n 39).
[48] Dostov and Shust (n 30) 34.
[49] Nakamoto (n 39) 4.
[50] Oleg Stratiev, 'Cryptocurrency and Blockchain: How to Regulate Something We Do Not Understand' [2018] 33 Banking and Finance Law Review 187.

the inhabitants of the island, who were then able to police any misconduct, similar to the DLT.[51] Interestingly,

> *The separation between the unit of value and the stone went so far that even the unit of value for stones that were lost at sea remained in circulation. The stone money of Yap can therefore be described as a quasi- virtual currency, as each unit of value was only loosely linked to a physical object.*[52]

DLT and blockchain differ from the Yap Island system by employing computerised technology, thus overcoming the limitations of human memory and communication.

2.4. Overview of the Legal Status of Cryptocurrencies around the World.

The regulation of cryptocurrencies shows a great divergence. It significantly varies between jurisdictions both in the accepted legal status of cryptocurrencies and in regulatory models – from an implicit ban on ownership and trade (China) to acceptance as a means of payment (Japan, Switzerland).[53] Around the globe, cryptocurrencies can be regarded as goods, commodities, securities, assets and money. Their legal status and regulation has also considerably evolved with time, sometimes becoming a complete opposite to the initially proposed. Most countries, however, have adopted a somewhat cautious approach, often placing cryptocurrencies into a grey area, at least initially.

[51] Aleksander Berentsen and Fabian Schar, 'A Short Introduction to the World of Cryptocurrencies' [2018] 100 Federal Reserve Bank of St. Louis Review 1, 3. See also M. L. Berg, 'Yapese Politics, Yapese Money and the Sawei Tribute Network before World War I' [1992] 27 (2) The Journal of Pacific History 150; Dostov and Shust (n 30) 32.

[52] Berentsen and Schar (n 51) 3.

[53] Oxford Analytica, 'Cryptocurrency regulations will vary' (Oxford Analytica Daily Brief, 10 May 2018) https://dailybrief.oxan.com/Analysis/DB233665/Cryptocurrency-regulations-will-become-more-variable accessed 5 August 2019; Matthew Allen, 'Swiss Luxury Brands Embrace Bitcoin' (SWI swissinfo.ch, 27 March 2019) <https://www.swissinfo.ch/eng/business/payment-solution_swiss-luxury-brands-embrace-bitcoin/44854604> accessed 20 August 2019.

Figure 4. Examples of Regulation of Cryptocurrencies in Selected Jurisdictions.[54]

Regulatory Model	Details	Countries
Ban on usage.	Purchase, sale, exchange or other use of cryptocurrencies is illegal.	Bangladesh, Bolivia, Ecuador
Ban on usage by legal persons.	Purchase, sale, exchange or other use of cryptocurrencies by financial firms, payment companies, etc. is illegal.	China
Treated as goods or securities.	Transactions involving cryptocurrencies are taxed as transactions involving sale or purchase of goods; profits from sale of cryptocurrency can be taxed as income from securities.	Argentina
Varies between states.	Can be treated and/or taxed as securities, commodity, property or currency.	USA
Treated as currency.	Considered a currency for tax purposes, the exchange of cryptocurrency for fiat currency is exempt from VAT.	Australia, European Union
Warning on usage of cryptocurrencies.	Legal status not clearly defined, Central Bank warning on usage due to ML risks.[55]	Russia
Not regulated.		Cyprus, Turkey[56]

[54] Based on Dostov and Shust (n 30) 48-52.

[55] The Central Bank of the Russian Federation (Bank of Russia), Пресс-служба Банка России, "Об Использовании При Совершении Сделок «виртуальных Валют», в Частности, Биткойн" (27 January 2014) <https://www.cbr.ru/press/PR/?file=27012014_1825052.htm> accessed 3 August 2019.

[56] The Library of Congress, 'Regulation of Bitcoin in Selected Jurisdictions' (June 2018) <https://www.loc.gov/law/help/bitcoin-survey/> accessed 5 August 2019.

A fitting conclusion to this Chapter is the recent statement by the ECB Crypto-Assets Task Force:

> *At the time of writing, the legal status of crypto-assets varied among countries, absent a common taxonomy of crypto-assets, and a shared understanding of how crypto-assets should be treated from a regulatory standpoint.*[57]

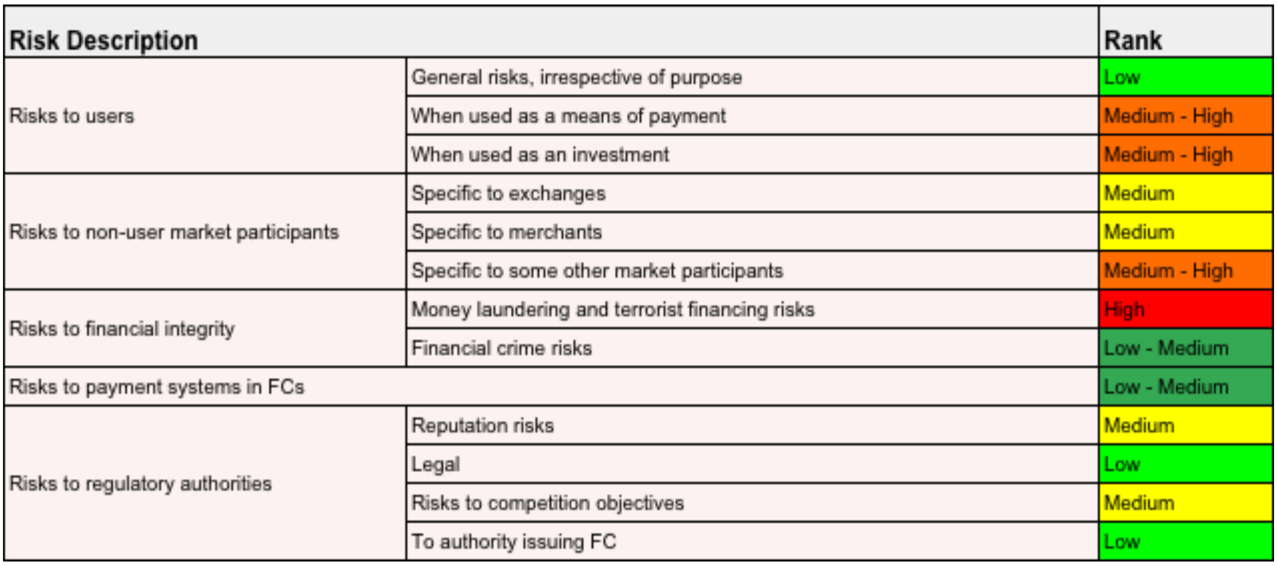
[57] ECB, ECB Crypto-Assets Task Force, 'Crypto-Assets:
Implications for financial stability, monetary policy, and payments and market infrastructures' (Occasional Paper Series No 223 May 2019) 28 <https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf> accessed 5 August 2019.

3. AML Challenges Posed by Virtual Currencies.

3.1. The Risk of Money Laundering Using Virtual Currencies.

One of the most comprehensive EU reports on financial risks posed by virtual currencies, compiled in 2014 by the EBA, found that 'approximately 70 risks can be identified as arising from VCs. Some of these are similar … to risks arising from conventional financial services or products … while others are specific to VCs'.[58] The areas with the highest risk levels are those of user risks in general and when cryptocurrencies are used as means of payment, as well as financial integrity risks, i.e. risks of financial crime and money laundering.

Figure 5. Highest Risk Areas based on the EBA's 'Overview of Risks'.[59]

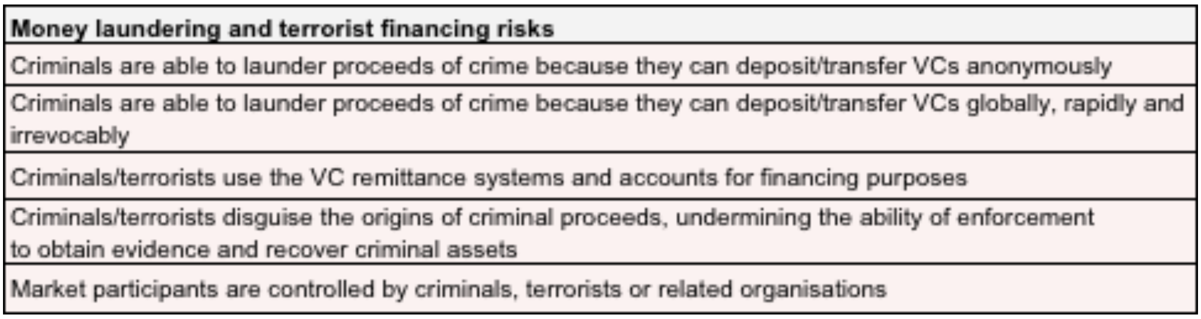


Risk Description		Rank
Risks to users	General risks, irrespective of purpose	Low
	When used as a means of payment	Medium - High
	When used as an investment	Medium - High
Risks to non-user market participants	Specific to exchanges	Medium
	Specific to merchants	Medium
	Specific to some other market participants	Medium - High
Risks to financial integrity	Money laundering and terrorist financing risks	High
	Financial crime risks	Low - Medium
Risks to payment systems in FCs		Low - Medium
Risks to regulatory authorities	Reputation risks	Medium
	Legal	Low
	Risks to competition objectives	Medium
	To authority issuing FC	Low

The only area in the report with all risks marked as 'High' is that of money laundering and terrorist financing. The EBA has identified the following ML risks for VCs:

[58] EBA, 'EBA Opinion on 'virtual currencies' (n 24) 5.
[59] Ibid 22.

Figure 6. ML and TF Risks of Virtual Currencies as Established by the EBA.[60]



Money laundering and terrorist financing risks
Criminals are able to launder proceeds of crime because they can deposit/transfer VCs anonymously
Criminals are able to launder proceeds of crime because they can deposit/transfer VCs globally, rapidly and irrevocably
Criminals/terrorists use the VC remittance systems and accounts for financing purposes
Criminals/terrorists disguise the origins of criminal proceeds, undermining the ability of enforcement to obtain evidence and recover criminal assets
Market participants are controlled by criminals, terrorists or related organisations

These risks arise mainly from the use of the decentralised cryptocurrencies, since they are the ones most integrated into the mainstream economy, and therefore vulnerable to ML.[61] Closed scheme virtual currencies 'have no integration with the physical world economy', and unidirectional scheme virtual currencies are 'not allowing money to flow out of the system',[62] and so cannot be effectively employed for ML.

The significance of the ML risks is further confirmed by the empirical data. While it is not possible to accurately measure the scale of money laundering in any economy for obvious reasons, it is estimated that the proportion of cryptocurrency involved in criminal activities is high. It was found that 'approximately one-fifth (23%) of the total dollar value of transactions and approximately one-half of bitcoin holdings (49%) through time are associated with illegal activity'.[63] In 2017, this amounted to approximately USD$76 billion in transactional value, which is comparable to the size of the illegal drugs markets in the EU and in the US.[64]

Additionally, it has been demonstrated that the efficiency of money laundering via bitcoin can considerably exceed that of 'traditional' methods: up to 85% in returns compared to

[60] Ibid.

[61] Vandezande (n 12) 278 – 279.

[62] Ibid.

[63] Sean Foley, Jonathan R Karlsen, Tālis J Putniņš, 'Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?' [2019] 32 The Review of Financial Studies 1798.

[64] Ibid.

around 50%.[65] On top of the high return rate, the turnaround time of money laundering on the dark web can be very quick and measured in hours, versus months or years for more traditional methods.[66] It should be noted however that this area is not very well understood, and cannot be measured precisely.

Cryptocurrencies are also purposefully used for terrorism financing, including that of ISIS. ISIS supporters were convicted for providing instructions on how to use cryptocurrencies for terrorist financing on Twitter.[67] Terrorist supporters posted YouTube videos, online articles and links to forums explaining how bitcoin can be used for terrorism financing. While we may never be completely certain of this, there is a considerable evidence of cryptocurrencies being used for successful terrorist attacks, including in Paris on 13 November 2015, resulting in 131 deaths and over 400 injured.[68] The most recent major terrorist attack allegedly funded through bitcoin appears to be the suicide bombing in Sri Lanka on Easter Sunday 2019.[69]

3.2. Drivers Behind Money Laundering Using Virtual Currencies.

This chapter will provide an overview of the main drivers behind these ML risks, supplemented by the description of the known ML technologies where cryptocurrency is used. The absolute majority of *known* techniques involves bitcoin, it being the easiest to use, most popular and widespread cryptocurrency with the largest market capitalisation.

[65] Rolf van Wegberg, Jan-Jaap Oerlemans, Oskar van Deventer, 'Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin' [2018] 25 Journal of Financial Crime 419, 430.

[66] Ibid 428.

[67] FATF, 'Emerging Terrorist Financing Risks' (FATF Report, October 2015) 36 <https://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf> accessed 10 August 2019.

[68] Irwin and Milad (n 35) 410.

[69] Yashu Gola, 'ISIS Used Bitcoin to Fund Horrific Sri Lanka Easter Bombings, Research Claims' (*CCN Markets*, 2 May 2019) <https://www.ccn.com/isis-bitcoin-fund-sri-lanka-easter-bombings/> accessed 28 August 2019.

3.2.1. Anonymity.

Perhaps the most obvious driver of cryptocurrency-based ML is that of anonymity. Anonymity is possible both at the stage of 'registering' for a cryptocurrency network, and at a point of exchange of cryptocurrency for a fiat currency, making the system very attractive for ML schemes. To be able to buy and sell bitcoin, a user needs to first set up a bitcoin wallet, of which there are a few types. The wallet will then create a bitcoin address, through which the currency is traded. Importantly, the user can create as many addresses as they like, even a new one for each transaction.[70] Unlike traditional bank accounts or online wallets, bitcoin addresses are not necessarily registered to the user's personal details – both bitcoin wallets and addresses can be anonymous. 'Comparable with numbered Swiss banking accounts, the bitcoin address itself acts as a unique identifier and the account is only accessible by the owner who has the login details to the bitcoin wallet.'[71]

While established cryptocurrency exchanges normally perform KYC, anonymous conversion of cryptocurrency to fiat currency and vice versa is still possible through bitcoin ATMs outside of regulated jurisdictions, face-to-face exchanges, the dark web and schemes involving third-party accounts, such as 'a third-party website or using a third-party service where the purchaser deposits cash directly into the company's nominated bank account and then the company deposits Bitcoins into the purchaser's nominated Bitcoin wallet'.[72]

This anonymity has a significant loophole, however, as all transactions with bitcoin are logged on the publicly accessible blockchain, available to anyone and at any given moment. All bitcoin transactions are also traceable to each preceding transaction. With each bitcoin address, a user gets a public and a private cryptographic keys, used to verify translations. The public keys are logged on the blockchain. It is therefore possible to track which public keys were used and where, thus allowing for further analysis and the linking of the transactions to those outside of the cryptocurrency network. Potentially, this can result in the identification of individual users, rendering the cryptocurrency network only pseudo-

[70] See, for example, Irwin and Milad (n 35) 412.
[71] van Wegberg, Oerlemans, van Deventer (n 66) 419.
[72] Irwin and Milad (n 35) 414.

anonymous in reality. Indeed, this technique allowed to identify cryptocurrency units belonging to the owner and founder of the notorious 'Silk Road' dark web marketplace, where illicit goods and ML services were traded for bitcoin.[73]

In turn, to solve the problem of bitcoin transactional visibility, a key service has become available on the dark web which provides the layering in a ML scheme – the so-called 'Bitcoin Mixer' or simply a 'mixing service'. Some mixing services allow complete anonymity, as described below. The objective of the cryptocurrency mixing service is to sever the money-trail of bitcoin transactions. This is typically achieved by the mixing service providing a newly created wallet address for the customer to transfer the 'tainted' currency to. Following this, the service pays out other bitcoins from its reserve to another wallet address provided by the customer, minus a fee which can be as little as 3%. As a result, the final bitcoins sent to the customer are dissociated from those sent to the mixing service and from their criminal source.[74]

Both the criminals and the authorities are able to accurately measure the traceability or 'taint' of cryptocurrency back to that originally deposited by inspecting the blockchain. 'If the bitcoin mixing is performed correctly, there is no link ("zero per cent taint")'[75], and therefore complete anonymity is achieved. With both the relatively low fee and a quantifiable level of anonymity, it is no wonder that 'bitcoins are therefore to be seen as the preferred currency of criminals'.[76]

In addition to this, internet privacy tools, such as TOR (The Onion Router) can be used to browse the Internet and to access a cryptocurrency network anonymously. It is possible that a combination of TOR with any mixing service also results in complete anonymity.[77] With TOR, 'an underground economy has emerged that is based on buying and selling criminal techniques and services on the Internet'.[78]

[73] Coindesk, 'Silk Road Timeline' (*CoinDesk* (blog) 3 October 2014) <https://www.coindesk.com/silk-road-timeline> accessed 20 August 2019.
[74] Ibid 423-426.
[75] Ibid 423.
[76] Ibid.
[77] Irwin and Milad (n 35) 419.
[78] van Wegberg, Oerlemans, van Deventer (n 66) 421.

Another common way to preserve anonymity when transacting cryptocurrency is to use underground exchanges. Their purpose is very similar to that of their 'white-label' counterparts, that is to convert cryptocurrency into a fiat or other currency, except with the added protection of the clients' anonymity.[79] It has been shown that it is possible to anonymously 'exchange' cryptocurrency into money on accounts with such established services as PayPal and Western Union, thus integrating laundered funds into the truly mainstream economy.[80]

3.2.2. 'Digitalisation' of the Black Market.

When considering money laundering using (pseudo)anonymous cryptocurrencies, it is logical to make a connection of this model with that of fungible cash transactions, often anonymous and untraceable. However, this would not be a very accurate analogy, exactly because cryptocurrencies are not cash. A more precise analogy would be that of cryptocurrencies and *e-money that became anonymous*. Similarly to e-money, cryptocurrencies allow the transition of a physical marketplace to an online realm, except this marketplace can now include the black market.[81] Previously, the black market could not be moved online without revealing the identity of its participants through the online payment methods that they used, but cryptocurrencies have for the first time allowed for anonymous online transactions.

Just like online shopping has revolutionised 'the structure of retailing, consumption patterns, choice, marketing, competition, and ultimately supply and demand', cryptocurrencies now 'have the potential to cause an important structural shift in how the black market operates'.[82] Of course, this could be a very dangerous development. There are notorious examples of now-defunct dark web marketplaces, such as Silk Road and AlphaBay, where the amount of money in circulation was measured in billions of dollars.[83] Proceeds

[79] Ibid 421.

[80] Ibid 429.

[81] Foley, Karlsen, Putniņš (n 63).

[82] Ibid.

[83] Coindesk, 'Silk Road Timeline' (*CoinDesk* (blog) 3 October 2014) <https://www.coindesk.com/silk-road-

from criminal activities, whether originating in fiat currency or in bitcoin itself can be laundered through ML schemes on the dark web, increasing its attractiveness for criminals and perpetuating crime.

3.2.3. Cross-Border Nature of the Network.

While it has always been relatively easy to move cash within one country for ML purposes, moving illicit funds across borders in any form is a lot more complex. As described, the cryptocurrency network is cross-border, allowing criminals to circumvent capital controls and government actions.[84] 'For money laundering purposes, a crypto-wallet is even better than cash because once the bitcoin is mined or purchased, it becomes similar to a computer file, capable of being stored and used anywhere on the Planet.'[85]

3.2.4. Transactional Speed and Absence of Intermediaries.

It is possible to obtain a bitcoin address instantly, much quicker than setting up an account with any other international payment intermediary. An average bitcoin transaction is currently processed in about ten minutes, thus allowing for very speedy cross-border transactions compared to, for example, a wire transfer.[86] Operationally, there are no security and capital control checks and no risk of being reported to relevant authorities in the process, as is the case with the regulated payment methods operating outside of the crypto domain.

timeline> accessed 20 August 2019*;* Christine Lagarde, 'Addressing the Dark Side of the Crypto World' (IMF Blog, 13 March 2018) <https://blogs.imf.org/2018/03/13/addressing-the-dark-side-of-the-crypto-world/> accessed 12 August 2019.

[84] Stratiev (n 50) 109.

[85] Ibid 109-110.

[86] Various sources (bitinfocharts.com), 'Average Confirmation Time of Bitcoin Transactions from June 2017 to June 2018 (in Minutes)' (*Statista Inc.*, 1 July 2019) <https://www.statista.com/statistics/793539/bitcoin-transaction-confirmation-time/> accessed 28 August 2019.

3.2.5. Irrevocability.

All bitcoin transactions are completely irreversible, thus making it technically impossible to, for example, cancel or put on hold a fraudulent transaction. If it is established or suspected that a particular transaction constitutes money laundering or financing of terrorism, it still cannot be reversed.

3.2.6. Absence of Consumer Protection.

Another important, albeit perhaps a less obvious, driver for ML using cryptocurrencies is the absence of any mandatory consumer protection. Administering consumer protection for financial products is normally the responsibility of a supervising authority, and the lack thereof in cryptocurrency networks also means that there is no requirement to provide consumer protection guarantees. While certain cryptocurrency exchanges and wallet providers may choose to arrange for consumer safety provisions, or possibly even be obliged to offer it in certain jurisdictions, the cryptocurrency networks definitely can and do operate without such provisions. This means that cryptocurrency exchanges or other ventures accumulating large amounts of value can potentially seize their clients' assets without any compensation or a recourse mechanism, and then use them for money laundering or terrorist financing. One example of such ventures is Initial Coin Offerings (ICOs), based on the same basic principle as Initial Public Offerings (IPOs) but operating with cryptoassets known as 'tokens' instead of shares. Due to the absence of consumer guarantees, a high percentage of ICOs turn out to be fraudulent and vanish with the customers' funds.[87] Of course, in case an ICO is run by criminals, the funds may well be used in ML schemes.

Another notorious example of abusing customer trust is the case of Mt. Gox, a crypto exchange that has claimed to had been hacked with all the assets stolen. 'Later investigations revealed that actually the money was fraudulently removed by the owner of

[87] See, for example, Ana Alexandre, 'New Study Says 80 Percent of ICOs Conducted in 2017 Were Scams' (Cointelegraph, 13 July 2018 <https://cointelegraph.com/news/new-study-says-80-percent-of-icos-conducted-in-2017-were-scams> accessed 20 August 2019.

the site, and although hackers had taken a few bitcoins, the largest share of the money was in fact removed at the actual money exchange site.'[88] Remarkably, the former chief of the Mt. Gox exchange was recently acquitted of embezzlement and received a relatively mild sentence overall.[89] If the exchange had to have provisions ensuring better safety of the customers' funds by law, or a requirement for a compulsory compensation in case of fraud, it is likely that the chief would be much less inclined to engage in it.

Additionally, there is no protection from losing bitcoin keys or software. If it is stolen by a criminal and then used for illicit activity, there is nothing stopping them from misusing the assets, and there is no retrieving mechanism.[90]

3.2.7. Lack of Adequate Regulation.

Despite the fact that this year marks the tenth anniversary of cryptocurrencies, the scale of divergence in regulatory approach and status of cryptocurrencies around the globe is extremely high, as previously described in Chapter 2. This clearly shows that regulating cryptocurrencies can be a bumpy ride. There are two main reasons for this. First, regulating for new, emerging technologies is a challenging process, aggravated by the speed of innovation, which often exceeds the speed of legislative developments. A good example here could be the EU General Data Protection Regulation (GDPR): it was first proposed in 2012, but reached the implementation stage only 6 years later, while the technology that it regulates had existed for decades already.[91]

[88] Mohammed Ahmad Naheem, 'Regulating virtual currencies – the challenges of applying fiat currency laws to digital technology services' [2018] 25 Journal of Financial Crime 562, 569.

[89] Sherisse Pham, 'Former Mt. Gox Chief Mark Karpeles Acquitted of Most Charges in Major Bitcoin Case' (*CNN Business*, 15 March 2019) <https://www.cnn.com/2019/03/14/tech/mark-karpeles-mt-gox/index.html> accessed 30 August 2019.

[90] Irwin and Milad (n 35) 412-413.

[91] European Data Protection Supervisor ,'The History of the General Data Protection Regulation' (8 December 2016) <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en> accessed 9 August 2019.

Second reason is the challenges presented by the nature of cryptocurrencies themselves. Their very name – crypto – means 'hidden'[92], and the decentralised design of the blockchain was not invented with ease of regulation in mind. The whole idea behind cryptocurrencies is to be outside the control of any state or public authorities, thus also placing it outside traditional regulatory scope. Apart from this, virtual currencies are different to more traditional financial products in that they are inherently more complex technically. A full understanding of the finer details of their design requires a high degree of mathematical knowledge, meaning additional efforts for effective regulation.[93]

Where it exists at all, regulation is often inconsistent and contradictory. This frequently leads to a certain legal vacuum, which can be abused by the criminals. A notable example could be the Silk Road case, where the defendant claimed that he was not engaged in money laundering, since bitcoin is considered a property, and not currency under the applicable US law - and the transactions therefore were not 'financial transactions'. Of course, as explained in the Introduction, money laundering is not limited to money or currency exclusively, and can be broadly applied to anything of value, so this could not be used a defense.[94] However, it also shows how legal loopholes can be misused to justify illicit activity.

[92] See, for example, 'crypto-' (Online Etymology Dictionary *Etymonline.com*) <https://www.etymonline.com/word/crypto-> accessed 10 August 2019.
[93] Stratiev (n 50) 173, 187.
[94] *United States v Ulbricht*, 858 F.3d 71, 135 (2d Cir 2017); Ibid 110.

4. Regulatory Responses to the AML Challenges.

4.1. The Rationale for the AML Regulation of Virtual Currencies.

A question arises – is there a need to regulate an entity that was not made to be regulated via traditional channels? It is worth noting that cryptocurrencies are, in fact, not completely unregulated. The network is set up to be internally regulated by its protocol, which provides 'specific rules and requirements that ought to be met and respected for the network to exist'.[95] Bitcoin was created as a cryptographic solution to the double-spend problem, otherwise managed by a supervising third party, thus replacing some elements of external regulation with cryptographic protocols.[96]

At the same time, it is very clear that external regulation is required as well. Reasons are multiple. To start, virtual currencies, and cryptocurrencies in particular, usually operate not in isolation but within the established financial markets, which are regulated. Virtual currencies therefore can influence these regulated financial markets, themselves falling into the regulatory scope. While it is sometimes argued that the market share of virtual currencies is insignificant, it is evident that it is also growing rapidly as the technology is developing.[97] In fact, 'cryptocurrencies are among the largest *unregulated* markets in the world'.[98] Additionally, regulatory and legal uncertainty in financial markets is often detrimental to their growth. In the case of cryptocurrencies, a notable example of this are some of the biggest cryptocurrency crashes in 2014 and 2017, caused by the legal uncertainty in China.[99] Similarly, the US Securities and Exchange Commission (SEC) had to reject multiple applications for cryptocurrency exchange-traded funds (ETF) due to the lack of existing regulation.[100] Numerous analytical reports by Central Banks and relevant

[95] Stratiev (n 50) 186.
[96] Nakamoto (n 39) 1.
[97] ECB, 'Cryptocurrencies and Tokens' (n 37) 6.
[98] Foley, Karlsen, Putniņš (n 63).
[99] See, for example, Vandezande (n 12) 5.
[100] Nikhilesh De, Stan Higgins and Muyao Shen, 'SEC Rejects 9 Bitcoin ETF Proposals' (*CoinDesk* 22 August 2018) <https://www.coindesk.com/sec-rejects-7-bitcoin-etf-proposals> accessed 18 August 2018.

authorities such as FATF and the International Monetary Fund (IMF) also recommend regulation of virtual currencies.[101]

As shown in Chapter 3, the most significant risk posed by virtual currencies is that of money laundering. It is therefore logical to consider it the most important area to regulate. Indeed, it appears that all relevant authorities' reports highlight money laundering as he major risk of cryptocurrencies, and recommend including it into the scope of regulation.[102]

4.2. Regulatory Response to the Cryptocurrencies' AML Challenges in the EU.

It is important to point out that at the moment, cryptocurrencies and cryptoassets in general are unregulated in the EU, with the exception of anti-money laundering regulation. They do not 'fit under any of the subject matter-relevant EU legal acts (particularly PSD2 and EMD2, and MiFID)'.[103]

Cryptocurrencies appeared and gained momentum when the 3rd AMLD was in force. At the proposal stage of the next, 4th AMLD, 'none of the opinions issued by the European Central Bank, the European Economic and Social Committee, or of the European Data Protection Supervisor reference developments in virtual currencies'.[104] However, in its 2014 'Opinion on virtual currencies', published when 'the legislative process was ongoing', the EBA recommended to include them within the scope of AML.[105] Following the terrorist attack on the 'Charlie Hebdo' magazine in Paris in January 2015, France also expressed its support to

[101] See, for example, FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations' (updated June 2019, 2012-2019) <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html> accessed 11 August 2019; ECB, ECB Crypto-Assets Task Force, 'Crypto-Assets:
Implications for financial stability, monetary policy, and payments and market infrastructures' (Occasional Paper Series No 223, May 2019) 29 <https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf> accessed 7 August 2019; Financial Stability Board (FSB), 'Decentralised financial technologies - Report on financial stability, regulatory and governance implications' (6 June 2019) 9, 10 <https://www.fsb.org/wp-content/uploads/P060619.pdf> accessed 11 August 2019; Christine Lagarde, 'Addressing the Dark Side of the Crypto World' (*IMF Blog*, 13 March 2018) <https://blogs.imf.org/2018/03/13/addressing-the-dark-side-of-the-crypto-world/> accessed 12 August 2019.

[102] See, for example, FATF (n 101); EBA, 'EBA Opinion on 'virtual currencies' (n 24) 6; ECB (n 101) 5.

[103] ECB (n 101) 29.

[104] Vandezande (n 12) 282.

[105] EBA, 'EBA Opinion on 'virtual currencies' (n 24).

'strengthen the efficiency' of the AML/CFT legal framework, including assessment of 'the risks posed by virtual currencies'.[106] Echoing this, the Commission and the Council declared to take further efforts to regulate for virtual currencies, but after the adoption of the 4th AMLD.[107] As a result, the following directive, 4th AMLD, although introduced in 2015 when cryptocurrencies were firmly on the radar, fails to mention them.

Next year, in February 2016, the European Commission in its Action Plan 'explicitly acknowledged that virtual currencies were not regulated at the level of the EU, which includes the legal framework regarding anti-money laundering'. The Commission 'also expressed its clear intent to bring certain virtual currency service providers under the scope of the anti-money laundering legal framework'.[108]

Following this, in July 2016, the Commission released its amendment proposal for the 4th AMLD – the precursor for the next AML Directive.[109] The Proposal is a response to the evolution of terrorism threat, technological advances and the increasing internationalisation of the financial system, facilitating ML around the world. While not always stated explicitly in the Proposal, it is believed that apart from technical developments, the Proposal was largely brought about by the recent terrorist attacks, notably in France and Belgium,[110] and the 'Panama Papers' scandal.[111] In regards to virtual currencies, The Commission clearly stated that it 'seeks to address … gaps' … 'in the oversight of the many financial means used by terrorists, from cash … to virtual currencies and anonymous pre-paid cards'.[112] The

[106] Vandezande (n 12) 283.

[107] Ibid; Council of the European Union, 'Proposal for a regulation of the European Parliament and of the Council on information accompanying transfers of funds; 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: Declarations by Member States' 5116/15 ADD 3 REV 4.

[108] Vandezande (n 12) 286; Commission, 'Commission presents Action Plan to strengthen the fight against terrorist financing' (Press Release, 2 February 2016) <https://europa.eu/rapid/press-release_IP-16-202_en.htm> accessed 7 August 2019; Commission, 'Communication from the Commission to the European Parliament and the Council on an Action Plan for strengthening the fight against terrorist financing', COM (2016) 50 final.

[109] Vandezande (n 12) 286; Commission, 'Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC', COM(2016) 450 final (Proposal for 4th AMLD Amendments).

[110] 5th AML Directive recitals (2) and (3).

[111] Liz Campbell, 'Dirty cash (money talks): 4AMLD and the Money Laundering Regulations 2017' [2018] 2 Criminal Law Review 102.

[112] Proposal for 4th AMLD Amendments 2.

Commission points out that anonymity is the primary AML risk posed by virtual currencies, and also lists a number of other possible risks, including the 'irreversibility of transactions, means of dealing with fraudulent operations, the opaque and technologically complex nature of the industry, and the lack of regulatory safeguards'.[113]

To address the issue of anonymity, the Commission proposes to extend the list of obliged entities to virtual currency exchange platforms and custodian wallet providers.[114] The Proposal also introduces a suggested legal definition of virtual currencies – the first of its kind in the EU.[115] However, other possible ML risks have not been addressed.

The Commission acknowledges that the problem of anonymity will not be addressed in full, as transactions are possible outside of the proposed regulated channels, such as cryptocurrency exchanges. To counter this, the Commission also proposes central registers of all cryptocurrency address holders on member-state level, and remarks that 'Financial Intelligence Units (FIUs) should be able to associate virtual currency addresses to the identity of the owner of virtual currencies. In addition, the possibility to allow users to self-declare to designated authorities on a voluntary basis should be further assessed'.[116]

The resulting Directive, 5th AMLD, prescribes to extend the list of obliged entities to two new entities:

> *'(g) providers engaged in exchange services between virtual currencies and fiat currencies;*
>
> *(h) custodian wallet providers (art 1 (1)).*

where

> *'(18) "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*

[113] Proposal for 4th AMLD Amendments 12.
[114] Proposal for 4th AMLD Amendments 12.
[115] Proposal for 4th AMLD Amendments art 1(2)(c).
[116] Proposal for 4th AMLD Amendments art 1(22) and 22.

> *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;*
>
> *(19) "custodian wallet provider" means an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies' (art 1 (2)).*

In effect, 5th AMLD made mandatory for virtual currency exchanges and custodian wallet providers to register with the nominated supervisory authority, perform CFT and ML risk assessment, comply with the CDD, and report suspicious activity.[117]

In regards to the central database, the Directive currently prescribes that the relevant information be made accessible to FIUs, and calls for further legislative proposals regarding the database. It also makes provisions for the further assessment of the option for cryptocurrency users to self-report to relevant authorities.[118]

Finally, the following AML Directive, the 6th, published in November 2018, 'aims to combat money laundering by means of criminal law, enabling more efficient and swifter cross-border cooperation between competent authorities'.[119] While it does not address the virtual currency aspect of the ML directly, it is still significant. One of the facilitating aspects of ML through VCs is precisely the ease of cross-border transactions, made possible by the lack of cross-border cooperation of public authorities, amongst other reasons. Additionally, the legal and regulatory vacuum and inconsistencies between jurisdictions also paly a role in ML with the VCs.

[117] HM Treasury, 'Transposition of the Fifth Money Laundering Directive: consultation' (April 2019) 17 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/795670/20190415_Consultation_on_the_Transposition_of_5MLD__web.pdf> accessed on 12 May 2019.

[118] 5th AML Directive, recital (9) and art 1 (41) 1.

[119] 6th AML Directive, recital (1).

4.3. Regulatory Response to the Cryptocurrencies' AML Challenges in the UK.

In the UK, the government first concerned itself with the questions of regulation for cryptocurrency in August 2014, which correlates to the EU developments preceding the 4th AMLD.[120] The first UK governmental report, 'Digital currencies: response to the call for information', was released in March 2015 and served as the first announcement of the government's intention to include cryptocurrency exchanges into the scope of the AML regulation.[121] Following this, a designated Taskforce was created, which consists of the main governmental actors of the UK financial sector - the Bank of England, the Financial Conduct Authority (FCA) and Her Majesty's Treasury (HM Treasury). Their Final Report, published in October 2018, is the result of the large-scale research into cryptoassets.[122]

Notably, the UK regulators employ the notion of 'cryptoasset', as opposed to 'virtual currency' used in the EU. At the same time, albeit unsurprisingly, the Taskforce states that

> *There is not a single widely agreed definition of a cryptoasset. Broadly, a cryptoasset is a cryptographically secured digital representation of value or contractual rights that uses some type of distributed ledger technology and can be transferred, stored or traded electronically*.[123]

This quasi-definition extends the EU definition found in the 5th AMLD to 'digital representation of contractual rights', not just 'value', and does not limit 'cryptoassests' to

[120] HM Treasury, 'Digital currencies: responses to the call for information' March 2015 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_respo nse_to_call_for_information_final_changes.pdf> accessed 15 May 2019.

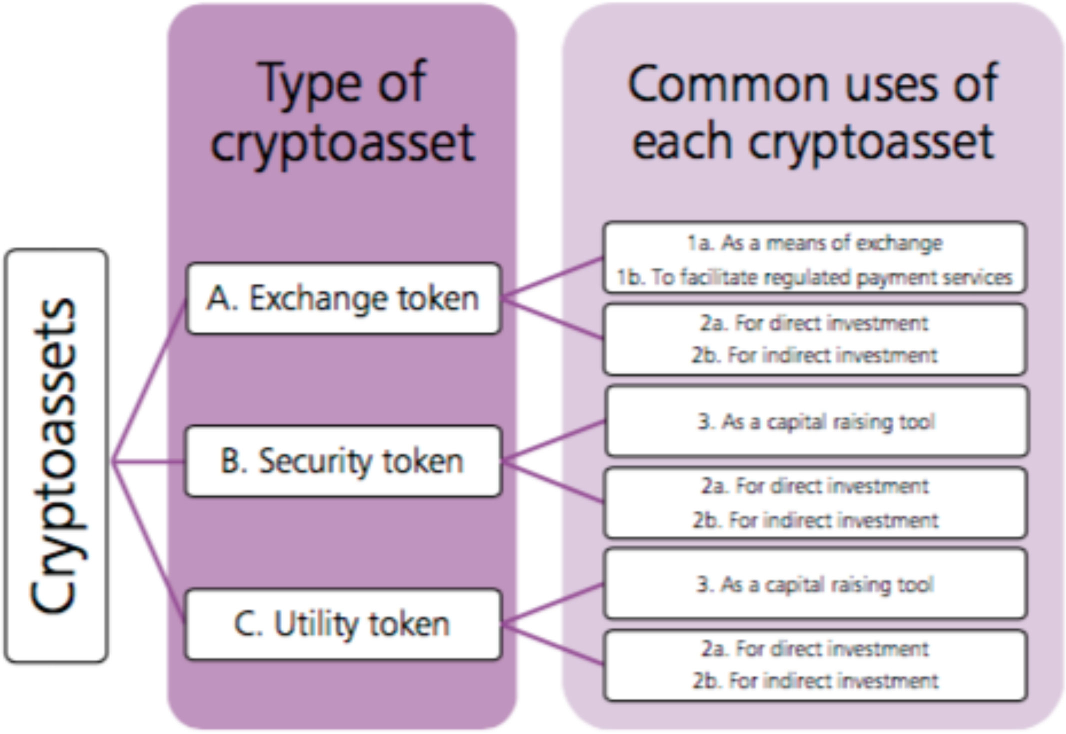
[121] Ibid.

[122] HM Treasury, FCA, Bank of England, 'Cryptoassets Taskforce: final report' October 2018 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf> accessed 15 May 2019.

[123] Ibid 11.

only decentralised networks. The Taskforce also introduces a classification of cryptoassets, which is similar to that of EBA.[124]

Figure 7: The Taskforce's Cryptoassets Framework.[125]


Cryptoassets
Type of cryptoasset
Common uses of each cryptoasset
A. Exchange token
B. Security token
C. Utility token
1a. As a means of exchange
1b. To facilitate regulated payment services
2a. For direct investment
2b. For indirect investment
3. As a capital raising tool
2a. For direct investment
2b. For indirect investment
3. As a capital raising tool
2a. For direct investment
2b. For indirect investment

The EU Directives have to be transposed into the national law of member states, usually within two years.[126] As it stands, the UK is set to leave the EU before the 5th AMLD is due to be transposed into the UK law on 10 January 2020. However, the UK government prioritized the transposition of the directive regardless of Brexit.[127] The EU Withdrawal Agreement included the terms of an implementation period, and 'the government is catering for the scenario where an implementation period is in place after the UK leaves the EU'.[128]

[124] EBA, 'Report with advice for the European Commission on crypto-assets' (n 27) 7; described in Chapter 2.
[125] Treasury, FCA, Bank of England (n 122).
[126] EU, 'Regulations, Directives and Other Acts' <https://europa.eu/european-union/eu-law/legal-acts_en> accessed on 11 May 2019.
[127] House of Commons Treasury Committee, 'Crypto-assets Twenty-Second Report of Session 2017–19' (19 September 2019) 28 <https://publications.parliament.uk/pa/cm201719/cmselect/cmtreasy/910/910.pdf> accessed 12 May 2019.
[128] HM Treasury, 'Transposition of the Fifth Money Laundering Directive: consultation' (n 117) 4.

HM Treasury is the leading UK authority for the transposition of the EU AML Directives.[129] On 15 April 2019, HM Treasury released a consultation paper, seeking the responses to be submitted up until 10 June 2019.[130] At the time of writing, the received feedback was being analysed, with no outcome yet released.

The UK implementation proposal of the 5th AMLD builds on the Final Report of the Taskforce with the FCA suggested as the registering authority.[131] There are two significant differences from the EU AMLD. First, the UK AML scope is proposed to extend to all cryptoassets, not just virtual currencies, which in case with the 5th AMLD mostly refers to cryptocurrencies. Second, HM Treasury acknowledges that 'illicit activity is being carried out at various points of cryptoasset exchange, not just through fiat-crypto exchange services'. It further enquires whether the AML regulation should include:

- *crypto-to-crypto exchange service providers*
- *peer-to-peer exchange service providers*
- *Cryptoasset Automated Teller Machines*
- *issuance of new cryptoassets, for example through Initial Coin Offerings (ICOs)*
- *the publication of open-source software*[132]

Moreover, the Consultation proactively asks if there are other types of cryptoassets, and whether its definition should be broadened, thus signalling a potential to include all existing and possible cryptoassets into scope. The HM Treasury also seeks further guidance on its approach to 'privacy coins', or types of cryptocurrency that conceal personal information about its users.[133]

[129] HM Treasury, 'About Us' <https://www.gov.uk/government/organisations/hm-treasury/about> accessed 14 May 2019.
[130] HM Treasury, 'Transposition of the Fifth Money Laundering Directive: consultation' (n 117).
[131] HM Treasury, 'Transposition of the Fifth Money Laundering Directive: consultation' (n 117) 18.
[132] Ibid.
[133] Ibid 19-21; 'Privacy Coin' (Decryptionary) <https://decryptionary.com/dictionary/privacy-coin/> accessed 20 August 2019.

In addition to this, HM Treasury notes that the cross-border nature of the cryptoasset networks makes it very easy to circumvent the regulations in one jurisdiction by setting up operations in another. The Consultation therefore also proposes 'extending the reach of UK AML laws to providers who are located outside of the UK' by applying them extraterritorially.[134]

Notably, the UK traditionally goes 'above and beyond' when transposing the EU Directives – a phenomenon known as 'gold-plating'.[135] It is clear that 5th AMLD won't be an exception. Gold-plating is criticised as negatively affecting law harmonisation and international business, and is officially reserved by the UK government for exceptional circumstances only.[136] Nonetheless, it appears to be justified in this case. While it is not possible to know the exact extent of the gold-plating now, before the Directive is fully implemented, there is a clear case for extending the 5th AMLD virtual currencies provisions. As acknowledged by the UK Taskforce and as described earlier in this work, 'anonymous conversion of cryptocurrency to fiat currency and vice versa', potentially used in ML schemes, can also happen outside of the regulated realm of the 5th AMLD. Cryptocurrency ATMs, face-to-face exchanges, schemes involving third-party accounts and mixing services are all outside the scope of 5th AMLD. It is worth noting that the UK AML regime is one of the most robust out of all the countries assessed by FATF, and the gold-plating of the new AMLD is also in line with that.[137]

The counter-argument to this initiative is the perceived hindrance to technological and business development which the excessive regulation may bring. However, this does not

[134] Arun Srivastava and others, 'Money Laundering Update' [2019] 167 Compliance Officer Bulletin 1, 9; HM Treasury, 'Transposition of the Fifth Money Laundering Directive: consultation' (n 117) 18.

[135] "Gold-plating is when implementation goes beyond the minimum necessary to comply with a Directive, by: extending the scope … etc." in HM Government, 'Transposition Guidance - How to implement European Directives effectively' February 2018 8 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682752/eu-transposition-guidance.pdf> accessed 15 May 2019. It is claimed that the UK frequently gold-plates EU Directives, for example, see Chris Davies, 'Gold Plating of EU Laws 'Has Ended' BBC News (24 April 2013) <https://www.bbc.com/news/uk-politics-22277927> accessed 19 May 2019.

[136] HM Government (n 135) 3.

[137] FATF, 'Anti-Money Laundering and Counter-Terrorist Financial Measures; United Kingdom, Mutual Evaluation Report' (December 2018) <https://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-united-kingdom-2018.html> accessed 28 August 2019.

seem to be proportionate here, considering that the scale of ML with the use of bitcoin, the most widely-used cryptocurrency, is close to 50% of all transactions.

4.4. Summary of the EU and the UK AML Regulation for Virtual Currencies.

As discussed, the EU provided a legal definition of virtual currencies and custodian wallet providers, admitted their ML and CTF potential, and incorporated them into the existing AML framework. The main objective of the 5th AMLD is to deal with the issue of anonymity. It excluded other ML risks posed by virtual currencies, although they were acknowledged at the Proposal stage. Additionally, the 6th AMLD indirectly addressed the problems that stem from the cross-border nature of cryptoasset networks through the promotion of international cooperation of competent authorities.

The UK at this stage is likely to incorporate into its AML regulation a much larger number of entities and types of cryptoassets. It is also likely to apply its AML law extraterritorially to providers outside of the UK, but related to the UK business. If this is to materialise, the UK VC AML regulations will have a knock-on effect outside of the UK, thus overcoming the limitations of 5th AMLD to an extent.

5. Possible Solutions for AML Regulation of Virtual Currencies in the EU and the UK.

5.1. Proposals for Cryptocurrencies Risk Assessment under the Existing AML Regime.

It is clear that the principle of the current AML regulation of virtual currencies both in the EU and the UK is to expand the existing AML regime to include cryptoassets where it is feasible. The downside of this approach is that in situations where the existing AML regime is not readily applicable, no alternative provisions are made. The technical questions, such as how to perform CDD and risk assessment for cryptoassets users and institutions, are not addressed either.

Critical literature contains some suggestions for AML risk assessment of virtual currency users. Notably, the use of mixing services can be viewed as a red flag, as well as any obfuscation of the financial trail preceding the purchase of a cryptoasset, and concealing the identities of the wallet owners.[138]

Another suggested approach to monitoring illegal activity is through data analysis. Suggested analysis types include 'network cluster analysis' and 'detection controlled estimation (DCE)', which have already been successfully applied to other forms of misconduct such as tax evasion and fraud.[139]

Cluster analysis is the process of identifying and grouping together similar objects within a dataset. 'At an intuitive level, the … method exploits the network topology – the information about who trades with whom'.[140] In the applicable context, the objects could be bitcoin users and the grouping (or clusters) identifies 'communities of users based on the transactions between users'.[141] This clustering can then be applied to a sample of known

[138] Naheem (n 88) 562, 570.
[139] Foley, Karlsen, Putniņš (n 63).
[140] Ibid.
[141] Ibid.

illegal and legitimate bitcoin users, who could have been identified through bitcoin seizures by law enforcement and on dark web forums, for example. The result of such analysis is an estimation of the level of relatedness from any one bitcoin user to a cluster of other bitcoin users. If the user has a high degree of relatedness to a cluster classed as legitimate, this user has a high likelihood to be legitimate as well. If the cluster the user relates to is not legitimate – the user is likely to be involved in misconduct. Network cluster analysis can be applied via many different algorithms; however, none can guarantee a complete accuracy of detection.

Another analytical tool, DCE, 'exploits the differences in the characteristics of legal and illegal users of bitcoin to probabilistically identify the population of illegal users'.[142] That is, by looking at the particular characteristics of a bitcoin user's behaviour, it is possible to assign them a specific risk rating. Examples of characteristics used in this analysis could be attempts to conceal identity by using mixing services, propensity to trade in privacy coins or even time-series variables which highlight a correlation between the time of activity on dark web marketplaces and the time when a user transacts.

Both network cluster analysis and DCE can only estimate the likelihood that a user is involved in illicit activities, and cannot constitute a proof of a predicate offence by itself. However, using different analysis types concurrently allows a better quality of results. Given that blockchain is an open ledger, it is also possible to conduct some analysis without attracting attention. Expanding on this idea even further, there is a potential for using Artificial Intelligence (AI) tools for finding suspicious users and transactions.

[142] Ibid.

5.2. Intractability of AML with Virtual Currencies.

An overview of the analytical literature shows that while it is universally agreed that ML is amongst the highest risks posed by virtual currencies, there are very limited attempts to offer solutions beyond that of including cryptoassets into the scope of the existing AML regulation. This leads us to the conclusion that while there are plentiful opportunities for using VCs for money laundering, there is currently no effective way to combat it in its entirety, and no indication that there will be one in the future. Importantly, there is also a limited incentive for the competent authorities to do so, simply because no single authority is responsible for regulating cryptocurrencies. Decentralised cryptocurrencies do not have any central governing body, thus existing in a vacuum where there is no organisation that can accept the responsibility for regulating them, and therefore no one to blame for any shortcomings.

5.3. Other Possible Solutions.

5.3.1. Supranational Regulation.

There is a widespread opinion that AML regulation for virtual currencies at state level won't be sufficient to combat cross-border ML. Therefore, a supranational regulator is required. Some researchers even propose the EU and the IMF as possible candidate.[143] The author, however, would argue that this suggestion is far from ideal. No authority is able to completely control development, modification and use of cryptocurrencies, because they do not require an authority to exist. Cryptocurrency networks are nothing other than an internet activity, which cannot be completely controlled even in restrictive countries like China because of circumventing technologies such as TOR or VPN. Similarly, solutions prescribing requirements for the cryptocurrency protocol, such as adding user identification details or ML provisions, would be pointless, because there is nothing stopping the creation

[143] Stratiev (n 50) 187; Prof. Dr Robby Houben, 'Cryptocurrencies from a money laundering and tax evasion perspective' [2019] 30 International Company and Commercial Law Review 261, 26.

of new cryptocurrencies without such provisions and with increased anonymity, such as ‘privacy coins’.

Additionally, the efficiency of existing global bodies tasked with financial regulation is questionable. Often, there exists a considerable disparity between their *de jure* and *de facto* scope, with the IMF a case in point.[144]

5.3.2. Prohibition as a Solution.

In this light, perhaps an outright ban on cryptocurrency would be merited? The author would argue that while it can serve as a deterrent and potentially devalue cryptocurrencies, it is not a viable solution. As discussed above, ultimately there is no way to have full control over the creation and use of cryptocurrency networks, including points of exchange between FC and VC. Therefore, there can be no sanctions for violation of the prohibition.

5.3.3. Incentivising AML-Compliant Cryptoassets as a Solution.

Since neither prohibition nor central management of all cryptocurrencies is feasible, the regulators could incentivise users towards more AML-compliant cryptocurrencies, thus potentially marginalising the rogue ones. This could be done by obliging cryptocurrency exchanges and other service providers to only allow cryptocurrencies whose inherent characteristics permit AML monitoring. This will automatically mark non-complaint cryptocurrencies and their users as suspicious, potentially decreasing their price in fiat currency and therefore their market share and utility for ML. There also could be a provision to include any instances of suspicious cryptocurrencies into the compulsory AML reporting, for the authorities to investigate.

Going further, the requirement to register with the relevant authority (likely to be the FCA in the UK) could be extended from the exchange or crypto services provider to new

[144] See, for example, Norman Mugarura, ‘The IMF, Its Mandate and Influence in Prevention of Financial Sector Abuse’ [2016] 23 Journal of Financial Crime 987; Ngaire Woods, ‘Making the IMF and the World Bank More Accountable’ [2001] 77 International Affairs 85, 89.

cryptocurrencies when they are created. The current number of active cryptocurrencies that are known to exist, ten years after bitcoin was created, is just below 2,500. This is comparable to the quantity of other types of entities regulated by the FCA, and therefore should be a realistic figure to oversee.[145] Alternatively, new cryptocurrencies could be overseen directly by the exchanges. Similar to stock exchanges imposing their requirements on a traded stock, AML requirements could be applied to cryptocurrencies before they are admitted for trading.

Fundamentally, the only reliable way to regulate cryptocurrencies is by amending the protocol which defines them. As pointed out in section 4.1, cryptocurrency networks are designed to be effectively regulated by their protocols, and it is not possible to maintain control over them through traditional external channels.[146] Therefore, the source code of a new cryptocurrency could be submitted for a review before the launch, with the requirement to specify how the cryptocurrency addresses AML requirements. Once approved, the cryptocurrency can receive its verifiable registration details from the FCA, or from the exchange, and subsequently be made available to users. This will attract legitimate users of the cryptocurrency market to the AML-complaint cryptocurrencies, and to protect these currencies from being used in ML. It will also shift the responsibility of developing AML controls from the regulators to the cryptocurrency creators, thus reducing the cost of regulation for the state and potentially making AML controls more functional since they are added at the creation stage of the protocol. In the case of existing cryptocurrencies, the same requirement of providing a 'prospectus' detailing AML characteristics could be applied to them retroactively. This would effectively mean 'forking' them and then allowing the use of the compliant fork only.

Of course, this will not eliminate rogue cryptocurrencies from the market completely – it is not possible. But this will considerably marginalise them and automatically mark their users

[145] FCA, 'About the FCA (FCA, 21 April 2016, updated 30 July 2019) <https://www.fca.org.uk/about/the-fca> accessed 28 August 2019.

[146] The idea of modifying a cryptocurrency protocol to implement AML provisions was mentioned at the University of Glasgow, College of Social Sciences, 'Cryptocurrencies and Financial Crime Compliance: opportunities for new regulatory paradigms?' (PhD Proposal, supervisor Dr. Micheál O'Flynn) <https://www.gla.ac.uk/scholarships/cossphdscholarshipcryptocurrenciesandfinancialcrimecomplianceopportunitiesfornewregulatoryparadigms/> accessed 28 March 2019.

as potential money launderers, thus depleting their capitalisation by separating the funds of law abiding users and criminals. Ultimately, it could even lead to the nullification of the value of these cryptocurrencies in fiat currency, thus making it useless for money laundering purposes. In the case of bitcoin and some (though not all) other cryptocurrencies, their monetary value is not inherent and not guaranteed, but always determined by the market demand. When it first appeared, bitcoin had no value in fiat currency. Therefore it is possible, at least theoretically, to revert the market price of a cryptocurrency back to zero, if there is no demand for it. In the case of cryptocurrencies with a finite number of units, such as bitcoin, bringing the value of the cryptocurrency down to miniscule numbers would have the same effect as nullifying it completely. The usability of rogue cryptocurrencies will also be limited, since it won’t be possible to use them at any regulated point of exchange, potentially including whole regions such as the EU.

The mandatory technical characteristics of an AML-compliant cryptocurrencies could be built into their protocol and based on the existing AML legislation, then updated in due course. In this model, an introduced requirement could be the addition of a transaction receipt to the blockchain, generated using existing cryptographic techniques which unequivocally verifies that the rules of the protocol have been followed and who approved the transaction. This model allows the cryptocurrency to remain decentralised while also providing the authorities with sufficient means to adequately monitor transactions.

For example, the 5th EU AML Directive implies a ban on anonymous accounts of any kind.[147] For an AML-compliant cryptocurrency, this could mean requiring all wallets to be authenticated and marked by a qualified body only after the provision of sufficient user identification details. Then, any transaction request would check whether the associated wallets are authenticated or not, and reject transactions involving unverified wallets. In this way, cryptocurrency payments and transfers would be tracked in a similar way to how banking transactions are tracked today, except that the authorities would have immediate access to the public ledger.

[147] 5th AML Directive, recital (20).

Another new requirement of the 5th EU AMLD is the decrease to the CDD threshold to 150 euro per month.[148] Here each AML-compliant cryptocurrency network could apply specific rules dependent on the size of the transfer, that is, having the nodes of the network which verify each transaction, policing users exceeding the threshold and denying transaction verification before a CDD can be completed by a qualified authority. The same imposition of rules into the cryptocurrency protocol could be used to meet other AML requirements and safeguards.

While computer science efforts may be needed to finalise the design, we would expect these AML-compliant cryptocurrencies to fundamentally retain many of the benefits of today's cryptocurrencies. We would expect lower transaction fees, faster transactions and a reduction in fraud. In addition, the overheads of regulating such a system would benefit from the same efficiencies that cryptocurrency transactions enjoy today, that is, a decentralised system which is effectively self fulfilling.

AML-compliant cryptocurrencies may provide the balance between freedom and control that is needed, and indeed may even be inevitable over the long term.

5.3.3.1. Potential Problems of the Incentivising of AML-Compliant Cryptoassets.

There are a few issues with this model. First, there is a distinct danger of stifling innovation by imposing costly regulatory requirements. Current EU and UK AML provisions already are widely criticised as disproportionate. Most of the cost of AML compliance lies with the private sector, and the AML regime progressively keeps getting stricter and therefore more expensive.[149] There is neither recognition nor compensation for adherence to the AML requirements. This is done with the backdrop of virtually non-existent evidence of the

[148] 5th AML Directive, art 1 (7)(a)(i).

[149] See, for example, Anna Odby, 'The European Union and Money Laundering: the Preventive Responsibilities of the Private Sector' in Bantekas, Keramidas (n 3); Campbell (n 111); Nicholas Ryder, 'Is It Time to Reform the Counter-Terrorist Financing Reporting Obligations? On the EU and UK System' [2018] 19 German Law Journal 1169.

efficiency of the AML regime, since its effect cannot be easily quantified.[150] This makes private sector question the merits of the regime and causes widespread discontent.[151]

Some of the EU and UK AML requirements are conflicting with human rights. The implicit ban on anonymity and the move towards databases of personal data, for example, are quite problematic for the right to privacy and the EU data protection laws.[152]

However, the risk of ML using cryptocurrencies is so significant that it cannot be disregarded. This will also put cryptocurrencies together with all the regulated financial products, thus levelling the playing field rather than disadvantaging any market actors. Considering that the addition of AML provisions could potentially increase the capitalisation of the cryptocurrency by attracting investors who do not want to be associated with the rogue cryptocurrencies, this could also be viewed as an easy way to add value. Compliance with AML requirements could be a selling point of new and existing cryptocurrencies on par with other technical characteristics.

Another issue is the poor law harmonisation between jurisdictions, and regulatory arbitrage. Since AML requirements can differ around the world, compliant cryptocurrencies in one jurisdiction might not be considered as such in another. Moreover, there are jurisdictions already accepting existing cryptocurrencies as a means of payment without any AML changes to the protocol, such as Japan and Switzerland. This, however, could be overcome by agreeing to the same AML principles for cryptocurrencies on an international level, for example, through FATF Recommendations.

[150] Ibid; Peter Alan Sproat, 'An Evaluation of the UK's Anti-Money Laundering and Asset Recovery Regime' [2007] 47 Crime Law and Social Change 169.

[151] See, for example, Campbell (n 111); Andrew Haynes, ‘Money laundering: from failure to absurdity’ [2008] 11 Journal of Money Laundering Control 303.

[152] See, for example, Campbell (n 111).

6. Conclusion.

The paper has critically examined the phenomenon of cryptocurrency-based money laundering and the current EU and UK legislative efforts to combat it. It has identified unresolved issues and offered potential solutions. Given the emerging nature and the technical complexity of the field, a comprehensive background information on virtual currencies has also been analysed and provided.

It has been found that the questions of the AML regulation of virtual currencies is largely an intractable one, at least in the present circumstances. However, it does not mean that the AML regulation cannot be improved upon. The paper summarises proposed methods for CDD and AML risk assessment for cryptocurrency networks, discusses different ideas to combat cryptocurrency-based ML, and finally describes a potential path to the minimisation of money laundering with the use of VCs through AML regulation.

It is clear today that the main technological break-through behind cryptocurrencies is, ironically, not the 'currency' aspect of it. Advantages of cryptocurrency as a payment method, such as decentralisation, financial inclusion and transactional speed, are countered by poor usability, serious limitations in consumer protection and extreme volatility – the very aspects that are the responsibility of the competent authorities in case of government-controlled fiat currencies. It is the system allowing for functional decentralisation, the DLT, that has proven the most advantageous.[153] Perhaps, this system could be re-applied to the cryptoassets to build financial products that could not be used for illicit purposes so easily, once our understanding of their potential improves.

It has been established that money laundering is always a consequence of a preceding crime. The question of its complete elimination is therefore the question of the possibility of eliminating crime in general, which has not been possible so far. Today, the primary objective of anti-money laundering regulation is not to annihilate it, but to make the money

[153] See, for example, The Economist, Anonymous, 'Show Me the Money' [2018] 428 9107 The Economist; London 12.

laundering process as complex and expensive for criminals as possible. If the cost of money laundering exceeds the value of criminal proceeds, it can render the associated crime pointless.[154] Disincentivising rogue cryptoasset initiatives in favour of AML-complaint ones would be very much in line with the contemporary AML goal.

[154] See, for example, Hans Geiger and Oliver Wuensch, 'The Fight Against Money Laundering. An Economic Analysis of a Cost-Benefit Paradox' [2007] 10 Journal of Money Laundering Control 91.

Bibliography.

Primary Sources.

United States v Ulbricht, 858 F.3d 71, 135 (2d Cir 2017)

Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering [1991] OJ 166/77

Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering - Commission Declaration [2011] OJ L 344/76

Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (Text with EEA relevance) [2005] OJ L309/15

Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance) [2015] OJ L141/73

Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance) [2018] OJ L156/43

Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law [2018] OJ L284/22

United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (adopted 20 December 1988, entered into force 11 November 1990 (Vienna Convention))

Official Publications.

BCBS, 'Prevention of Criminal Use of the Banking System for the Purpose of Money-Laundering' (28 December 1988) <https://www.bis.org/publ/bcbsc137.htm> accessed 30 July 2019.

Council of the European Union, 'Proposal for a regulation of the European Parliament and of the Council on information accompanying transfers of funds; 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: Declarations by Member States' 5116/15 ADD 3 REV 4

EBA, ‘EBA Opinion on ‘virtual currencies’ (4 July 2014) <https://eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf> accessed 7 August 2019

--‘Report with advice for the European Commission on crypto-assets’ (9 January 2019) <https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf> accessed 9 August 2019

ECB, ‘Cryptocurrencies and Tokens’ (September 2018) <https://www.ecb.europa.eu/paym/groups/pdf/fxcg/2018/20180906/Item_2a_-_Cryptocurrencies_and_tokens.pdf> accessed 30 July 2019

-- Crypto-Assets Task Force, ‘Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures’ (Occasional Paper Series No 223, May 2019) <https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf> accessed 7 August 2019

European Commission, ‘Commission presents Action Plan to strengthen the fight against terrorist financing’ (Press Release, 2 February 2016) <https://europa.eu/rapid/press-release_IP-16-202_en.htm> accessed 7 August 2019

--‘Communication from the Commission to the European Parliament and the Council on an Action Plan for strengthening the fight against terrorist financing’, COM (2016) 50 final

--‘Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC’, COM(2016) 450 final

European Data Protection Supervisor ,’The History of the General Data Protection Regulation’ (8 December 2016) <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en> accessed 9 August 2019

FATF, ‘Anti-Money Laundering and Counter-Terrorist Financial Measures; United Kingdom, Mutual Evaluation Report’ (December 2018) <https://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-united-kingdom-2018.html> accessed 28 August 2019.

--‘International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations’ (updated June 2019, 2012-2019) <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html> accessed 11 August 2019

-- ‘Money Laundering - Financial Action Task Force (FATF)’ <https://www.fatf-gafi.org/faq/moneylaundering/> accessed on 30 July 2019

FCA, 'About the FCA (FCA, 21 April 2016, updated 30 July 2019) <https://www.fca.org.uk/about/the-fca> accessed 28 August 2019

FSB, 'Decentralised financial technologies - Report on financial stability, regulatory and governance implications' (6 June 2019) <https://www.fsb.org/wp-content/uploads/P060619.pdf> accessed 11 August 2019

HM Government, 'Transposition Guidance - How to implement European Directives effectively' February 2018 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682752/eu-transposition-guidance.pdf> accessed on 15 May 2019

HM Treasury, 'About Us' <https://www.gov.uk/government/organisations/hm-treasury/about> accessed 14 May 2019

-- 'Digital currencies: responses to the call for information' March 2015 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf> accessed 15 May 2019

-- 'Transposition of the Fifth Money Laundering Directive: consultation' April 2019 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/795670/20190415_Consultation_on_the_Transposition_of_5MLD__web.pdf> accessed 12 May 2019

-- FCA, Bank of England, 'Cryptoassets Taskforce: final report' October 2018 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf> accessed 15 May 2019

House of Commons Treasury Committee, 'Crypto-assets Twenty-Second Report of Session 2017–19' 19 September 2019 <https://publications.parliament.uk/pa/cm201719/cmselect/cmtreasy/910/910.pdf> accessed 12 May 2019

EU, 'Regulations, Directives and Other Acts' <https://europa.eu/european-union/eu-law/legal-acts_en> accessed on 11 May 2019

Secondary Sources.

Alexander R, 'Editorial – How to Regulate Bitcoin – the Debate Continues' [2018] 39 (3) Company Lawyer 65

Alexandre A, 'New Study Says 80 Percent of ICOs Conducted in 2017 Were Scams' (Cointelegraph, 13 July 2018 <https://cointelegraph.com/news/new-study-says-80-percent-of-icos-conducted-in-2017-were-scams> accessed 20 August 2019

Alldridge P, ’The Moral Limits of the Crime of Money Laundering’ [2001] 5 Buffalo Criminal Law Review 279
Baker E and Napper P, ‘UK Part I: UK Money Laundering – Typological Considerations’ in Srivastava A, Simpson M, and Powell R (eds), *International Guide to Money Laundering Law and Practice* (5th edn, Bloomsbury Professional 2019)

Campbell L, ‘Dirty cash (money talks): 4AMLD and the Money Laundering Regulations 2017’ [2018] Criminal Law Review 102

CoinMarketCap, ‘Cryptocurrency Market Capitalizations’ (Coinmarketcap.com 18 August 2019) <https://coinmarketcap.com/> accessed 18 August 2019

Davies C, ‘Gold Plating of EU Laws ‘Has Ended’ BBC News (24 April 2013) <https://www.bbc.com/news/uk-politics-22277927> accessed 19 May 2019

Decryptionary, ‘Privacy Coin’ <https://decryptionary.com/dictionary/privacy-coin/> accessed 20 August 2019

De N, Stan Higgins S and Shen M, ‘SEC Rejects 9 Bitcoin ETF Proposals’ (*CoinDesk* 22 August 2018) <https://www.coindesk.com/sec-rejects-7-bitcoin-etf-proposals> accessed 18 August 2018

Dostov V and Shust P ‘Cryptocurrencies: An Unconventional Challenge to the AML/CFT Regulators?’ [2014] 21 Journal of Financial Crime 249

--‘Evolution of the Electronic Payment Industry: Problems of a Qualitative Transition’ [Виктор Достов и Павел Шуст, ‘Эволюция Отрасли Электронных Платежей: Проблемы Качественного Перехода’] (Working Paper, Russian Presidential Academy of National Economy and Public Administration, May 2017) <ftp://w82.ranepa.ru/rnp/wpaper/051713.pdf> accessed 28 March 2019

Geiger H and Wuensch O, ‘The Fight Against Money Laundering. An Economic Analysis of a Cost-Benefit Paradox’ [2007] 10 Journal of Money Laundering Control 91

Gola Y, ‘ISIS Used Bitcoin to Fund Horrific Sri Lanka Easter Bombings, Research Claims’ (*CCN Markets*, 2 May 2019) <https://www.ccn.com/isis-bitcoin-fund-sri-lanka-easter-bombings/> accessed 28 August 2019.

Haynes A, ‘Money laundering: from failure to absurdity’ [2008] 11 Journal of Money Laundering Control 303

Hicks DC, ‘Chapter 35 - Money Laundering’ in Fiona Brookman et al, *Handbook on Crime* (Willan Publishing 2010)

Houben R, ‘Cryptocurrencies from a money laundering and tax evasion perspective’ [2019] 30 International Company and Commercial Law Review 261

Etymonline.com, ‘crypto-’ (Online Etymology Dictionary *Etymonline.com*) <https://www.etymonline.com/word/crypto-> accessed 10 August 2019

Finley K, ‘After 10 Years Bitcoin Changed Everything and Nothing’ (*Wired*, 31 October 2018) <https://www.wired.com/story/after-10-years-bitcoin-changed-everything-nothing/> accessed 30 July 2019
Foley S, Karlsen JR, Putniņš TJ, ‘Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?’ [2019] 32 The Review of Financial Studies 1798

Hicks DC, ‘Chapter 35 - Money Laundering’ in Fiona Brookman et al, *Handbook on Crime* (Willan Publishing 2010)

Irwin ASM and Milad G, ‘The Use of Crypto-Currencies in Funding Violent Jihad’ [2016] 19 Journal of Money Laundering Control 407

Keramidas G, ‘The Legal Nature of Transnational Financial Crime’ in Bantekas I, Keramidas G (eds), International and European Financial Criminal Law (LexisNexis Butterworths 2006)

Lagarde C, ‘Addressing the Dark Side of the Crypto World’ (*IMF Blog*, 13 March 2018) <https://blogs.imf.org/2018/03/13/addressing-the-dark-side-of-the-crypto-world/> accessed 12 August 2019

Lexico.com, ’cryptocurrency, n’ <https://www.lexico.com/en/definition/cryptocurrency> accessed 5 August 2019

-- ‘bitcoin, n’ <https://www.lexico.com/en/definition/bitcoin> accessed 5 August 2019

Mugarura N, ‘The IMF, Its Mandate and Influence in Prevention of Financial Sector Abuse’ [2016] 23 Journal of Financial Crime 987

Naheem MA, ‘Regulating virtual currencies – the challenges of applying fiat currency laws to digital technology services’ [2018] 25 Journal of Financial Crime 562

Nakamoto S, ‘Bitcoin: A Peer-to-Peer Electronic Cash System’ (<www.bitcoin.org>, allegedly 31 October 2008) <https://bitcoin.org/bitcoin.pdf> accessed 30 July 2019

--email from Satoshi Nakamoto to the Cryptography Mailing List ‘Bitcoin v0.1 released’ (9 January 2009) <Mail-archive.com/cryptography@metzdowd.com/msg10142.html> accessed 7 August 2019

Odby A, ‘The European Union and Money Laundering: the Preventive Responsibilities of the Private Sector’ in Bantekas I, Keramidas G (eds), International and European Financial Criminal Law (LexisNexis Butterworths 2006)

The Economist, Anonymous, ‘Show Me the Money’ [2018] 428 9107 T*he Economist; London* 12

Pham S, 'Former Mt. Gox Chief Mark Karpeles Acquitted of Most Charges in Major Bitcoin Case' (*CNN Business*, 15 March 2019) <https://www.cnn.com/2019/03/14/tech/mark-karpeles-mt-gox/index.html> accessed 30 August 2019

Ryder N, 'Is It Time to Reform the Counter-Terrorist Financing Reporting Obligations? On the EU and UK System' [2018] 19 German Law Journal 1169
Schneider F and Windischbauer U, 'Money Laundering: Some Facts' (2008) 26 European Journal of Law & Economics 387

Simpson M and Williams S, 'International Initiatives' in Srivastava A, Simpson M, and Powell R (eds), *International Guide to Money Laundering Law and Practice* (5th edn, Bloomsbury Professional 2019)

Sproat PA, 'An Evaluation of the UK's Anti-Money Laundering and Asset Recovery Regime' [2007] 47 Crime Law Soc Change 169

Statista, various sources (bitinfocharts.com), 'Average Confirmation Time of Bitcoin Transactions from June 2017 to June 2018 (in Minutes)' (*Statista Inc.*, 1 July 2019) <https://www.statista.com/statistics/793539/bitcoin-transaction-confirmation-time/> accessed 28 August 2019.

Stratiev O, 'Cryptocurrency and Blockchain: How to Regulate Something We Do Not Understand' [2018] 33 Banking and Finance Law Review 187

Unger B, 'Money Laundering Regulation: From Al Capone to Al Qaeda in Unger B and van der Linde D (eds) *Research Handbook on Money Laundering* (Edward Elgar Publishing 2013)

University of Glasgow, College of Social Sciences, 'Cryptocurrencies and Financial Crime Compliance: opportunities for new regulatory paradigms?' (PhD Proposal, supervisor Dr. Micheál O'Flynn)
<https://www.gla.ac.uk/scholarships/cossphdscholarshipcryptocurrenciesandfinancialcrimecomplianceopportunitiesfornewregulatoryparadigms/> accessed 28 March 2019.

Vandezande N, *Virtual Currencies: A Legal Framework* vol 1 (Intersentia 2018)

-- Virtual Currencies under EU Anti-money Laundering Law' [2017] 33 Computer Law and Security Report 341

van Wegberg R, Oerlemans JJ, van Deventer O, 'Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin' [2018] 25 Journal of Financial Crime 419

Woods N, 'Making the IMF and the World Bank More Accountable' [2001] 77 International Affairs 85