MONEY LAUNDERING THROUGH CRYPTOCURRENCIES: ANALYSING THE RESPONSES OF THE UNITED STATES AND AUSTRALIA AND PROVIDING RECOMMENDATIONS FOR THE UK TO ADDRESS THE MONEY LAUNDERING RISKS POSED BY CRYPTOCURRENCIES.

HENRY DANIEL HILLMAN

A thesis submitted in partial fulfilment of the requirements of the University of the West of England, Bristol for the degree of Doctor of Philosophy

Faculty of Business and Law, University of the West of England, Bristol
August 2020

Acknowledgements

I am very grateful to my supervisory team throughout my PhD, Professor Nicholas Ryder and Dr Clare Chambers have both endured reading many draft sections of this thesis and given helpful guidance for which I will always be thankful. During the course of my PhD we have become colleagues and brilliant friends.

I am thankful to my peers and colleagues at UWE who have shared this journey with me, Amy Man and Sam Bourton especially have put up with me complaining, and we have each questioned why we started this long and very winding academic journey. I would like to thank everyone at UWE who has provided guidance and encouragement during my research.

I would like to apologise to Emily, as I have probably been a less than perfect husband while writing this thesis, thank you for putting up with me, I love you, and no, this does not mean I will be getting a ‘proper job’, whatever that is.

Abstract

This thesis aims to analyse the phenomenon of cryptocurrencies, specifically the legal understanding of cryptocurrencies, to assess whether they may be used to launder money, and if so, how this risk should be addressed in the United Kingdom. Cryptocurrencies have had a tumultuous existence since the publication of original white paper proposing the first cryptocurrency, Bitcoin, by Satoshi Nakamoto in October 2008. Bitcoin in particular has had dramatic fluctuations in its value, and it has been at the centre of high-profile scandals such as the collapse of the Mt Gox exchange in February 2014 and been utilised as the preferred payment method for ransomware demands, such as the 'WannaCry' cyber-attack on the NHS in May 2017. While awareness of cryptocurrencies is growing, the understanding, use and regulation of them remains limited in the United Kingdom. Cryptocurrencies allow transactions, of any size, to be completed within minutes, and without the need for financial institutions to facilitate, or any centralised government interference. The cryptocurrency model relies on a publicly distributed ledger that is maintained by all the computers in the system to keep it up to date and free from fraud and replaces individuals' names with public codes, making cryptocurrencies pseudonymous. The limited awareness of cryptocurrencies, and the degree of anonymity afforded to users, could be viewed as an ideal opportunity for money launderers who are seeking to hide and disguise their proceeds of crime via a decentralised cryptocurrency system.

This thesis concludes that the United Kingdom has not kept pace with international best practice in anti-money laundering regulation with regards to cryptocurrencies, but also that the current international standards do not fully regulate cryptocurrencies from

an anti-money laundering perspective. The gap between the United Kingdom and the leading regulation in the United States of America and Australia will be closed by the implementation of the 5th Anti-Money Directive. However, this thesis proposes that a tailored approach to cryptocurrencies is needed as the application of existing anti-money laundering measures is not compatible with cryptocurrencies and fails to address the blockchain.

Contents

Table of Cases

UK Cases

Australian Cases

USA Cases

Table of Legislation

UK

Bribery Act 2010

Commonwealth of Australia Constitution Act

Criminal Finances Act 2017

Criminal Justice Act 1988

Criminal Justice Act 1993

Drug Trafficking Offences Act 1986

Financial Services and Markets Act 2000

Misuse of Drugs Act 1971

Money Laundering Regulations 2007

Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017

Proceeds of Crime Act 1987

Proceeds of Crime Act 2002

Prosecution of Offences Act 1985

Terrorism Act 2000

Australia

Acts Interpretation Act 1915 (SA)

Anti-Money Laundering and Counter-Terrorism Financing Act 2006

Australian Crime Commission (Western Australia) Act 2004 (WU)

Crimes (Sentencing Procedure) Act 1999 (NSW)

Criminal Code Act 1995

Crimes Act 1914 (Cth)

Financial Transactions Reporting Act 1988

Legislation Act 2001

Monetary Units Act (Vic)

Penalties and Sentences Act 1992 (Qld)

Penalty Units and Other Penalties Act 1987 (Tas)

Road Traffic (Administration) Act 2008 (WA)

USA

Annunzio–Wylie Money Laundering Act 1992

Bank Secrecy Act, Pub. L. 91–508

Code of Federal Regulations Title 31 - Money and Finance: Treasury

Money Laundering Control Act Pub. L. 99-570

Uniting and Strengthening America by Providing Appropriate Tools to Restrict, Intercept and Obstruct Terrorism Act 2001, Pub. L. No. 107-56

Pub. L. No. 99-570, 100 Stat. 3207-18

Securities Exchange Act 1934

US Code Title 18 - Crimes and Criminal Procedure

US Code Title 31 - Money and Finance

US Code Title 7 – Agriculture

International Treaties

Convention against Corruption (adopted 21 October 2003, entered into force 14 December 2005) 43 ILM 37.

Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (adopted 20 December 1988, entered into force 11 November 1990) UNTS 1582.

Convention against Transnational Organised Crime (adopted 15 November 2000, entered into force 29 September 2003) UNTS 2225.

Convention on Psychotropic Substances (adopted 21 February 1971, entered into force 16 August 1976) 520 UNTS 1019.

Single Convention on Narcotic Drugs (adopted 30 March 1961, entered into force 13 December 1964) 520 UNTS 151 (Single Convention on Narcotic Drugs).

Vienna Convention on the Law of Treaties (adopted 22 May 1969, entered into force 27 January 1980) 1155 (UNTS) 331.

EU Treaties

Consolidated Version of The Treaty on The European Union [2012] OJ C326/25.

Consolidated Version of The Treaty on The Functioning of The European Union [2012] OJ C326/156.

Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (adopted 08 August 1990, entered into force 01 September 1993) ETS 141.

Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (adopted 16 May 2005, entered into force 01 May 2005 CETS 198.

EU Legislation

Council Directive 2001/97/EC: [2001] OJ L.344/76

Council Directive 2005/60/EC: [2005] OJ L309/15

Council Directive 2013/36/EU: [2013] OJ L176/338

Council Directive 2015/849/EU: [2015] OJ L.141/73

Council Directive 2018/843/EU: [2018] OJ L 156/43

Council Directive 91/308/EEC: [1991] OJ L166/77

List of Abbreviations

ACIC	Australian Criminal Intelligence Commission
ADCA	Australian Digital Commerce Association
AFP	Australian Federal Police
AGD	Attorney General's Department
AML	Anti-Money Laundering
AML/CFT	Anti-Money Laundering and Countering the Financing of Terrorism
AML/CTF Act 2006	Anti-Money Laundering and Counter Terrorist Financing Act 2006
APCA	Australian Payments Clearing Association
API	Application Program Interface
AUSTRAC	Australian Transaction Reports and Analysis Centre
BSA 1970	Bank Secrecy Act 1970
CACT	Criminal Asset Confiscation Taskforce
CDD	Customer Due Diligence
CDPC	European Committee on Crime Problems
CFTC	Commodity Futures Trading Commission
CGT	Capital Gains Tax
CIP	Customer Identification Program
CJEU	Court of Justices of the European Union
CTR	Currency Transaction Report
DEA	Drug Enforcement Agency
DoJ	Department of Justice

DoS	Department of State
DoT	Department of the Treasury
DTOA 86	Drug Trafficking Offences Act 1986
ECB	European Central Bank
EU	European Union
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation
FCA	Financial Conduct Authority
FinCEN	Financial Crimes Enforcement Network
FIU	Financial Intelligence Unit
GAO	Government Accountability Office
GPML	Global Programme against Money Laundering
GST	Goods and Services Tax
HMRC	Her Majesty's Revenue and Customs
IFTI	International Funds Transfer Instruction
IMF	International Monetary Fund
IRS	Internal Revenue Service
JMLSG	Joint Money Laundering Steering Group
KYC	Know Your Customer
MEP	Member of the European Parliament
MMORPG	Massively Multiplayer Online Role-Playing Games
MOO	Multi Objected Oriented
MUD	Multi-User Dungeon
NCA	National Crime Agency

PATRIOT Act 2001	Uniting and Strengthening America by Providing Appropriate Tools to Restrict, Intercept and Obstruct Terrorism Act 2001
POCA 2002	Proceeds of Crime Act 2002
RICO 1970	Racketeering Influenced and Corrupt Organizations Act 1970
RPG	Role-Playing Game
SAR	Suspicious Activity Report
SEC	Securities Exchange Commission
STR	Suspicious Transaction Report
SYSC	Senior Management Arrangements, Systems and Controls
TFEU	Treaty of the Functioning of the European Union
TFI	Office of Terrorism and Financial Intelligence
TFIU	Terrorism Financing Investigations Unit
TTR	Threshold Transaction Report
UK	United Kingdom
UN	United Nations
UNODC	United Nations Office on Drugs and Crime
US	United States of America
VA	Virtual Asset
VASP	Virtual Asset Service Provider
WMD	Weapons of Mass Destruction
WoW	World of Warcraft

Title:

Money Laundering through Cryptocurrencies: Analysing the responses of the United States and Australia and providing recommendations for the UK to address the money laundering risks posed by cryptocurrencies.

Chapter 1. Introduction

1.1. Background

Cryptocurrencies have had a tumultuous existence since the publication of the original white paper proposing the first cryptocurrency, Bitcoin, by Satoshi Nakamoto in October 2008.[1] Bitcoin in particular has had dramatic fluctuations in its value,[2] and it has been at the centre of high-profile scandals such as the collapse of the Mt Gox exchange in February 2014,[3] and been utilised as the preferred payment method for ransomware demands, such as in the 'WannaCry' cyber-attack on the NHS in May 2017.[4] While awareness of cryptocurrencies is growing, the understanding, use and regulation of them remains limited in the UK, as identified by the Financial Conduct Authority (FCA) in March 2019 when it published research into UK consumers' use of

[1] The published name of the author(s) is widely accepted to be a pseudonym and their real identity remains unknown: Bitcoin Wiki, 'Research' <http://bitcoin.org/bitcoin.pdf> accessed 10 June 2015.
[2] Huge spikes in the value of Bitcoin can be seen through a 10-year chart of its value against the US$: XE, 'XE Currency Charts: XBT to USD' <https://www.xe.com/currencycharts/?from=XBT&to=USD&view=10Y> accessed 07 October 2019.
[3] BBC News, 'MtGox bitcoin exchange files for bankruptcy' (28 February 2014) <https://www.bbc.co.uk/news/technology-25233230> accessed 07 October 2019.
[4] BBC News, 'NHS cyber-attack: GPs and hospitals hit by ransomware' (13 May 2017) <https://www.bbc.co.uk/news/health-39899646> accessed 097 October 2019.

cryptocurrencies.[5] The headline findings were that cryptocurrencies were being bought based on limited information, with purchasers often being influenced by a rejection of mainstream media, a fear of missing out on trends, and seeking to 'get rich quick'.[6] It follows that if consumers are poorly informed, then they are more likely to make poor financial choices. An indication of this can be seen in the numbers of individuals being used as money mules is increasing both in younger people[7] and older people,[8] which raises concerns that cryptocurrencies could be utilised in a similar fashion.

Cryptocurrencies allow transactions, of any size, to be completed within minutes, without the need for financial institutions to facilitate, or any centralised government interference.[9] The cryptocurrency model relies on a publicly distributed ledger that is maintained by all the computers in the system, to keep it up to date and free from fraud.[10] The ledger, known as a blockchain replaces individuals' names with public codes.[11] The anonymity attached to cryptocurrencies is described as pseudonymous,[12] as although the users' names are not known, other details are published on the blockchain;[13] such as their Bitcoin address, the time of the

[5] Financial Conduct Authority, 'How and why consumers buy cryptoassets: A report for the FCA' (07 March 2019) <https://www.fca.org.uk/publication/research/how-and-why-consumers-buy-cryptoassets.pdf> accessed 23 September 2019.
[6] ibid p.47.
[7] BBC News, 'Rise in teenage money mules prompts warnings' (16 September 2019) <https://www.bbc.co.uk/news/business-49717288> accessed 23 September 2019.
[8] BBC News, ''Money mules': Rising numbers are in middle age' (18 June 2019) <https://www.bbc.co.uk/news/uk-48671542> accessed 23 September 2019.
[9] As demonstrated by the Bitcoin white paper: Bitcoin Wiki, 'Research' <http://bitcoin.org/bitcoin.pdf> accessed 10 June 2015.
[10] ibid p.8.
[11] ibid.
[12] United States Government Accountability Office, 'Virtual Currencies: Emerging Regulatory, Enforcement, and Consumer Protection Challenges' <http://gao.gov/assets/670/663678.pdf> accessed 16 December 2015 at p.6.
[13] The public ledger of Bitcoin. See chapter three at 3.3.2 for explanation of what the blockchain.

transaction, and the amount. The limited awareness of cryptocurrencies, and the degree of anonymity afforded to users, could be viewed as an ideal opportunity for anybody seeking to hide and disguise their proceeds of crime.

Therefore, the aim of this research is to analyse the phenomenon of cryptocurrencies, specifically the legal understanding of cryptocurrencies. Additionally the research will assess whether cryptocurrencies may be used to launder money, and if so, how this risk should be addressed. The recommendations of this research are in relation to the United Kingdom (UK), based on an analysis of cryptocurrencies, the development of existing anti-money laundering (AML) regulation, and the responses of the United States of America (US) and Australia.

1.2. Research Question

How can the UK learn from international guidance and the approaches of the United States and Australia to address the money laundering risks posed by cryptocurrencies?

1.3. Research Objectives

This thesis will critique the approach of the UK to the money laundering threat posed by cryptocurrencies. In order to answer the research question, it is necessary to identify and distinguish the different types of virtual currencies, so as to determine which virtual currencies require regulation, and the most appropriate use of regulation. It will be established that cryptocurrencies are a class of virtual currencies which

require specific attention. The concept of money will be explored, specifically whether cryptocurrencies are money. The reason being is if cryptocurrencies are considered to be classified as money then AML legislation should already be applied. This research will examine the development of the AML legislation from its beginnings as part of the United Nations (UN) 'War on Drugs', through to the modern-day entanglement with terrorism financing.[14] The aim of this historical analysis will be to better predict developments and to demonstrate the evolution of AML regulation in response to the continuing evolution of money laundering. This research includes case studies of the US and Australia, analysing their reactions to the development of cryptocurrencies. These case studies are used to contrast with the position of the UK and inform the recommendations of this thesis. The US is a world leader in AML regulation,[15] often being the first to adopt new measures,[16] and first criminalised money laundering in 1986,[17] the same year as the UK.[18] Australia has also been at the forefront of tackling money laundering, enacting criminal offences the 1987,[19] and has recently taken the step of regulating cryptocurrencies.[20]

[14] See chapter four at 4.5 for a detailed chronology of AML development, with reference to: Uniting and Strengthening America by Providing Appropriate Tools to Restrict, Intercept and Obstruct Terrorism Act 2001 and the development of the term 'reverse money laundering': S. D. Cassella, 'Reverse money laundering (2003) 7(1) Journal of Money Laundering 92 at pp.92-93.
[15] N. Ryder, *Money laundering – an endless cycle? A comparative analysis of the anti-money laundering policies in the United States of America, the United Kingdom, Australia and Canada* (Routledge, London, 2012) at 1.3.
[16] Examples include the Bank Secrecy Act, Pub. L. 91–508, Money Laundering Control Act Pub. L. 99-570 and Annunzio–Wylie Money Laundering Act 1992 §1571. See chapter four timeline of anti-money laundering developments for more detail.
[17] Money Laundering Control Act Pub. L. 99-570.
[18] Drug Trafficking Offences Act 1986.
[19] Proceeds of Crime Act 1987.
[20] AUSTRAC, 'New Australian laws to regulate cryptocurrency providers' <http://www.austrac.gov.au/media/media-releases/new-australian-laws-regulate-cryptocurrency-providers> accessed 23 July 2018.

Where possible this thesis will not address the crime of terrorist financing, which has become entangled with money laundering since the turn of the century. This is justified by the distinct nature of the two practices, and therefore each requiring a distinct regulatory approach. This position is supported by Alexander[21] and Roberge[22] who both distinguish money laundering and terrorist financing based on the aims of the two crimes, money laundering is concerned with the origins of the money, compared to terrorist financing which is concerned with its destination. Cryptocurrencies undoubtedly have terrorist financing applications, and while there may be some common ground with money laundering, terrorist financing cannot be adequately covered within this thesis in conjunction with money laundering.

This thesis critiques the current approach toward cryptocurrencies in the UK, with reference to international guidance and the measures adopted in the US and Australia, to recommend appropriate reforms. This analysis comes at a time when the UK government has publicly stated it will regulate cryptocurrencies, so as to comply with the 5th Anti-Money Laundering Directive,[23] but detail on this regulation is lacking.[24]

[21] R. Alexander, *Insider Dealing and Money Laundering in the EU: Law and Regulation* (Aldershot: Ashgate, 2007) at p.173.
[22] Ian Roberge, 'Misguided Policies in the War on Terror? The Case for Disentangling Terrorist Financing from Money Laundering' (2007) 27(3) Political Studies Associations 196.
[23] Council Directive 2018/843/EU 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 L 156/43.
[24] Discussed in chapter five at 5.7 and outlined in: HM Treasury, 'Cryptoassets Taskforce: final report' (29 October 2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf> accessed 20 September 2019.

1.4. Central Argument

This thesis argues that a tailored approach is needed towards the regulation, and monitoring of cryptocurrencies, and simply transposing existing regulations onto cryptocurrencies will not be effective. Justifications for this include concerns that transactions within the networks of cryptocurrencies do not go through regulated entities, and that existing AML tools are not compatible with cryptocurrencies, such as freezing transactions to allow time for investigations by regulators. Current international best practice issued by the Financial Action Task Force (FATF), and legislation enacted by the European Union (EU), ignores the wealth of data available through the distributed ledgers of cryptocurrencies. It is recommended that the UK utilises the data available through the blockchain to monitor money laundering and aid investigations. A plethora of software tools exist which can visualise the blockchain and analyse the data available,[25] allowing supervision to widen from just the intersections between fiat currency and cryptocurrency to all transactions. The wealth of transaction data available in a digital format, paired with the traditional AML measures applied to cryptocurrency service providers, will begin to address the currently unregulated realm of cryptocurrencies.

Despite the shortcomings of the current level of AML regulation of cryptocurrency service providers, it is recommended that the UK follows international recommendations pertaining to applying AML to cryptocurrency service providers. The

[25] Tools such as Maltego: Maltego, 'Visualising the Bitcoin Blockchain in Maltego' (12 April 2016) <http://maltego.blogspot.com/2016/04/visualization-bitcoin-blockchain-in.html> accessed 07 October 2019 and a variety of tools offered here: Examples can be found at Blockchain Luxembourg, 'Bitcoin Developer APIs' <https://www.blockchain.com/api> accessed 26 September 2019.

UK should follow the guidance of the FATF[26] as the leading global AML organisation, and implement the 5th Anti-Money Laundering Directive enacted by the EU.[27] The reason for this is that the UK is currently lagging behind in developing AML regulation of cryptocurrencies and it should utilise the examples set by the US and Australia so as to close the gap. The 5th Anti-Money Laundering Directive adds "*virtual currency exchange platforms as well as custodian wallet providers to the list of obliged entities within the scope of the Directive*;"[28] which mirrors the guidance of the FATF with regards to bringing points of intersection between virtual currencies and the traditional financial system under the scope of EU AML regulations. The UK implemented the 5th Anti-Money Laundering Directive in January 2020,[29] and exceeded the requirements of the Directive by applying AML measures to transactions involving exchanges between cryptocurrencies as well as exchanges between cryptocurrencies and fiat currencies.

This thesis argues that consistent terminology should be used to refer to cryptocurrencies to provide clarity to regulators and market users. Currently a number of different terms are being used by international and supranational organisations, such as the FATF and the EU, and nationally by the UK, the US, and Australia. This

[26] The Financial Action Task Force is the leading international organisation tackling money laundering, as identified in chapter four, their latest guidance can be found here: Financial Action Taskforce, 'FATF Report to the G20 Finance Ministers and Central Bank Governors' <http://www.fatf-gafi.org/media/fatf/documents/reports/FATF-Report-G20-FM-CBG-July-2018.pdf> accessed 23 July 2018.
[27] Council Directive 2018/843/EU 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 L 156/43.
[28] EUROPA, 'Revision of the Fourth Anti-Money-Laundering Directive' <http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/607260/EPRS_BRI%282017%29607260_EN.pdf> accessed 10 September 2019.
[29] The Money Laundering and Terrorist Financing (Amendment) Regulations 2019, SI 2019/1511.

thesis recommends the term cryptocurrencies as this term specifically refers to exclusively digital virtual currencies, which operate based on a decentralised network using a distributed ledger. The term 'virtual assets', used by the FATF, is too broad as the term could also include virtual currencies which are centralised, and can be regulated through regulation of that central authority. Cryptocurrencies are a specific subset of virtual currencies, which due to their decentralised nature require unique AML measures. The EU use the term 'virtual currencies' and Australia used the term 'digital currency',[30] both of which suffer from the same shortcomings as the FATF term, as they do not sufficiently define cryptocurrencies. The agencies of the US also predominantly use the term 'virtual currencies',[31] but the terminology used by the various authorities in the US is not consistent. It is still too early to determine whether cryptocurrencies are going to replace fiat money, or even compete with it, but the current levels of cryptocurrency usage require a clear response from the UK government and authorities.

1.5. Identifying Cryptocurrencies

Cryptocurrencies are a category of virtual currency. The term virtual currencies used alone refers to any currencies which exist solely in electronic form, having no official physical form. A virtual currency is defined by the FATF as;

[30] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.5.
[31] As demonstrated throughout the GAO report on in 2014: United States Government Accountability Office, 'Virtual Currencies: Emerging Regulatory, Enforcement, and Consumer Protection Challenges' <http://gao.gov/assets/670/663678.pdf> accessed 04 September 2019. The term is also used by FinCEN: FinCEN, 'Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies' (9 May 2019) <https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf> accessed 04 September 2019. The CFTC refer to Bitcoin directly, but also use the term: CFTC, 'Bitcoin and Other Virtual Currencies' https://www.cftc.gov/Bitcoin/index.htm> accessed 04 September 2019.

> "*a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status … It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency.*"[32]

The focus of the FATF definition is on the functions of money and how virtual currencies meet the requirements based on user acceptability. This contrasts to the European Central Bank (ECB) viewed virtual currencies as 'schemes',[33] and in 2012 defined them 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*."[34] The ECB updated their position in 2015, and stated that "*the word 'unregulated' should be deleted from the definition used in 2012,*"[35] as it recognised some jurisdictions had regulated virtual currencies.[36] The definition was therefore updated to "*digital representation of value, not issued by a central bank, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money*."[37] The ECB do not recognised virtual currencies as money, but accept that they can be used as an alternative to money.

[32] Financial Action Task Force, 'Virtual Currencies – Key Definitions and Potential AML/CFT Risks' <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 27th October 2019 at page 4.
[33] ECB, 'Virtual Currency Schemes' <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> accessed 02 June 2019.
[34] ibid at p13.
[35] ibid at p25.
[36] ibid.
[37] ibid.

Both the FATF and the EU place emphasis on the transferability of virtual currencies for fiat currencies, but the FATF also considers the administration of the virtual currency as part of its classifications, distinguishing between centralised and decentralised systems. Figure 1 below demonstrates how the FATF categorises virtual currencies.

Figure 1. FATF Categories of Virtual Currency[38]

	Centralised	Decentralised
Convertible	Linden Dollars (used in Second Life) are an example of a convertible virtual world currency; users may exchange their currency for US Dollars. The currency is centralised, Linden Labs (the developer of Second Life) act as administrators.	Examples of decentralised currencies include Bitcoin and Dogecoin. These are convertible for fiat currency but not controlled by a central administrator.
Non-Convertible	World of Warcraft (WoW) gold is non-convertible virtual world currency; users may not convert this into a fiat currency. WoW gold is controlled by the game developers, Blizzard	None exist.[39]

[38] Financial Action Task Force, 'Virtual Currencies – Key Definitions and Potential AML/CFT Risks' <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 27th October 2019 at p.8.
[39] ibid.

As can be seen in Figure 1, the FATF consider the structure and convertibility of the virtual currency in order to categorise them. Structures are either centralised or decentralised, and a virtual currency can be either convertible or non-convertible. A virtual currency is centralised when it is controlled by a single administrating authority; examples of these are the currencies of virtual worlds. The degree of control exercised may vary according to the practices of the administrator and whether the currency is convertible or not. A decentralised currency has no central authority; instead it functions using algorithms and programming code to manage the production of the currency. The focus of this research is upon convertible decentralised virtual currencies, known as cryptocurrencies. Cryptocurrencies are particularly novel due to their decentralised nature, which is also what makes them so challenging for regulators, there is no administrator who can be subject to regulation. The operation of cryptocurrencies is best explained through the leading example of Bitcoin.

1.5.1. Bitcoin

Bitcoin warrants particular attention due to its value,[40] and because it is the forerunner to the growth of cryptocurrencies.[41] Bitcoin is a virtual currency but is also referred to as a cryptocurrency, a currency which uses cryptography to disguise or protect the users of the currency. Cryptocurrencies utilise cryptography techniques to conceal the identity of the sender and receiver of a message or transfer, Southall and Taylor[42] trace the technique used by Bitcoin, and many other currencies, back to proposals

[40] BBC News, 'Bitcoin Currency Hits New Record High' <https://www.bbc.co.uk/news/business-42135963> accessed 19 March 2019.
[41] Though widely considered the first cryptocurrency, the original paper proposing Bitcoin references a number of papers including previous proposals for web-based money such as: W. Dai, 'b-money' (1998) <http://www.weidai.com/bmoney.txt> accessed 13 October 2019.
[42] E. Southall and M. Taylor, 'Bitcoins' [2013] 19(6) Computer and Telecommunications Law Review 177.

made by Chaum in the early 1980's. Chaum proposed sending private messages with a serial key system;[43] messages were sent using a public key, but only the sender and recipient could access the message using a private key. Chaum subsequently suggested the technique could be used to facilitate anonymous payments.[44]

Bitcoin is not the first digital currency; previous digital currencies have been created but failed to persist. Examples of this include 'Beenz' which launched in 1999 and promised to create "*a generation of e-millionaires*"[45] but closed in 2001,[46] just weeks after rival currency 'Flooz'[47] also shut down. As is discussed later in chapter three;[48] numerous factors determine whether something is accepted as money, and as their demise demonstrates, early digital currencies failed to be accepted as money by a large enough community.

Bitcoin was created by Satoshi Nakamoto in 2009.[49] The true identity of Bitcoin's creator(s) is unknown as Satoshi Nakamoto is a pseudonym. It is not known if Satoshi Nakamoto is one person or a group of people as throughout the self-published paper proposing Bitcoins, the term 'we' is used to refer to the author, suggesting it may be more than one person. Bitcoins can be distinguished from early digital currencies, and subsequent digital currencies can be seen to have copied the characteristics of

[43] D. Chaum, 'Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms' [1981] 24(2) Communications of the ACM 84.
[44] D. Chaum, 'Blind Signatures for Untraceable Payments' in D. Chaum. R.L. Rivest and A.T. Sherman (ed), '*Advances in Cryptology*' (Session III, Springer US, 1982) pp199-203.
[45] BBC News, 'Business: The Company File: Beenz means business' (16 March 1999) <http://news.bbc.co.uk/1/hi/business/297133.stm> accessed 12 June 2019.
[46] Commerce Times, 'Beenz.com Closes Internet Currency Business' <http://www.ecommercetimes.com/story/12892.html> accessed 12 June 2015.
[47] CNet, 'E-currency Site Flooz Goes Offline' <http://news.cnet.com/2100-1017-271385.html> accessed 12 June 2019.
[48] See 3.4 and 3.5.
[49] Bitcoin Wiki, 'Research' < http://bitcoin.org/bitcoin.pdf> accessed 10 October 2019.

Bitcoin. Bitcoin operates using the process summarised below as it appeared in the original paper by Satoshi Nakamoto:[50]

1) *New transactions are broadcast to all nodes.*
2) *Each node collects new transactions into a block.*
3) *Each node works on finding a difficult proof-of-work for its block.*
4) *When a node finds a proof-of-work, it broadcasts the block to all nodes.*
5) *Nodes accept the block only if all transactions in it are valid and not already spent.*
6) *Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.*[51]

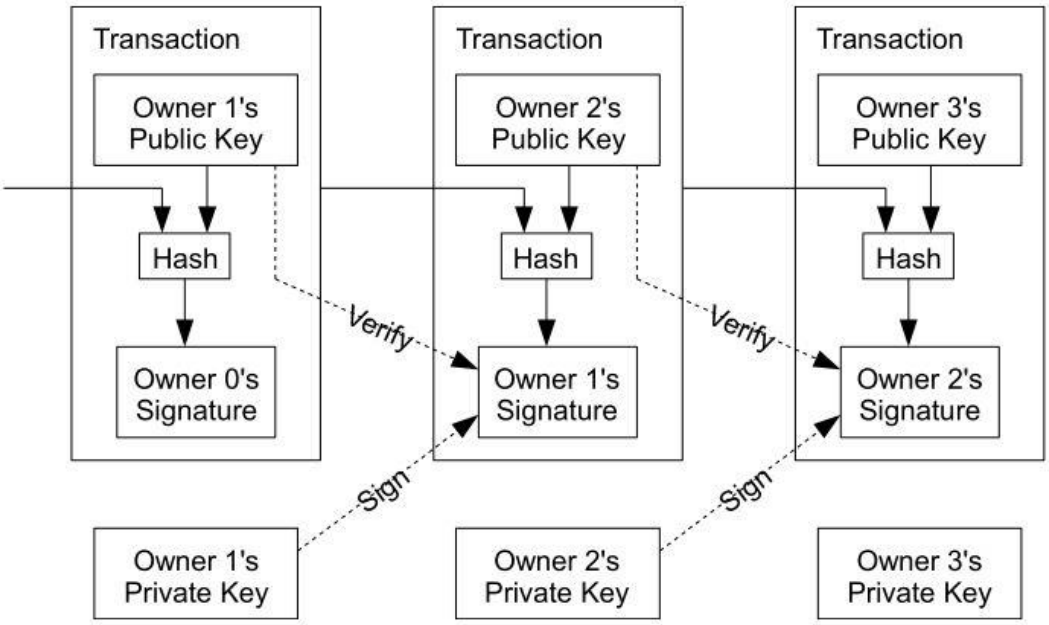
Stage three introduces the concept of proof-of-work, this part of the process is known as mining. The mining process involves a user's computer, known as a node, providing an answer which matches the solution the system is requesting in order to produce a 'block', known as a 'proof-of-work', Blocks are sets of data which are permanent record in the Bitcoin network, they are a leger of Bitcoin transactions,[52] and known as the blockchain.[53] By finding the proof-of-work and completing the block the user then acquires some newly created Bitcoins, currently 6.25 Bitcoins.[54] Each block can only

[50] ibid.
[51] ibid at p.3.
[52] ibid at p.8.
[53] Bitcoin, 'How it Works' <https://bitcoin.org/en/how-it-works> accessed 13 October 2019.
[54] B. Bambrough, 'A Bitcoin Halvening Is Two Years Away - Here's What'll Happen To The Bitcoin Price' (Forbes, 29 May 2018) <https://www.forbes.com/sites/billybambrough/2018/05/29/a-bitcoin-halvening-is-two-years-away-heres-whatll-happen-to-the-bitcoin-price/#4bffecd05286> accessed 19 March 2019.

be produced once, the Bitcoin reward goes to the miner who first produces the block, and duplicates are not accepted. The alternative way to obtain Bitcoins is via cryptocurrency exchanges.[55]

Users send messages to each other in order to send and receive Bitcoins; this process uses a cryptography technique similar to that proposed by Chaum. When a user sends another user some Bitcoins two keys are used. The first is the public key which tells the network of the transaction between the two keys, the second is a private key which is a signature from the sender which prevents the amounts being transferred from being altered by anyone else in the network.[56] This is shown below in Figure 2.

Figure 2. Bitcoin Transactions[57]



[55] Rates can be viewed here: Bitcoin Charts, 'Markets' <http://bitcoincharts.com/markets/> accessed 18 June 2015.
[56] Bitcoin.org, 'How Does Bitcoin Work?' <http://bitcoin.org/en/how-it-works> accessed 19 January 2014.
[57] Taken from: Bitcoin Wiki, 'Research' <http://bitcoin.org/bitcoin.pdf> accessed 10 June 2015.

The use of keys rather than names allows all transactions to be public and verifiable, to ensure no Bitcoins are spent twice, but still ensure the anonymity of those making the transactions. This anonymity will be lost if the user's key were to become public, and then all transactions may be traced. The anonymity attached to cryptocurrencies is addressed by the United States Government Accountability Office in their 2014 report, which described such currencies as pseudonymous.[58] The term pseudonymous is used as, although the users name is not known, other details are published on the blockchain, such as their Bitcoin address, the time of the transaction, and the amount. Transactions of Bitcoins are authenticated by users of the network. Authentication ensures the sender has sufficient funds and that there are no duplicated uses of Bitcoin. This authentication occurs when the proof-of-work is found; at this point the computer which solved the proof-of work verifies all of the transactions which took places since the last proof-of-work was produced.[59] In order to control the number of Bitcoins being produced the difficulty of the proof-of-work problems is adjusted based on the average time between blocks.[60] The variability in difficulty is to compensate for increasing computing power. The Bitcoin system aims for a block to be produced every 10 minutes.[61]

Bitcoin's model of coin production, transaction security and transaction logging has been adopted by numerous subsequent currencies, such as Ethereum,[62] Dogecoin[63]

[58] United States Government Accountability Office, 'Virtual Currencies: Emerging Regulatory, Enforcement, and Consumer Protection Challenges' <http://gao.gov/assets/670/663678.pdf> accessed 16 December 2015 at p.6.
[59] Bitcoin Wiki, 'Research' <http://bitcoin.org/bitcoin.pdf> accessed 10 June 2015 at p.3.
[60] ibid.
[61] ibid.
[62] Ethereum, 'Learn about Ethereum' <https://www.ethereum.org/learn/> accessed 13 October 2019.
[63] Dogecoin, 'Dogecoin' <https://dogecoin.com/> accessed 13 October 2019.

and LiteCoin.[64] The various currencies compete amongst each other by claiming to offer faster transaction speeds or increased security.[65] A key feature of cryptocurrencies is the use of a blockchain, also known as distributed ledger.[66] A crytpocurrency's blockchain is usually publicly available.[67] The accessibility of cryptocurrency blockchains can be further aided through the use of Application Programme Interfaces[68] (APIs) which allow for the creation of applications to analyse the transaction data published in the blockchain. The identity protection afforded by cryptocurrencies such as Bitcoin can also be challenged as Meiklejohn *et al* "*were able to identify 1.9 million public keys with some real-world service or identity,*"[69] however, "*in many cases the identity was not a real name, but rather (for example) a username on a forum.*"[70] More recently, Juhász *et al* identified 22363 users' 1797 associated IP addresses.[71] While difficulties will remain with determining which users require identification and investigation, Juhász *et al* argue their "*method is cheap in terms of resources,*"[72] and their "*algorithms are relatively easy to implement and can be combined with other Bitcoin-transaction related information.*"[73] The research of

[64] LiteCoin, 'LiteCoin' <https://litecoin.org/> accessed 13 October 2019.
[65] The Guardian, 'Nine Bitcoin alternatives for future currency investments' <http://www.theguardian.com/technology/2013/nov/28/bitcoin-alternatives-future-currency-investments> accessed 17 June 2015.
[66] Financial Conduct Authority, 'FCA publishes Feedback Statement on Distributed Ledger Technology' (15 December 2017) <https://www.fca.org.uk/news/press-releases/fca-publishes-feedback-statement-distributed-ledger-technology> accessed 13 October 2019.
[67] As demonstrated by: Blockchain, 'Block Explorer: Bitcoin' <https://www.blockchain.com/explorer> accessed 13 October 2019, Blockchain, 'Block Explorer: Ethereum' <https://www.blockchain.com/explorer?currency=ETH> accessed 13 October 2019, and Blockchain, 'Block Explorer: Bitcoin Cash' <https://www.blockchain.com/explorer?currency=BCH> accessed 13 October 2019.
[68] H. Henderson, 'application programming interface (API)' in Harry Henderson (ed) Encyclopedia of Computer Science and Technology (3rd ed, Facts On File, 2017) <https://search-credoreference-com.ezproxy.uwe.ac.uk/content/entry/fofcomputer/application_programming_interface_api/0>
[69] Sarah Meiklejohn, et al, "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names," (2013) 38(6) ;Login: 10 at p.14.
[70] ibid.
[71] P. L. Juhász, J. Stéger, D. Kondor and G. Vattay, 'A Bayesian approach to identify Bitcoin users' (2018) 13(12) PLoS ONE 1 at p.13.
[72] ibid at p.18.
[73] ibid.

Meiklejohn *et al* and Juhász *et al* demonstrate that the anonymity of cryptocurrencies may be eroded by the aforementioned techniques, but more research is needed.

Bitcoin, and other cryptocurrencies, are exchanged globally and are referred to in similar terms as money, such as the term ‘currency’ within cryptocurrency, the term ‘cash’ in Bitcoin Cash, and the symbol used in Bitcoin’s logo being akin to a monetary symbol. Due to the connotations towards money, and cryptocurrencies representing such a novel and undefined phenomenon, money is analysed in chapter 3, to determine whether cryptocurrencies are indeed money, or have the potential to become money.

1.6. UK Withdrawal from the EU

This research has taken place during a time of political upheaval, most notably for the UK due to the ongoing exit from the European Union (EU). As this research is concerned with the AML regulation of cryptocurrencies it will not focus on the political wrangling related to the UK leaving the EU for a number of reasons. Firstly, it has not yet happened, and as with many things relating to leaving the EU, there is little to no direction given. Secondly, as will be seen in chapter four, in relation to money laundering, the behaviour of the UK since 1970 indicates that very little is likely to change as the UK has been an early adopter of international best practice. Thirdly, and finally, as the UK is a member of the FATF, and, as is also seen in chapter four, the EU and the FATF prescribe very similar approaches to money laundering. The UK will continue to be compliant with EU AML legislation, by virtue of meeting the FATF standards, whether it is a member of the EU or not. As identified in chapter five, the

UK implemented the 5th EU Anti-Money Laundering Directive in January 2020,[74] showing that it will continue to keep pace with international best practice. The recommendations from this research suggest that no jurisdiction or international organisation has sufficiently addressed the risks posed by cryptocurrencies, and that the UK should take initiatives of its own to utilise the potential of blockchains to assist investigations. This further justifies the omission of a debate over the UK's future relationship with the EU, as it will distract from the aims of this research.

1.7. Chapter Structure

Following on from this introduction, chapter two will consist of a literature review and a justification of the methodology and methods used in this research. Chapter three will provide contextualisation by introducing and defining key terms for the purpose of this thesis; this will provide clarity. The chapter also considers the concept of money from a socio-political perspective and determines whether cryptocurrencies are money. The objective of this comparison is to improve the understanding of cryptocurrencies, this is aided by questioning the concept of money, as money is a concept which most in society readily accept and relate to without ever considering why.[75] As cryptocurrencies are frequently compared to money in the media,[76] and cryptocurrency transactions can be used in lieu of money, this comparison is pertinent and valuable. The contextualisation chapter will distinguish the different types of virtual

[74] The Money Laundering and Terrorist Financing (Amendment) Regulations 2019, SI 2019/1511.
[75] Bank of England, 'What is Money?' (19 February 2019) <https://www.bankofengland.co.uk/knowledgebank/what-is-money> accessed 07 October 2019.
[76] BBC News, 'Bitcoin explained: How do crypto-currencies work?' (12 February 2018) <https://www.bbc.co.uk/news/av/technology-43026143/bitcoin-explained-how-do-crypto-currencies-work> accessed 20 July 2018.

currencies and identify cryptocurrencies as the specific virtual currencies which pose the highest risk, and thus the focus of this thesis and its recommendations.

Chapter four focusses on the phenomenon of money laundering, the term is defined, the process will be explained, and examples of the impacts of money laundering will be briefly explored. The chapter provides a timeline of the international, regional and domestic AML developments, beginning in the 1960s with the initial attempts of the UN. The timeline identifies themes, which will provide an insight into the likely trajectory of future AML developments, such as the rise of the FATF to the lead international organisation, taking over from the UN, and the increased influence of EU legislation as its Anti-Money Laundering Directives have become more prescriptive. The UK, the US and Australia are all members of the UN, and are fully compliant with UN AML conventions, as well as all being members of the FATF, and each achieving high levels of compliance in their recent mutual evaluation reports,[77] and the UK is, at the time of writing, a member of the EU. The ongoing departure of the UK from the EU is not a central theme of this thesis, along with many other issues, the status of EU AML is not known, so little will be achieved through speculation, and, as chapter four demonstrates, there are a number of indicators which suggest the UK will continue to keep pace with EU AML developments. Firstly, the UK has been an early adopter of

[77] FATF, 'Anti-money laundering and counter-terrorist financing measures – United Kingdom, Fourth Round Mutual Evaluation Report' (Paris, December 2018) <fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-Kingdom-2018.pdf> accessed 11 September 2019, Financial Action Task Force, 'Third Mutual Evaluation Report on Anti-Money Laundering and Combatting the Financing of Terrorism: United States of America' <http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20US%20full.pdf> accessed 03 September 2019, and Financial Action Task Force, 'Anti-money laundering and counter-terrorist financing measures - Australia, Fourth Round Mutual Evaluation Report' <https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Report-Australia-2015.pdf> accessed 23 July 2019.

international AML best practices and there is no evidence to suggest this will change. Secondly, the position of the FATF and the EU are notably similar, so by being compliant with FATF Recommendations the UK will be comparably compliant with EU regulation, and vice versa. Thirdly, a key motivator for the UK to adhere to two points above is the status of London as an important global financial centre,[78] in order to retain this position after the UK leaves the EU, amongst other factors, the UK will have to maintain its AML compliance, or face loss of reputation. Chapter four will provide an analysis of the prevailing international approach to the money laundering risks posed by cryptocurrencies, this is particularly helpful in predicting and recommending an approach for the UK, as the UK is a member of a number of international organisations. Given that cryptocurrencies are non-physical, they are inherently an international concern, therefore the approach of the international community will provide valuable assistance to the UK as it determines its approach.

Chapter five concentrates on the UK and considers how the UK can adapt its approach to cryptocurrencies and the money laundering risks posed. The relevant money laundering offences will be considered, as well as the preventative measures, in order to determine the applicability of the current AML laws to cryptocurrencies. The relevant authorities are identified, and their stances on cryptocurrencies are analysed. The UK case study will allow its approach to cryptocurrencies to be contrasted to that of the US and Australia and assesses the UK's compliance with the current FATF guidance for regulating cryptocurrency service providers.

[78] J. Treanor, The Guardian, 'London still world's top financial centre despite Brexit, says survey' <https://www.theguardian.com/business/2017/sep/11/london-financial-centre-brexit-frankfurt-dublin-new-york-donald-trump> accessed 20 July 2018.

Chapters six and seven will be on the US and Australia respectively, detailing their approach to money laundering and how each jurisdiction is addressing the money laundering risks posed by cryptocurrencies. In each case study the relevant money laundering legislation will be considered in two categories; firstly, the criminal offences of money laundering will be analysed, in order to determine whether the offences can be committed using cryptocurrencies. Secondly, the relevant AML will be analysed, this is the legislation which is designed to detect and prevent money laundering occurring, requiring the compliance of institutions in affected industries. The purpose of analysing the criminal offences and the preventative measures is to identify which elements of each jurisdiction's approach to the money laundering risks of cryptocurrencies needs to be addressed. As well as analysing the law, the case studies will also consider the roles of each jurisdiction's relevant authorities, and their approach to cryptocurrencies, legislation is imperative, but it is ineffective if it is not being enforced by the relevant bodies. Lastly, each jurisdiction is judged against the FATF guidance to assess their levels of compliance with regards to cryptocurrencies and recommendations are made for the UK. The US and Australia have implemented similar regulation of cryptocurrency service providers but achieved it through contrasting mechanisms. The US, through the actions of the Financial Crimes Enforcement Network (FinCEN), has taken a regulator led approach to expanding AML regulation to cryptocurrency service providers, whereas Australia, through its Parliament as a legislature, has taken a legislator led approach.

Chapter eight provides an overall conclusion, emphasising the central argument of this thesis; the UK should adopt a tailored approach to cryptocurrencies rather than apply existing measures. Simply applying anti-money laundering legislation to the fringes of the system is ineffective in gathering financial intelligence. A tailored approach to cryptocurrencies will better utilise the data available from blockchains and potentially aid money laundering investigations. It is argued that utilising the wealth of transaction data available in a digital format, paired with the traditional AML measures applied to cryptocurrency service providers, will begin to address the currently unregulated realm of cryptocurrencies. Having identified the approaches of the US and Australia in chapters six and seven, it is recommended that the UK takes a legislator led approach to widening the regulatory perimeter to cryptocurrency service providers, this is because the FCA has failed to initiate a regulator led expansion of AML regulation. This thesis also recommends further research is required, specifically in collaboration with those who are able to best analyse the blockchain to realise its huge potential as an investigative tool.

1.8. Research Themes

A number of issues must be addressed in order to answer the research question. Cryptocurrencies must be placed in context, it must be determined whether they are money, or have the potential to be money as currently cryptocurrencies lack a clear legal status. This research stops short of concluding that cryptocurrencies have the same standing as money, this will be fully explored in chapter three, but it will be argued that cryptocurrencies are capable of becoming money if their value stabilises

and their usage increases. This argument is made based on cryptocurrencies being placed within a hierarchy of money.

A further important consideration is the prevailing approach to money laundering, the risk-based approach. Cryptocurrencies and their use must be judged against the risk-based approach to money laundering, a key determining factor being the higher the usage, both in volume and value, the greater the risk. Other considerations which will determine the level or risk, and as such proportionate response, are the ease of use, the speed at which the money laundering process can be completed, and the amounts of money which may realistically be laundered through cryptocurrencies. While cryptocurrencies pose money laundering risks, and successful prosecutions demonstrate their use for money laundering purposes, there is no evidence that the majority of transactions are illicit. If particularly onerous requirements are placed on cryptocurrency service providers, it may cause such businesses to try and avoid the regulation and push the industry underground. This would leave users in a potentially vulnerable position and make pursuing money laundering more difficult.

While cryptocurrencies are a very modern phenomenon, the past is still a valuable resource in predicting the future, what has gone before provides hindsight to previous developments, and a valuable learning opportunity. Cryptocurrencies are new, but money laundering is most definitely not, as chapter four will demonstrate, therefore this thesis will use the development of anti-money laundering legislation over the past half century, to predict the future developments of anti-money laundering in relation to cryptocurrencies.

This thesis will use a case study approach, to take the issue of money laundering risks posed by cryptocurrencies, and analyse the reaction within the US and Australia to advise the approach in the UK. The focus of the recommendations relates on the UK, but given the inherently international nature of cryptocurrencies, and of money laundering, the recommendations will have wider applicability. The recommendations for the UK are to implement the 5th Anti-Money Laundering Directive so as to meet current international standards, but to also address the regulatory gaps that remain. The UK should seek to harness the wealth of intelligence within distributed ledgers and utilise developments in AI and machine learning to help automate the monitoring process. Coupling the data gathered from distributed ledgers with AML regulation of cryptocurrency service providers will better address the regulatory gaps created by cryptocurrencies.

Chapter 2. Literature Review and Methodology

2.1. Literature Review

This literature review considers existing knowledge of money laundering, identifying trends in existing anti-money laundering (AML) regulation, and in the development of AML regulation internationally and domestically in the United Kingdom (UK), the United States of America (US), and Australia. The existing legislation is identified, as well as the relevant domestic and international authorities, it is observed that the UK has fallen behind the US and Australia in AML regulation, as it has yet to address the threats posed by cryptocurrencies. International guidance and initial attempts to regulate cryptocurrencies are observed to be a commendable first step to addressing the money laundering threat, but as the majority of cryptocurrency transactions remain outside of AML regulation, a clear regulatory gap exists.

2.2. Themes

The principal purpose of this research is to analyse the money laundering risks posed by cryptocurrencies, but a number of issues must be explored in order to answer the research question. Cryptocurrencies must be examined, definitions must be analysed, specifically against the concept of money, considering whether cryptocurrencies are a form of money. The phenomenon of money laundering needs to be explained and it must be determined whether cryptocurrencies may be used in this process, and whether the current criminal offences are applicable. As well as the criminal offences, the applicability of the preventative measures will be analysed. Ultimately this thesis

will consider how cryptocurrencies should be regulated in order to address the money laundering risks posed.

2.2.1. Defining Cryptocurrencies

Cryptocurrencies must be defined, which requires them to be identified as a specific class of virtual currencies and differentiated from fiat currencies and e-money. Fiat currencies are government backed currencies, and designated legal tender. E-money is "*a digital representation of a fiat currency,*"[1] which is used to transfer fiat currency electronically; it is not a separate currency, merely the mechanism by which legal tender is transferred. Virtual Currency is defined by the Financial Action Task Force (FATF) as;

> "*a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status … It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency.*"[2]

[1] Financial Action Task Force, 'Virtual Currencies – Key Definitions And Potential AML/CFT Risks' <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 27th November 2014.
[2] ibid 4.

This definition could apply to both virtual world currencies, including Second Life Linden Dollars,[3] and stand-alone cryptocurrencies, such as Bitcoin;[4] but distinctions between these currencies must be made. Virtual currencies may be either convertible or non-convertible, and centralised or decentralised.[5] A virtual currency is convertible if it may be exchanged for a fiat currency; if this is not possible, the currency is non-convertible; these distinctions will be explored in chapter three. In addition to the convertibility of a virtual currency, chapter three will also define virtual worlds and distinguish these from virtual currencies, once these distinctions are made, the focus of the thesis will be on convertible decentralised currencies, known as cryptocurrencies.[6] This focus is justified as cryptocurrencies pose the greatest money laundering threat, as identified by the FATF.[7] Cryptocurrencies are problematic because there is no central authority managing the cryptocurrency, or providing a redress system, so no institution exists which can apply AML measures such as suspicious activity reports (SARs) or customer due diligence. Confusion exists as to the accepted terminology to use when referring to cryptocurrencies, with a number of different terms being used by both international and supranational organisations, such as the FATF and the EU, and nationally by the UK, the US, and Australia. The term

[3] Full explanation of Linden Dollars can be found at: Linden Labs, 'LindeX™ Exchange' <https://secondlife.com/my/lindex/#> accessed 28 August 2018. (login may be required) Tromans explores the issue of Second Life: Richard Tromans, 'The World is not Enough: Law for a Virtual Universe' (2007) 70 Euro Law 21.

[4] Bitcoin is defined and explained in chapter three at 3.3.2, more can be found on the ongoing debate of the definition and regulation in Richard Alexander, 'How to Regulate Bitcoin – the Debate Continues' (2018) 39(3) Comp Law 65, Robbert Jacobs, 'European Union: Virtual Currencies – Warning' (2018) 33(3) JIBLR 29 and Benjamin Geva, 'Disintermediating Electronic Payments: Digital Cash and Virtual Currencies' (2016) 31(12) JIBLR 661.

[5] cf Financial Action Task Force (n1) p4.

[6] The term cryptocurrency will be used to refer to convertible decentralised virtual currencies. Being cryptography based allows these virtual currencies to be decentralised. The currencies can be seen to resemble system hypothesised by Chaum in Chaum, D, 'Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms' [1981] 24(2) Communications of the ACM 84.

[7] cf Financial Action Task Force (n1) p.9

'virtual assets', used by the FATF, is too broad as the term could also include virtual currencies which are centralised, and can be regulated through regulation of that central authority. Cryptocurrencies are a specific subset of virtual currencies, which due to their decentralised nature require unique AML measures. The EU uses the term 'virtual currencies'[8] and Australia uses the term 'digital currency',[9] both of which suffer from the same shortcomings as the FATF term, as they do not sufficiently define cryptocurrencies. The agencies of the US also predominantly use the term 'virtual currencies',[10] but the terminology used by the various authorities in the US is not consistent.

Prominent academics writing on virtual worlds include Castronova, who defines virtual worlds and traces their development,[11] and Lastowka,[12] Hunter,[13] Kerr[14] and Brenner[15] who all consider the application of criminal law within virtual environments. Notably, Brenner attempts to categorise crimes based on the harm caused by the offence; hard harms and soft harms.[16] Hard harms are seen as traditional offences, physical harm

[8] As used in the 5th Anti-Money Laundering Directive: Council Directive 2018/843/EU 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 L 156/43.
[9] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.5.
[10] As demonstrated throughout the GAO report in 2014: United States Government Accountability Office, 'Virtual Currencies: Emerging Regulatory, Enforcement, and Consumer Protection Challenges' <http://gao.gov/assets/670/663678.pdf> accessed 04 September 2019. The term is also used by FinCEN: FinCEN, 'Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies' (9 May 2019) <https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf> accessed 04 September 2019. The CFTC refer to Bitcoin directly, but also use the term: CFTC, 'Bitcoin and Other Virtual Currencies' https://www.cftc.gov/Bitcoin/index.htm> accessed 04 September 2019.
[11] E. Castronova, Virtual Worlds: A First Hand Account of Market and Society of the Cyberian Frontier, [2001] SSRN CESifo Working Paper Series No. 618.
[12] G. Lastowka, *Virtual Justice: The New Laws of Online Worlds* (Yale University Press, 2010)
[13] G. Lastowka and D. Hunter, 'Virtual Crimes' (2004) 49 NYL Sch Rev 294.
[14] O. S. Kerr, 'Criminal Law in Virtual Worlds' [2008] Chi Legal F 415.
[15] S. Brenner, 'Fantasy Crime' (2008) 11(1) V and J Ent & Tech L 1.
[16] ibid at p.4.

against another human, be that murder, rape, other bodily harm or theft and damage to property. Soft harms are non-physical wrongs the law has addressed, offences against harming 'morality', 'affectivity' or causing 'systemic' harm.[17] Brenner argues that offences against morality include the possession and abuse of substances or breaching gambling legislation; these crimes don't directly harm another individual but are against the "*moral sense of the community.*"[18] 'Affectivity' harms are non-physical harms to individuals, be that to their reputation through the former offence of libel[19] or to their security through harassment or stalking.[20] 'Systemic' harms are harms to the system and can be described as regulatory offences such as failure to pay tax or fulfil legal obligations.[21] This thesis is distinguished from the research of these academics as the focus is placed on standalone cryptocurrencies, and not the virtual worlds which the currencies may originate from. If the crime of money laundering were to be placed within Brenner's categories, it would either sit within 'morality' harms of 'systemic' harms, but it would not sit within the virtual worlds Brenner researches.

Interaction with the physical world is another theme which has arisen from the literature review with regard to things which exist within computer systems. The magic circle concept could be applied; first proposed by Huizinga in 1938,[22] it recommends an exclusion zone inside which the rules of the game are to be followed. This protects the game from real world influences,[23] as well as the players; for example, a tackle on

[17] ibid at p.8.
[18] Lawrence Freidman, *Crime and Punishment in American History* (Basic Books 1934) as cited by Brenner (n15) at p.4.
[19] cf Brenner (n15) at p.10.
[20] cf Brenner (n15) at p.12.
[21] cf Brenner (n15) at p.17.
[22] J. Huizinga, *Homo Ludens: A Story of the Play-Element in Culture* (Beacon Press, 1938).
[23] Y. S. Tseng, 'Governing Virtual Worlds: Interration 2.0' (2011) 35 J Law & Policy 547.

a football pitch could easily constitute an assault otherwise. The magic circle can only go so far, potential criminal offences outside of the rules of a sport will still be investigated by authorities, as demonstrated by the racial abuse case in 2012 concerning the footballer John Terry.[24] Based on the magic circle principle it follows that only where the authorities are failing, the rules are inadequate, or the act is of particular severity will the law step in. The magic circle argument may be used to further justify this research; cryptocurrencies may only become a regulatory issue when they interact and affect the traditional financial system. Money laundering would be a clear example of how cryptocurrencies will have effects in the real world; this approach further justifies the focus of the research on convertible currencies as the interactivity of non-convertible currencies is limited.

Contribution to knowledge

This thesis argues for consistency in the terminology used to refer to cryptocurrencies to avoid the current confusion caused by a plethora of terms being used. The UK uses the term 'cryptoassets',[25] which is yet another variation on the terms used by the FATF, the EU, the US, and Australia, and potentially adding to the confusion. The term 'assets' appears deliberate as the FCA does not accept cryptocurrencies as currency or money.[26] The term 'cryptocurrencies' is the best term to use, as this specifically refers to decentralised convertible virtual currencies, which is the class of virtual currencies which pose a money laundering risk, as accepted by all of the organisations

[24] *R v Terry* (Westminster Magistrates, 13 July 2012).
[25] Financial Conduct Authority, 'Guidance on Cryptoassets – Consultation Paper' <https://www.fca.org.uk/publication/consultation/cp19-03.pdf> accessed 19 March 2019 at 2.3.
[26] ibid at 2.7.

and jurisdictions considered in this thesis. Cryptocurrencies have breached the magic circle concept, as they intersect with the traditional financial system.

2.2.2. Defining Money

An important element of this research is to consider the development of money and whether cryptocurrencies can satisfy the definitions of money. Money needs to be defined, which involves exploring the legal definition of money, as well as the concept of money in general, encompassing both theories of money and its functions. Money is a social tool and understanding its role in society is often taken for granted. Definitions of a currency centre on the concept of a certain type of money being the legal tender of a country, and controlled by the central bank of that country, this is consistent with chartalist theories of money.[27] The largest exception to this is the Euro which a currency shared by 19 countries across Europe, and controlled by the European Central Bank, the central bank of the European Union. The Euro can still be incorporated into chartalist theories. If cryptocurrencies can be defined as money, then the relevant AML provisions would apply to cryptocurrency service providers. As such it will be considered whether cryptocurrencies satisfy descriptions of money and whether the functions of money are performed. Chapter three will consider two metallist theories of money and three chartalist theories of money. The metallist theories considered by this thesis are the orthodox theory, explained through the

[27] A. Smith, *An Inquiry Into the Nature and Causes of The Wealth of Nations*, (The Cannon Edition, New York, The Modern Library, 1937).

works of Menger,[28] North,[29] and Jones,[30] and the Marxist theory proffered by Karl Marx.[31] As will be explored in Chapter three, the focus of metallist theories of money is on the physical item which is used as money, so it is difficult to argue cryptocurrencies satisfy the definition as they do not exist physically. The three chartalist theories analysed by this thesis are the state theory of toney, supported by Knapp,[32] Hurst,[33] Smith[34] and Minsky,[35] credit theory, proffered by Innes[36] and Keynes,[37] and social construction theory, which is argued by Zelizer.[38] The theories of money considered can be placed in to the two categories, of metallist or chartalist, because they share certain characteristics. Metallist theories view money as having intrinsic value, the item used as money is valuable even when not being used as money. Chartalist theories consider money to be valuable as tokens of credit, the thing used as money may not have any value in itself, but it gains value through being usable. Money is then the mechanism by which debts are accepted and repaid. Differences in the types of theories also exist when determining who creates money, and where the power relationships exist. The metallist theories view money as a creation of society and merchants; the state has a minor role, instead it is to support the system through contract and property law.[39] Chartalist theories give the state a

[28] K. Menger, 'On Origins of Money' (1892) 2(6) Economic Journal 293.
[29] D. C. North, Institutions, Institutional Change and Economic Performance (Cambridge University Press, 1990).
[30] R. A. Jones, 'The Origin and Development of Media of Exchange' (1976) 84 (4, Part 1) August Journal of Political Economy 757.
[31] K. Marx, *Capital: Vol 1* (London, Penguin, 1976).
[32] G. F. Knapp, *The State Theory of Money* (Macmillan, 1924).
[33] J. W. Hurst, *A Legal History of Money in the United States 1774-1970* (University of Nebraska Press, 1973).
[34] cf Smith (n27).
[35] H. P. Minsky *Stabilising An Unstable Economy* (Yale University Press, 1986).
[36] A. M. Innes, 'What is Money' (1913) 30 Banking LJ 377.
[37] J. M. Keynes, *A Treatise on Money* (Harancourt Brace, 1930).
[38] V. A. Zelizer, 'The Social Meaning of Money: "Special Monies"' (1989) 95(2) 342.
[39] cf North (n29).

greater role, particularly in the state theory of Money, in which the only reason money has value is because the state is willing to accept it.[40] This research will compare these theories of money, determining whether cryptocurrencies fit with the theories. No single theory of money is universally accepted, Bell instead constructs a hierarchy of money, which identifies classes of money and considers which theories may fit within each class.[41] While the hierarchy is formulated around chartalist theories of money, Bell also assesses metallist theories,[42] but finds them to be a poor fit for modern forms of money. Accepting that no existing theories of money are infallible, this research will seek to build on the concept of Bell and place the cryptocurrencies within her hierarchy of money.

As well as the theoretical concept of money, this thesis will consider the functions of money, and whether cryptocurrencies satisfy these functions. In identifying the functions of money Hudson begins with Aristotle's three principles of money; a means of exchange, a measure of value and a store of value.[43] Bell also traces metallist theories back to the functions of money identified by Aristotle,[44] of which the medium of exchange function is the considered the most important, as this replaced barter, though Bell questions whether barter economies ever existed.[45] The three core functions of money have clearly existed for an exceedingly long time, this research will

[40] cf Knapp (n32).
[41] S. Bell, 'The Role of the State and the Hierarchy of Money' (2001) 25 Cambridge Journal of Economics 149 at p.149.
[42] ibid at p.149.
[43] A. Hudson, *The Law of Finance* (Sweet and Maxwell, 2013) at p.40.
[44] cf Bell (n41) at p.151.
[45] ibid.

consider whether cryptocurrencies can perform these functions adequately enough to subsequently claim cryptocurrencies are in fact money.

The concept of money is an important theme in establishing the need to regulate cryptocurrencies, if cryptocurrencies perform the functions of money in society, then the magic circle principle will be categorically breached; if cryptocurrencies can be money then they will have significant interaction with the physical world and cannot be left to be solely regulated by it participants. This research will identify whether AML measures should already apply to cryptocurrencies, establishing cryptocurrencies as money would simplify this contention as money laundering offences, and AML regulation, would be as applicable to cryptocurrencies as they are to Great British Pounds.

Contribution to Knowledge

Chapter three assesses money from a novel perspective and places cryptocurrencies on the hierarchy of money proposed by Bell and identifies that although cryptocurrencies have similar characteristics to money, they cannot be placed as high on the hierarchy as State money. Cryptocurrencies do not fit within existing theories of money as their characteristics straddle both metallist and chartalist theories, notably the absence of state control complying with metallist theories, and its assigned value complying with chartalist theories. Cryptocurrencies are not used as money, rather they are used for investment purposes, but their capacity to effect international transactions of considerable worth means they require AML regulation irrespective of their status as money or not.

2.2.3. Money Laundering

As defined by Lilly money laundering is "*the process whereby the identity of dirty money that is the proceeds of crime and the real ownership of these assets is transformed so that the proceeds appear to originate from a legitimate source.*"[46] Existing AML legislation applies to financial institutions, and other businesses which are exposed to potential money laundering avenues, this is very broad. The analysis of money laundering in chapter four demonstrates, the nature of money laundering is also very broad, utilising any means by which value can be transferred and used to conceal its origin, thus justifying the broad scope of AML regulation. The three-stage process of money laundering, outlined by Gilmore,[47] also used by Ryder,[48] is used to explain the elements of money laundering common to most cases; placement, layering and integration. These stages can be completed in a variety of ways; Ping considers a wide variety of money laundering techniques,[49] evidencing how they have been utilised by criminals with case studies. The variety of methods adopted demonstrates the ingenuity of money launderers and suggests that new technology will quickly be adopted if money laundering can be achieved. This research does not seek to develop theories in relation to the money laundering process, however, the process must be outlined in order for the vulnerabilities of cryptocurrencies to be considered in light of traditional money laundering techniques.

[46] P. Lilley, *Dirty Dealing: The Untold Truth about Global Money Laundering* (London, Kogan Page, 2006) at p6.
[47] W.C. Gilmore, *Dirty Money: The Evolution of Money Laundering Counter-Measures* (Strasbourg, Council of Europe Press, 1995).
[48] N. Ryder, 'The Financial Services Authority and Money Laundering: A Game of Cat and Mouse' (2008) 67(3) Cambridge LJ 635.
[49] Ping He, 'A Typological Study on Money Laundering' (2010) 13(1) JMLC 15.

This research is concerned with the potential for cryptocurrencies to be used for money laundering purposes, as such the research needs to be placed within the existing money laundering literature, which is substantial. This research is not intending to provide a critique of the concept, or the impact of the approaches to combat money laundering in general. This subject has considerable literature already dedicated to it, notably from authors such as Ryder who looks it its cyclical nature,[50] Lilly who provides a clear simple definition of money laundering based on its aims,[51] and Robinson traces the origins of the term.[52] As well as academic writing on money laundering, there are also professional guides to complying with AML measures, such guides can be found for each of the case study jurisdictions in Simpson, Smith and Srivastava's *International Guide to Money Laundering Law and Practice*.[53] This thesis is concerned with whether the measures apply to cryptocurrencies, an area in which there is limited guidance for professionals. The research is also distinguished from work which focussed on the impacts of money laundering, while these impacts are used as part of the justification for researching money laundering, this thesis does not seek to repeat the work of academics such as McDowell and Novis,[54] and Unger.[55] Money laundering is plainly defined by Buchanan:

[50] N. Ryder *Money laundering – an endless cycle? A comparative analysis of the anti-money laundering policies in the United States of America, the United Kingdom, Australia and Canada* (Routledge, London, 2012).
[51] cf Lilley (n46).
[52] J. Robinson, *The Laundrymen* (London, Pocket Books, 1995).
[53] M. Simpson, N. Smith and A. Srivastava (eds), *International Guide to Money Laundering Law and Practice* (Haywards Heath, Bloomsbury Professional, 2010).
[54] J. McDowell and G Novis, 'The Consequences Of Money Laundering And Financial Crime' (2001) 6(2) Economic Perspectives 6.
[55] B. Unger, *The Scale and Impacts of Money Laundering* (Edward Elgar, Cheltenham, 2007).

> "*Simply stated, money laundering is the processing of criminal profits through the financial system to obscure their illegal origins and make them appear legitimate. It is not just enough to hide the proceeds of illegal activities. Equally important in the laundering process is to render the proceeds re-usable for other purposes. Although on the surface money laundering may be simple to define, it is extremely difficult to investigate and prosecute.*"[56]

The purpose of defining money laundering in this research is to be able to consider whether money laundering may be committed using cryptocurrencies. It will not be possible to say definitively that money laundering is taking place, this is an issue for the prosecuting authorities, but this research can assess the potential for cryptocurrencies to be used to launder the proceeds of crime and examples of this can be seen through relevant convictions in the UK and US. This research can be justified in part by the work of Irwin *et al*.,[57] who found that the "*main advantage of the virtual world scenario is the level of anonymity afforded to entities when obtaining financial instruments and placing and moving funds around virtual environments and financial service providers*."[58] The research of Irwin *et al.* focussed on virtual worlds rather than just cryptocurrencies, but many of their conclusions could be applied to cryptocurrencies, as will be explored in chapter four. It is not possible to accurately estimate the amount of money laundering which takes places domestically or internationally. Robinson places money laundering as the third biggest industry in the world,[59] and the International Monetary Fund (IMF) estimate that the amount of money

[56] B. Buchanan, 'Money laundering – a global obstacle' (2004), 18(1) Research in International Business and Finance 115 at p.117.
[57] A. S. M. Irwin, J. Slay, R.C. Kim-Kwang, L. Lui, 'Money laundering and terrorism financing in virtual environments: a feasibility study' (2014) 17(1) JMLC 50.
[58] ibid at p.70.
[59] cf Robinson (n52).

laundered could be valued at 2-5% of global GDP.[60] The secretive nature of money laundering means reliable records are unavailable and varying estimates are produced; the United Nations Office on Drugs and Crime (UNODC) estimated 2.7% of global GDP,[61] equating to US$1.6 trillion, was being laundered in 2009,[62] which is the figure used by the FATF, but Unger found wide ranging estimates; [63] $45 and $280 billion by Reuter and Greenfield,[64] to $2.85 billion by Walker and Unger.[65] The case study jurisdictions each attempt to estimate money laundering domestically, the Australian Transaction Reports and Analysis Centre (AUSTRAC) estimates "*AUD200 billion is laundered in the Asia-Pacific region.*"[66] In the UK the Financial Conduct Authority (FCA) estimated in 2013 that "*£10billion of illicit funds*"[67] passes through the UK financial system, but this has since been revised upwards, in 2017 the National Crime Agency (NCA) believed a previous estimation of £39 billion to £90 billion to be a "significant underestimate".[68] The NCA was unable to provide a new estimate, but stated that there have been a number of money laundering operations it has identified,

[60] International Monetary Fund, 'Money Laundering: the Importance of International Countermeasures' <http://www.imf.org/external/np/speeches/1998/021098.htm> accessed 15 June 2015.
[61] Gross Domestic Product: "*an aggregate measure of production equal to the sum of the gross values added of all resident, institutional units engaged in production (plus any taxes, and minus any subsidies, on products not included in the value of their outputs).*" Organization for Economic Co-operation and Development, 'Gross Domestic Product' <http://stats.oecd.org/glossary/detail.asp?ID=1163> accessed 15 June 2015.
[62] United Nations Office on Drugs and Crime, 'Illicit Money: How Much is Out There?' <http://www.unodc.org/unodc/en/frontpage/2011/October/illicit-money_-how-much-is-out-there.html> accessed 15 June 2015.
[63] B. Unger, 'Can Money Laundering Decrease?' (2013) 41(5) Public Finance Review 658 at p.663.
[64] P. Reuter and V.A. Greenfield, 'Measuring Global Drug Markets: How Good Are the Numbers and Why Should We Care about Them?' (2001) 2(159) World Economics 73.
[65] J. Walker and B. Unger, 'Estimating Money Laundering: The Walker Gravity Model' (2009) 5(821) Review of Law and Economics 53.
[66] AUSTRAC, 'Introduction to Money Laundering' <https://michaelsmithnews.typepad.com/files/money-laundering.pdf> accessed 5 September 2019.
[67] Financial Conduct Authority, 'Anti-Money Laundering Annual Report 2012/13' <http://www.fca.org.uk/static/documents/anti-money-laundering-report.pdf> accessed 15 June 2015.
[68] National Crime Agency, 'National Strategic Assessment of Serious and Organised Crime 2017' <http://www.nationalcrimeagency.gov.uk/publications/807-national-strategic-assessment-of-serious-and-organised-crime-2017/file> accessed 05 September 2018.

each handling over £100 million. In the US, the Treasury believes "*about $300 billion is generated annually in illicit proceeds.*"[69] This research will not seek to estimate the amounts of money being laundered as such research will most likely produce yet another number, which will further confuse the issue as each of these estimations is likely to be inaccurate because each calculation has been produced using a different methodology. Furthermore estimations are usually based on different definitions of key terms; Unger and Busuioc identify that differing definitions of money laundering, the proceeds of different predicate offences being included, and the different statistical methods, lead to "*controversy between the purists, people who want to measure and model precisely, and the innovators – those who try to measure the immeasurable, even if they run the risk of being criticised*."[70] Despite the difficulties in establishing an accurate estimation of money laundering, the attempts are important in raising awareness of money laundering and justifying the allocation of resources to tackling it.

Contribution to Knowledge

This thesis identifies cryptocurrencies as a new mechanism for laundering money, in light of the characteristics of cryptocurrencies and the clear evidence cryptocurrencies are used for money laundering, as demonstrated by prosecutions. Chapters five, six, and seven demonstrate that the money laundering offences of each of the three case

[69] United States Treasury, 'National Money Laundering Risk Assessment' <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf> accessed 5 September 2019.
[70] cf Unger (n55) at p.32.

studies can be committed using cryptocurrencies, and that the existing preventative measures are not compatible with cryptocurrencies.

2.2.4. Cryptocurrency Money Laundering

Convictions in the UK and US demonstrate that money laundering is taking place using cryptocurrencies. As with conventional money laundering techniques, accurate statistics are not available, but in 2018, Europol estimated that "*3-4% of the £100bn in illicit proceeds in Europe are laundered through cryptocurrencies*."[71] Cryptocurrencies have been central to a number of high profile crimes, such as the collapse of the Mt Gox exchange in February 2014,[72] and been utilised at the preferred payment method for ransomware demands, such as in the 'WannaCry' cyber-attack on the NHS in May 2017.[73] Bitcoin was the currency of choice for the infamous illicit online market place Silk Road,[74] and its founder Ross Ulbricht is serving a life sentence in the US.[75] The number of cases in the UK remains low, but it is clear that cryptocurrencies are being utilised to launder the proceeds of crime. Laundered cryptocurrency has also been confiscated from convicted criminals, but successful confiscation has largely been reliant on circumstantial luck; a police force was able to freeze the cryptocurrency

[71] BBC News, 'Criminals hide 'billions' in crypto-cash – Europol' (12 February 2018) <https://www.bbc.co.uk/news/technology-43025787> accessed 08 October 2019.
[72] BBC News, 'MtGox bitcoin exchange files for bankruptcy' (28 February 2014) <https://www.bbc.co.uk/news/technology-25233230> accessed 07 October 2019.
[73] BBC News, 'NHS cyber-attack: GPs and hospitals hit by ransomware' (13 May 2017) <https://www.bbc.co.uk/news/health-39899646> accessed 097 October 2019.
[74] J. Lane, 'Bitcoin, Silk Road and the Need for a New Approach to Virtual Currency Regulation' (2013-2014) 8 Charleston Law Review 511 at 513.
[75] Department of Justice, U.S. Attorney's Office Southern District of New York, 'Ross Ulbricht, A/K/A "Dread Pirate Roberts," Sentenced in Manhattan Federal Court To Life In Prison' (Manhattan, New York, 29 May 2015) <https://www.justice.gov/usao-sdny/pr/ross-ulbricht-aka-dread-pirate-roberts-sentenced-manhattan-federal-court-life-prison> accessed 05 September 2019.

assets of an individual having caught them with their "*fingers on the keyboard*",[76] such as in the case of West, and in the case of Teresko police gained access to the defendants Bitcoin wallet through finding access details on paper during a search of his address.[77] A likely method of seizing illicit cryptocurrency, which was also used against West, is to use a court order requiring the convicted individual to give up the cryptocurrency or face further jail time.[78] Once the cryptocurrency is confiscated there are currently two options for authorities wishing to convert the currency; they can either use a cryptocurrency exchange or sell the cryptocurrency at public auction, Hall observes that the US approach is use public actions, whereas Dutch authorities use exchanges.[79]

Irwin *et al*. found the anonymity of cryptocurrencies as appealing to money launderers,[80] Stokes considers the "*emergence of new and alternative payment technologies and products pose a genuine money laundering risk*"[81] and that more research is required into cryptocurrencies.[82] Houben argues that "*national level is probably not the best level to adequately address*"[83] the risks of cryptocurrencies, and that "*European level is more appropriate, preferably in the execution of a global approach, as crypto activity is also not limited by the European border*."[84] The issue of

[76] M. Busby, 'Bitcoin worth £900,000 seized from hacker to compensate victims' The Guardian (London, 23 August 2019).
[77] J Hall, 'Restraint orders: R. v Teresko (Sergejs) Kingston Crown Court: HH Judge Lodder QC: unreported 11 October 2017' (2018) 1 CLR 81.
[78] ibid.
[79] cf Hall (n79) at 82.
[80] cf Irwin *et al.* (n57).
[81] R. Stokes, 'Virtual Money Laundering: The Case of Bitcoin and the Linden Dollar' (2012) 21(3) Information and Communications Technology Law 221 at 231.
[82] ibid at 232.
[83] R. Houben, 'Cryptocurrencies from a money laundering and tax evasion perspective' (2019) 30(5) International Company and Commercial Law Review 261 at 268.
[84] ibid at 268.

cryptocurrencies and money laundering has not been ignored by academia, but this research considers international and national efforts to bring cryptocurrencies within the regulatory perimeter, and observes gaps within that regulation.

Contribution to knowledge

This thesis argues that the existing money laundering offences are sufficient to cover the use of cryptocurrencies to launder money. The UK money laundering offences do not need reform for the purpose of applying to cryptocurrencies, the drafting of the offences is wide enough to obtain convictions, as demonstrated by the prosecutions of Teresko,[85] White,[86] and West.[87] Where the UK law is unclear is in relation to converting seized cryptocurrency, in the Teresko case an exchange was used,[88] but in 2019 a UK police force used the public auction method for the first time.[89] It is recommended that the UK processes cryptocurrency seizures faster in order to realise the value of the confiscated goods at the correct value, however it is currently unclear which method of conversion is preferred.

[85] Crown Prosecution Service, 'More than £1.2million of Bitcoin seized from drug dealer' (19 July 2018) <https://www.cps.gov.uk/south-east/news/more-ps12-million-bitcoin-seized-drug-dealer> accessed 11 September 2019.
[86] BBC News, 'Liverpool 'dropout' jailed for Silk Road dark web site' (12 April 2019) <https://www.bbc.co.uk/news/uk-england-merseyside-47913780> accessed 11 September 2019 and National Crime Agency, 'Student behind $100m dark web site jailed for 5 years 4 months' (12 April 2019) <https://www.nationalcrimeagency.gov.uk/news/student-behind-100m-dark-web-site-jailed-for-5-years-4-months?highlight=WyJiaXRjb2luIiwiYml0Y29pbnMiXQ==> accessed 11 September 2019.
[87] BBC News, 'Prolific Sheerness hacker ordered to pay back £922k' (23 August 2019) <https://www.bbc.co.uk/news/uk-england-kent-49450676> accessed 24 September 2019.
[88] cf Hall (n79) at 82.
[89] Wilsons Auctions, '£500k of bitcoin seized from UK criminal to be auctioned, with no reserve!' (19 September 2019) <https://www.wilsonsauctions.com/news/500k-of-bitcoin-seized-from-uk-criminal-to-be-auctioned-with-no-reserve/> accessed 30 September 2019.

2.2.5. Anti-Money Laundering Legislation

As will be seen in chapter four, attempts to combat money laundering date back to the 1960s, with the United Nations Single Convention on Narcotic Drugs 1961.[90] The development of anti-money laundering regulation will be viewed in a timeline in chapter four to demonstrate the evolution of such regulation and attempt to predict future developments. As well as international efforts at combatting money laundering, domestic legislation from each of the case study jurisdictions will demonstrate the development of AML measures. Each of the case study jurisdictions have been attempting to combat money laundering for decades The US and the UK both made money laundering a criminal offence in 1986; with the Money Laundering Control Act 1986,[91] and the Drug Trafficking Offences Act 1986[92] respectively. Australia implemented its first money laundering offences in 1987; through the Proceeds of Crime Act 1987.[93] This research will track the development of international and domestic money laundering legislation, in light of this the applicability of these provisions to cryptocurrencies can be assessed, and the likelihood of legislative action in relation to cryptocurrencies may be considered. In order to achieve this, it is best to take each area in turn, starting with the international approach, and then considering each of the case studies, as each of the case study jurisdictions. This thesis highlights a changing of the guard in the setting of international best practice, with the FATF and the EU taking over from the UN.

[90] Single Convention on Narcotic Drugs (adopted 30 March 1961, entered into force 13 December 1964) 520 UNTS 151 (Single Convention on Narcotic Drugs).
[91] Money Laundering Control Act Pub. L. 99-570.
[92] Drug Trafficking Offences Act 1986.
[93] Proceeds of Crime Act 1987.

International Anti-Money Laundering Regulation

Money laundering is recognised as an international issue, and cryptocurrencies intangible nature means national borders do not apply, thus it is necessary to analyse the international legal approach to money laundering. The principal literature in international law is produced by the United Nations (UN) and the principal AML laws of the UN can be found in the UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances[94] (Vienna Convention 1988), and the UN Convention against Transnational Organised Crime[95] (Palermo Convention 2000). The Vienna Convention 1988 remains focussed on drug related crime, as Ryder opines, the "*Vienna Convention was limited to the laundering of the proceeds of crime from the manufacturing and sale of narcotics.*"[96] The Palermo Convention 2001 marked an important change in the UN approach, extending money laundering offences to include the proceeds of "*serious crimes.*"[97] Zagaris cites a key aim of the Palermo Convention 2000 was to strengthen the "*power of governments to combat serious crimes by providing a basis for stronger common action against money laundering through synchronized national laws.*"[98] In 2003, the UN adopted the UN Convention on Corruption.[99] Carr praises the comprehensiveness of the Convention,[100] arguing it is "*very difficult to fault*",[101] but notes that the biggest weakness with the Convention,

[94] Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (adopted 20 December 1988, entered into force 11 November 1990) UNTS 1582 (Vienna Convention 1988).
[95] Convention against Transnational Organised Crime (adopted 15 November 2000, entered into force 29 September 2003) UNTS 2225 (Palermo Convention 2000).
[96] N. Ryder, *Financial Crime in the 21st Century: Law and Policy* (Edward Elgar, Cheltenham, 2011) at p.15.
[97] Convention against Transnational Organised Crime (adopted 15 November 2000, entered into force 29 September 2003) UNTS 2225 (Palermo Convention 2000) art.6.
[98] B. Zagaris, *International White Collar Crime: Cases and Materials* (New York: Cambridge University Press, 2010) at p.64.
[99] Convention against Corruption (adopted 21 October 2003, entered into force 14 December 2005) 43 ILM 37.
[100] I. Carr, 'Fighting corruption through the United Nations Convention on Corruption 2003: a global solution to a global problem?' (2005) 11(1) Int. T.L.R. 24 at p.29.
[101] ibid.

which is true of most UN measures, is that international legislation alone is not the solution. Carr does not criticise the convention itself but the will of countries to utilise it, in "*countries where politicians turn a blind eye to corruption to ensure or maintain their status, there is unlikely to be legislative interference*" on corrupt practices. The adoption of an all crimes approach to money laundering offences is a step forward from the UN, and the Palermo Convention was a key step in the decoupling of money laundering from drug trafficking. While the UK is a signatory to UN Convention relating to money laundering, it goes further than its obligations, as it is also compliant with EU and FATF measures, which are more prescriptive than UN Conventions are able to be.

The EU also attempts to harmonise approaches to money laundering, the most recent legislation is the 5th Anti-Money Laundering Directive,[102] which must be adopted by EU Member States by 10 January 2020, replacing the 4th Anti-Money Laundering Directive.[103] It is observed in chapter four that the EU has reacted to the issue of money laundering later than the UN, but the 5th Anti-Money Laundering Directive moves the EU ahead of the UN in advancing AML measures. The 5th Anti-Money Laundering

[102] Directive 2018/843/EU of The European Parliament And Of The Council of 30 May 2018 amending Directive 2015/849/EU on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU [2018] OJ L. 156/43.

[103] Directive 2015/849/EU 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 [2015] OJ L.141/73.

Directive applies AML legislation to cryptocurrency exchanges,[104] which will bring some cryptocurrency transactions under AML regulation.

At the time of this research, UK is still a member of the EU, and this research considers the influence of EU legislation on the legislation of the UK. This thesis will not focus on the UK's exit from the EU, this is for a number of reasons, firstly it has not yet happened, and as with many things relating to leaving the EU, there is little to no direction given by the UK government. Secondly, as will be seen in chapter four, in relation to money laundering, the behaviour of the UK since 1970 indicates that very little is likely to change as the UK has been an early adopter of international best practice. Thirdly, and finally, as the UK is a member of the FATF, and it is seen in chapter four that the EU and the FATF prescribe very similar approaches to money laundering, the UK will continue to be compliant with EU AML legislation, whether it is a member of the EU or not.

In addition to the legal instruments, the guidance of the FATF is influential on the AML approaches of the three case study jurisdictions as they are all members of FATF. Alexander observes that despite the most recent set of 40 Recommendations[105] being "*non-binding in a legal sense, some of the 40 Recommendations have become*

[104] European Commission, 'Strengthened EU rules to prevent money laundering and terrorism financing' <http://ec.europa.eu/newsroom/just/document.cfm?action=display&doc_id=48935> accessed 05 September 2018 and European Commission, 'Questions and Answers: Anti-money Laundering Directive' <http://europa.eu/rapid/press-release_MEMO-16-2381_en.htm> accessed 16 September 2019.
[105] Financial Action Task Force, 'The FATF Recommendations' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf> accessed 04 September 2019.

mandatory."[106] The FATF provide the most widely used guidance on cryptocurrencies and the money laundering threats they may pose,[107] the advice of the FATF is utilised by the UN in its approach to cryptocurrencies.[108] The guidance of the FATF will be considered, and how the influence of the FATF Recommendations may be utilised in developing a consistent approach to preventing money laundering through cryptocurrencies.

Domestic Anti-Money Laundering Legislation

The domestic legislation of each of the case study jurisdictions form the primary sources of law, the legislation is considered in two ways, firstly can the relevant money laundering offences be committed using cryptocurrencies, and secondly, do the AML provisions apply to cryptocurrency transactions; either transactions within cryptocurrency networks, or transactions which interact with fiat currencies, involving the purchasing and selling of cryptocurrencies.

UK

Money laundering has been a criminal offence in the UK since the Drug Trafficking Offences Act 1986[109] was passed, and chapter four tracks the development of

[106] K Alexander, 'The International Anti-Money-Laundering Regime: The Role of the Financial Action Task Force' (2001) 4(3) JMLC 231 at p.241
[107] Financial Action Task Force, 'Virtual Currencies – Key Definitions And Potential AML/CFT Risks' <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 27th November 2014.
[108] United Nations Office on Drugs and Crime, 'Basic Manual on the Detection and Investigation of the Laundering of Crime Proceeds Using Virtual Currencies' <http://www.imolin.org/pdf/UNODC_VirtualCurrencies_final_EN_Print.pdf> accessed 01 September 2019.
[109] Drug Trafficking Offences Act 1986.

legislation up to the present day. The evolution of legislation in the UK will be seen to exceed the UN conventions and, as with the 'failure to disclose' offence of the Drug Trafficking Offences Act 1986,[110] the UK has been world leading. The UK decoupled money laundering from drug offences with the Criminal Justice Act 1993,[111] amending the Criminal Justice Act 1988,[112] and widening money laundering offences to the proceeds of all crimes, not just drugs.[113] In chapter four, this thesis argues that separating money laundering and drug offences is a positive step; cleaning the proceeds of illegal drug sales is money laundering, but not all illicit money comes from illegal drug sales. By the same argument, this thesis argues that while the UK has been world leading in combatting money laundering, it has also been at the forefront of taking money laundering legislation backwards. By confusing money laundering and terrorist financing through the Terrorism Act 2000,[114] which introduced the concept of laundering terrorist property, the UK has recoupled money laundering to a distinctly different offence. Alexander distinguishes from the common concept of money laundering from terrorist funding, in terrorist financing "*the focus is not on the where the property has come from but where it is destined: its ultimate purpose,*"[115] which differs from money laundering which "*concerns property which is derived from crime and efforts to combat it therefore focus on its origin.*"[116] Coupling money laundering and terrorism financing is confusing as the processes are different; the processes operate in opposite directions as Alexander describes, and so use different

[110] ibid s.24.
[111] Criminal Justice Act 1993.
[112] Criminal Justice Act 1988.
[113] Criminal Justice Act 1993 ss.29-32, Adding ss.93A-D to the Criminal Justice Act 1988.
[114] Terrorism Act 2000.
[115] R. Alexander, *Insider Dealing and Money Laundering in the EU: Law and Regulation* (Aldershot: Ashgate, 2007) at p.173.
[116] ibid.

techniques, and while there may be some common ground, the two issues require separate approaches.

The current money laundering offences of the UK are found within the Part 7 of the Proceeds of Crime Act.[117] The three main offences are concealing,[118] arrangements,[119] and acquisition, use and possession.[120] It is also an offence to fail to disclose knowledge of money laundering,[121] or tip off a person suspected of money laundering.[122] The preventative measures are found in the Money Laundering Regulations 2017.[123] The applicability of the Proceeds of Crime Act 2002 and the Money Laundering Regulations 2017 will be considered in relation to cryptocurrencies. The most recent piece of legislation, the Criminal Finances Act 2017[124] is acknowledged, but does not add any provisions relevant to cryptocurrencies.

US

The US was the first country to criminalise money laundering, with the Money Laundering Control Act 1986.[125] The US AML legislation is split into two categories by Tomas and Roppolo;[126] firstly, criminal law, and secondly, the implementation of

[117] Proceeds of Crime Act 2002, Part 7.
[118] ibid s.327.
[119] ibid s.328.
[120] ibid s.329.
[121] ibid s.332.
[122] ibid s.333.
[123] Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.
[124] Criminal Finances Act 2017.
[125] Money Laundering Control Act Pub. L. 99-570.
[126] J. P. Thomas and W. V. Roppolo, 'United States of America' in A. Srivastava, M. Simpson and N. Moffat, *International Guide to Money Laundering Law and Practice* (Bloomsbury, 2013) at 41.20.

regulations under the Bank Secrecy Act[127] (BSA 1970). The BSA 1970 is still the principal AML legislation of the US, but it has had numerous amendments, as can be seen in chapter four. The Annunzio-Wylie Money Laundering Act 1992[128] amended the BSA 1970 by introducing suspicious activity reporting requirements for financial institutions,[129] these were extended by the Money Laundering Suppression Act 1994.[130] More changes to the BSA 1970 came through the Uniting and Strengthening America by Providing Appropriate Tools to Restrict, Intercept and Obstruct Terrorism Act 2001[131] (PATRIOT Act 2001), which extended reporting requirements to cover terrorist financing. The PATRIOT Act 2001 also gave money laundering legislation extra-territorial effect.[132] The amended version of the BSA 1970 remains the principal source of US AML law and is considered in detail in chapter six. As with the UK legislation, 21st century developments have intertwined money laundering with terrorist financing. The incorporation of counter terrorist financing legislation has led to the term 'reverse money laundering', defined by Cassella as the "*process of conducting financial transactions with clean money for the purpose of concealing or disguising the future use of that money to commit a criminal act.*"[133] The Cassella concept of reverse money laundering is rejected by this thesis, as it could apply to any organised crime, it is not specific to terrorist financing. Furthermore, as established in relation to the UK, the confusion of money laundering and terrorist financing is unhelpful as the processes and behaviours, are very different. This research is focussed on the potential money

[127] Bank Secrecy Act, Pub. L. 91–508.
[128] Annunzio–Wylie Money Laundering Act 1992.
[129] ibid §1571.
[130] Money Laundering Suppression Act 1994.
[131] Uniting and Strengthening America by Providing Appropriate Tools to Restrict, Intercept and Obstruct Terrorism Act 2001.
[132] cf Ryder (n50) at p.44.
[133] S. D. Cassella, 'Reverse money laundering (2003) 7(1) Journal of Money Laundering 92 at pp.92-93.

laundering risks posed by cryptocurrencies. The analysis of the US legislation will focus on money laundering offences within Title 18 of the United State Code §§1956-1957;[134] introduced by the Money Laundering Control Act 1986,[135] and on the present version of the BSA 1970, incorporating the most recent amendments by the PATRIOT Act 2001. Cryptocurrencies will be considered in relation to the relevant legislation, analysing the applicability of the law, and where relevant suggesting reform.

Australia

Australia implemented its first money laundering offences through the Proceeds of Crime Act 1987.[136] The development of AML legislation in Australia has followed a similar pattern to the US and the UK, particularly the most recent money laundering legislation, the Anti-Money Laundering and Counter-Terrorism Financing Act 2006.[137] The 2006 Act, like the US and the UK, entwines money laundering and terrorist financing. The primary source of money laundering offences in Australia is the Criminal Code Act 1995,[138] which codifies all federal offences. Subdivision 400.3-9[139] will be the most relevant division of the Criminal Code for this thesis as this is where the money laundering offences are contained, of which there are 19. This is a much larger number of offences than the UK and the US; this is because money laundering offences are arranged very differently in Australia. The US and UK have a small number of offences, and sentencing provisions allow for the appropriate sentence to be imposed, whereas

[134] 18 USC §1956-1957.
[135] Pub. L. No. 99-570, 100 Stat. 3207-18.
[136] Proceeds of Crime Act 1987.
[137] Anti-Money Laundering and Counter-Terrorism Financing Act 2006.
[138] Criminal Code Act 1995.
[139] ibid Subdivision 400.3-9.

in Australia the same three offences are repeated 6 times to prescribe the sentencing guidelines depending on the value of money or property involved.

The preventative measures of Australia are contained in the Anti-Money Laundering and Counter Terrorist Financing Act 2006 (AML/CTF Act 2006),[140] of which the key measures are Threshold Transaction Reports (TTRs),[141] Suspicious Activity Reports (SARs),[142] and due diligence requirements.[143] Chapter seven demonstrates that Australia follows the same broad split in approaching money laundering as the US and the UK; criminalising money laundering, as required by the UN treaties and the FATF, and requiring financial institutions to adhere to preventative measures.

Contribution to Knowledge

This thesis identifies themes in the development of AML legislation since its inception in the 1960s. Money laundering is tracked from its origins as secondary crime linked to the drugs trade, through to it being accepted as a standalone offence, and then the reverse step of conflating terrorist financing with money laundering. It is observed in this thesis that the role of the UN has receded, giving way to the FATF and the EU in developing current international best practice, and that the FATF and EU have become increasingly prescriptive through their Recommendations and legislation respectively. With regard to national AML regulation, the UK, the US, and Australia have been early adopters of AML regulation, they have been quick to implement UN conventions and

[140] Anti-Money Laundering and Counter-Terrorism Financing Act 2006.
[141] ibid Part 3 s.43.
[142] ibid Part 3 s.41.
[143] ibid Parts 2 and 3.

subsequently the Recommendations of the FATF, the UK has also implemented EU AML directives. With regard to cryptocurrency regulation, Australia and the US are ahead of the UK, demonstrating that the regulation of cryptocurrency service providers is possible, and that adapting an AML approach to include cryptocurrency service providers can be achieved in a timely fashion. Both jurisdictions have widened their AML regulation and require cryptocurrency service providers to adhere to customer due diligence and reporting requirements, this shows that cryptocurrency service providers can be regulated in the same way as traditional financial institutions. Though the end result has been the same in both jurisdictions, the development of their AML regulation has been instigated differently; in the US, FinCEN has taken the lead in a regulatory led widening of the regulatory perimeter, compared to Australia where Parliament has delivered a legislator led widening of the regulatory perimeter. The UK will follow a legislator led approach by virtue of implementing the 5th Anti-Money Laundering Directive. This thesis identifies that while international guidance and domestic measures are a positive step, they fail to recognise the wealth of data available through public ledgers, which needs to be addressed through utilising technology. Bitcoin's blockchain can be viewed freely online,[144] and there are numerous blockchain API tools available to enable analysis of the blockchain.[145] At present, it is not clear if the financial intelligence available through the blockchain is being analysed for AML purpose, but it is a valuable resource that needs to be utilised. Currently a money laundering investigation will only begin when suspicion is aroused, but by automating analysis of the blockchain, money laundering investigations could

[144] Blockchain Luxembourg, 'Block Explorer' <https://www.blockchain.com/explorer> accessed 30 September 2019.
[145] Examples can be found at Blockchain Luxembourg, 'Bitcoin Developer APIs' <https://www.blockchain.com/api> accessed 26 September 2019.

get a head start and patterns of transactions could be identified. Blockchain analysis should be the responsibility of the FIU as financial intelligence will be produced.

2.3. Placing the thesis

The relationship between cryptocurrencies and money laundering is an under-researched area. Some attempts have been made to consider the implications of money laundering and virtual currencies, such as that of Irwin *et al*.,[146] but this research specifically seeks to consider whether the current laws apply to cryptocurrencies and whether any proposed reforms will address the gap in the law, or whether a new approach is required. This thesis analyses money laundering in isolation of terrorist financing, this is justified based on the differences between money laundering and terrorist financing. Principally, as Alexander observes, the focus of the activity in terrorist financing is "*where it is destined: its ultimate purpose,*"[147] whereas money laundering is the opposite, it "*concerns property which is derived from crime and efforts to combat it therefore focus on its origin.*"[148] Cassella also notes this difference, terrorist financing is the "*process of conducting financial transactions with clean money for the purpose of concealing or disguising the future use of that money to commit a criminal act,*"[149] therefore, while there may be overlaps in the appeal of cryptocurrencies for terrorist financing, this will require separate research.

[146] cf Irwin *et al.* (n57).
[147] cf Alexander (n115) at p.173.
[148] ibid.
[149] cf Cassella (n133) pp.92-93.

2.3.1. Regulatory Gaps

This thesis exposes the weaknesses of AML legislation targeted at cryptocurrencies. It demonstrates that the money laundering offences of each of the three case studies can be committed using cryptocurrencies, but also that the existing preventative measures are not compatible with cryptocurrencies. The prevailing approach from the FATF is to recommend that cryptocurrencies should be regulated under existing AML measures, with the emphasis being placed in the intersections between cryptocurrencies and the traditional financial system.[150] This approach leaves a clear gap in the regulation of cryptocurrencies; the speed and ease of transactions within cryptocurrency networks means that the transactions with the traditional financial system will be too far along the money laundering process to appear suspicious. This research demonstrates this gap in regulation in each of the case study jurisdictions and in the international guidance.

This research has taken place at a time of political uncertainty in all three jurisdictions, as each jurisdiction has held divisive general elections. In July 2016, Australia retained the same leading coalition, but with a bare majority of 1 seat,[151] and the same slim majority was retained in the 2019 election.[152] The US election of November 2016 resulted in a change of government and a new President,[153] and the UK elections of

[150] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 07 October 2019.
[151] Australian Broadcasting Corporation, 'Federal Election 2016' <http://www.abc.net.au/news/federal-election-2016/results/> accessed 27 September 2019.
[152] The Guardian, 'Australian election 2019: live results' (18 May 2019) <https://www.theguardian.com/australia-news/ng-interactive/2019/may/18/live-results-for-the-2019-australian-election-track-the-votes> accessed 09 October 2019.
[153] BBC News, 'US Election 2016' <http://www.bbc.co.uk/news/election/us2016/results> accessed 27 September 2019.

2015[154] and 2017[155] which have seen the UK move from coalition, to a small Conservative majority government and, at the time of writing, a fragile Conservative minority government seeking another general election.[156] Government change hampers the passing of legislation, the legislating house of the country is dissolved while campaigning takes place, and a period of time after the election can be spent formulating a government.[157] Elections further hamper the passing of AML legislation as elections are rarely fought on this issue; money laundering does not have immediately identifiable consequences as will be seen in chapter four, Unger notes that there are no direct victims of money laundering, instead "*there are always secondary victims such as family, friends, acquaintances, and society at large.*"[158] While recent elections have shown that politicians are not aware exactly what the electorate want, it is clearly a lot easier to campaign on more tangible issues, as such manifestos are silent on money laundering and cryptocurrencies, and instead much more focussed on taxes, security and the economy. As a result of elections, the legislature will be focussed on proposals which stem from the manifestos and election campaigns, which is likely to push back any proposed AML legislation. This thesis analyses the law of the three jurisdictions and considers the reform that can take place once settled governments are in place.

[154] BBC News, 'Election 2015' <http://www.bbc.co.uk/news/election/2015/results> accessed 27 September 2019.
[155] BBC News, 'Election 2017' <http://www.bbc.co.uk/news/election/2017/results> accessed 27 September 2019.
[156] BBC News, 'Brexit: Boris Johnson's second attempt to trigger election fails' (10 September 2019) <https://www.bbc.co.uk/news/uk-politics-49630094> accessed 09 October 2019.
[157] As demonstrated in 2017 in the UK: BBC News, 'Theresa May and the DUP deal: What you need to know' (26 June 2017) <https://www.bbc.co.uk/news/election-2017-40245514> accessed 09 October 2019.
[158] B. Unger & D. v.d. Linde, *Research Handbook On Money Laundering* (Edward Elgar, Cheltenham, 2013) at p.20.

There is limited academic comment regarding the money laundering risks of cryptocurrencies; those who have considered the money laundering threat have found the threat to be minimal due to the volatility of the most prominent cryptocurrency, Bitcoin, and the relatively low value of Linden Dollars, the currency of Second Life. Irwin *et al*. viewed the anonymity of cryptocurrencies as appealing to money launderers,[159] but focussed on virtual worlds rather than just cryptocurrencies. Stokes considers the "*emergence of new and alternative payment technologies and products pose a genuine money laundering risk*"[160] and that more research is required into cryptocurrencies.[161] Houben argues that "*national level is probably not the best level to adequately address*"[162] the risks of cryptocurrencies, and that "*European level is more appropriate, preferably in the execution of a global approach, as crypto activity is also not limited by the European border*."[163] This thesis will contribute to knowledge in understanding cryptocurrencies and analyse whether cryptocurrencies can be defined as money, as this is unclear. The most important contribution from this thesis will be in analysing and contrasting the global and domestic reactions to cryptocurrencies and proposing reform in the UK, but that will also be applicable internationally.

2.3.2. Relevant Authorities and Organisations

In identifying the relevant authorities and organisations to this thesis, the research can be split into two broad areas; domestic and international. In each of the case study jurisdictions, this thesis will focus on the actions of the governments, legislators and

[159] cf Irwin *et al*. (n57)
[160] cf Stokes (n81) at 231.
[161] cf Stokes (n81) at 232.
[162] cf Houben (n83) at 268.
[163] cf Houben (n83) at 268.

regulators of each of the case study jurisdictions. The focus of this thesis is on the application of AML regulation, as such the Financial Intelligence Unit (FIU) in each jurisdiction will be identified and its response to cryptocurrencies will be analysed. The UK FIU is the National Crime Agency, in the US it is the Financial Crime Enforcement Network, and in Australia it is the Australian Transaction Reports and Analysis Centre. In the UK the responsibility for regulation rests with Financial Conduct Authority, rather than the FIU as it does in the US and Australia, therefore the Financial Conduct Authority's response to cryptocurrencies will also be analysed.

As chapter four demonstrates, money laundering attracts the attention of prominent international organisations, most notably the UN, the FATF, and the EU. Cryptocurrencies and money laundering are both international issues and therefore the response of the international community must be considered; the constraints of this research mean that the priority will be placed on the major international organisations and their influences on the case study jurisdictions.

2.4. Literature Review Summary

This thesis seeks to build on the academic debate regarding cryptocurrencies, in situating the research within the existing literature it must be made clear from the outset that the focus will be placed on the money laundering risks of cryptocurrencies; where relevant the research will be distinguished from terrorist financing risks. The aims of the research are to assess the applicability of both money laundering offences and AML provisions to cryptocurrencies; the relevant laws of three case study jurisdictions will be analysed, and the influence of international organisations will be

considered. The primary sources will be the legislation of the case study jurisdictions, and the relevant international organisations will be considered based on their links to the three jurisdictions; all are members of the UN and the FATF, and, at the time of this research, the UK is still implementing EU legislation.

2.5. Methodology

This thesis adopts a socio-legal methodology, this methodology does not exist in isolation; it includes traditional doctrinal research but recognises the need to consider wider sources than legal text.

Doctrinal research has been defined as providing "*a systematic exposition of the rules governing a particular legal category, analyses the relationship between rules, explains areas of difficulty and, perhaps, predicts future developments*."[164] Mann describes it as a "*synthesis of various rules, principles, norms, interpretive guidelines and values. It explains, makes coherent or justifies a segment of the law as part of a larger system of law*."[165] Van Hoecke has described the doctrinal approach as a hermeneutic discipline[166] comparing it to a study of literature, the principal difference being that doctrinal research involves "*interpreting texts and arguing about a choice among diverging interpretations*."[167] The principle strength of the doctrinal methodology is the focus on primary materials; the essence of the approach is to

[164] D. Pearce, E. Campbell and D. Harding ('Pearce Committee'), Australian Law Schools: A Discipline Assessment for the Commonwealth Tertiary Education Commission (Australian Government Publishing Service, 1987) p.7.
[165] T. Mann (ed), Australian Law Dictionary (Oxford University Press 2010) at p.97.
[166] M. van Hoecke, 'Legal Doctrine: Which Method(s) What Kind of Discipline?' in M. van Hoecke, Methodologies of Legal Research (Bloomsbury, 2011) p.4.
[167] ibid.

assess the law, through statutes and case law. This focus on legal texts also points towards to be biggest criticism of doctrinal research; it is limited to specific legal questions which may only be answered by analysing legal text, this restricts legal research as it does not allow for the social, political or economic impact of the law to be considered. While this method of legal research will be invaluable in this research, it is also limited, as stated, the definition of the doctrinal approach highlights the most prevalent criticism against it, it is merely descriptive, it is argued that socio-legal research has achieved more valuable knowledge because of its considerations for how and why the law exists as it does and how it can be reformed.[168]

Adopting a socio-legal methodology addresses the principal weakness of doctrinal research. To discount socio-legal research would risk producing a very narrow thesis, as it would involve ignoring issues identified by other methods of research used within this research, and as such valuable considerations would be missed; the value of the research would be reduced if it was solely doctrinal.

Defining the parameters of socio-legal research has proven difficult as it encompasses a broad spectrum. The most effective way of establishing these parameters is to distinguish socio-legal research from the traditional doctrinal approach to legal research. Whereas doctrinal research limits a researcher to legal text, the socio-legal methodology allows a researcher to "*cast their net wider than law reports, statutes and Hansard, and academic commentaries upon doctrinal sources. Instead it requires*

[168] R. Cotterrell, Law's Community (OUP 1995).

researchers to gather 'data wherever appropriate to the problem, by using whatever methods are most likely to generate such data."[169] This may be applied to the research at hand; it is accepted from the outset that there will be limited primary legal resources directly pertaining to cryptocurrencies due to cryptocurrencies being a relatively new phenomenon, and were a purely doctrinal approach adopted the available sources would be unlikely to be sufficient for a thesis. By utilising sources from other disciplines, the wealth of research in this area may be analysed and the potential legal impacts may be considered.

2.5.1. Methods employed for the research.

Under the socio-legal methodology, this thesis will employ a case study approach in order to draw comparisons between the three selected jurisdictions. As has been demonstrated already, the socio-legal methodology is a very broad one; therefore, it is important to consider the specific methods that will be adopted under the umbrella of the socio-legal research. Case studies are used as a method in this research, but case studies will also require methods within them, and do no stand alone as a research method.

Case studies

Three case study jurisdictions have been selected; Australia, the UK and the US. The selection of jurisdictions has been limited to three as it would not be viable to attempt to compare too many jurisdictions. The United States has been selected as it is a world

[169] A. Bradshaw, Sense and Sensibility: Debates and Developments in Socio-Legal Research Methods' in P Thomas (ed) Socio-Legal Studies (Aldershot, Ashgate-Dartmouth, 1997) p.99.

leader in adopting AML measures; it was the first country to criminalise money laundering,[170] it has an influential role in directing the international agenda with the biggest economy[171] and housing the UN headquarters in New York,[172] and it is a founding member of the Financial Action Task Force.[173] Australia has been selected as it is also an early adopter of AML initiatives; Australia criminalised money laundering within a year of the US doing so,[174] it is also a founding member of the FATF,[175] and one of the first countries to develop legislation which specifically addresses cryptocurrencies.[176] This research is conducted in the UK, and the UK has historically been an early adopter of AML measures, criminalising money laundering in the same year as the US in 1986,[177] and it is a founder member of the FATF.[178] Despite the previous proactivity of the UK, this research identifies the UK as lagging behind in its reaction to the development of cryptocurrencies.[179] The UK case study will analyse the UK and seek to recommend reform based on the conclusions of the US and Australia case studies. The three jurisdictions have been selected in part due to their similarities; as identified, all three jurisdictions are founding members of the

[170] In 1986 through the Money Laundering Control Act Pub. L. 99-570.
[171] Based on Gross Domestic Product: World Bank 'GDP (current US$)' (2018) <https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?most_recent_value_desc=true&view=chart> accessed 29 April 2020.
[172] United Nations, 'Secretariat' <https://www.un.org/en/sections/about-un/secretariat/index.html> accessed 29 April 2020.
[173] Financial Action Task Force, 'History of the FATF' <http://www.fatf-gafi.org/about/historyofthefatf/> accessed 29 April 2020.
[174] Proceeds of Crime Act 1987.
[175] Australian Government: Department of Home Affairs, 'Crime Prevention – Financial Action Task Force' (17 March 2020) <https://www.homeaffairs.gov.au/about-us/our-portfolios/criminal-justice/crime-prevention/financial-action-task-force> accessed 29 April 2020.
[176] The terms "*registered digital currency exchange provider*" and "*registrable digital currency exchange service*" were added to the list of regulated activities within the Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.5.
[177] Drug Trafficking Offences Act 1986.
[178] [178] Financial Action Task Force, 'History of the FATF' <http://www.fatf-gafi.org/about/historyofthefatf/> accessed 29 April 2020.
[179] Until the implementation of the 5th Anti-Money Laundering Directive in January 2020, the UK had not enacted any reforms to address cryptocurrencies. Money Laundering and Terrorist Financing (Amendment) Regulations 2019.

FATF, they are all considered developed countries, and they can all be seen to be early adopters of AML measures.[180] There are also differences between each of the jurisdictions, the US and Australia are federal countries whereas the UK is not, the analysis of the US and Australia will focus on national legislation, it is not possible to cover state or territory legislation within this thesis.

The UK's historical membership in the EU provides the opportunity to assess EU law, which may be described as supranational law, completing tripartite assessment of money laundering law; national, international and supranational. As developed countries, and members of the FATF the three jurisdictions may be expected to present strong AML controls, but in analysing cryptocurrencies, the research will explore the effect of such controls on vehicles that the jurisdictions have little influence over.

The socio-legal methodology will be applied to the case studies; therefore, the case studies, consistent with the methodology of the thesis, will involve doctrinal analysis, but also consider non-legal sources. In order to define and understand the position of the law currently in force it will be necessary to undertake a comprehensive assessment of the primary sources of law in the UK the US and Australia; these sources will be case law and legislation. This element of the case study research will be doctrinal, also referred to as 'black-letter' approach.[181] As stated already, the doctrinal approach seeks to identify and explain the law using all its forms. Based on

[180] See chapter four at 4.7.
[181] J. Mason and M. Mason, Writing Law Dissertations: An Introduction and Guide to the Conduct of Legal Research (Pearson 2007) at p. 44

this definition the aim of the analysis is to determine the applicability of current money laundering legislation to cryptocurrencies in each jurisdiction. In determining the applicability of the law, the legislation will be interpreted based on the relevant legal definitions of the terms used; and it will be seen whether the offences can be committed using cryptocurrencies.

The case studies will involve criminal and civil law, as well as European legislation in the case of the UK. Although the applicability of the law will be doctrinal, the overall analysis of the law will also be socio-legal as the influences from international legislation will also be considered; each of the jurisdictions is party to a number of international agreements and organisations, for example all three jurisdictions are members of the FATF, and so each jurisdictions legislation may be analysed in light of the Recommendations issued by the FATF.

The three case studies will be separate but, as much as possible, be comparable in order to achieve a like for like analysis. A strict comparison could not be undertaken due to the differences in the legal systems in each jurisdiction. The parameters of the cases studies must be made clear; the research will be centred on the national legislation of each of the jurisdictions; it will not be possible to fully analyse the legislation of all US states or Australian federal territories. Similarly, in relation to enforcement authorities, national agencies will be the predominant subjects of analysis. Each jurisdiction implements its AML legislation using numerous regulatory authorities. In this research regulatory authorities will be divided into three categories; primary, secondary, and, where relevant, tertiary authorities. Primary authorities are

government departments; as Ryder identifies, this category will include authorities with policymaking powers.[182] Secondary authorities are regulatory bodies; these may be financial intelligence units or law enforcement agencies. Tertiary authorities are industry bodies which represent professions that are affected by regulation, or organisations representing cryptocurrencies.[183] The cryptocurrency industry is not one that is well represented by tertiary authorities, as such these will not be considered in detail. The research is primarily concerned with the legislation, and overall approach of the jurisdictions to AML; by categorising the authorities, a clearer comparison of approaches may be achieved. By using the case study method, the findings from each jurisdiction can then be compared.

The comparison between the three case studies will be *de lege lata* / *de lege lata*, comparing the laws that in place at the time of research. In light of this comparison, some *de lege ferenda* / *de lege lata* inferences may be made; the practice of one jurisdiction may be advised for the other.[184] Comparing the law of different jurisdictions is invaluable in considering reform; it is highly unlikely for a legal issue to be entirely unique to one jurisdiction. Additionally, the nature of the internet means much of the western world, if not the entire world, faces similar challenges in regulating a non-physical jurisdiction, upon which traditional physical borders do not apply.

[182] cf Ryder (n50) at p.25.
[183] ibid.
[184] J. Karha, 'How to Make Comparable Things: Legal Engineering at the Service of Comparative Law' in M.Van Hoecke, Epistemology and methodology of Comparative Law (Hart Publishing 2004).

Prior to analysing domestic legislation, a history of international developments will be provided; in undertaking the research in this order the primary domestic legislation may be viewed in light of the international legal sources, which will assist with interpretation, and in applying the law to cryptocurrencies.

Documentary Analysis

The method of analysis is informal documentary analysis. Informal in that no coding is used to analyse the documents. The subject of the analysis will be a variety of documents, consistent with the socio-legal methodology. Analysis is a very broad term; defined by the Oxford Dictionary as a "[d]*etailed examination of the elements or structure of something*."[185] To better define analysis for the purpose of this research; the various documents will be read, and the text pertinent to money laundering and cryptocurrencies will be examined. This examination will explain the legal approach to cryptocurrencies and money laundering, drawing links between the texts, as well as identifying differences. The purpose of this examination is to identify the current legal status, and treatment, of cryptocurrencies, and to predict the impending developments to that legal status and treatment.

Primary Sources

Various sources are used in this research. The primary sources of law are legislation and case law from each of the case study jurisdictions; all three of the case study

[185] Oxford English Dictionary, 'Analysis' <https://en.oxforddictionaries.com/definition/analysis> accessed 10th September 2019.

jurisdictions practice common law. As well as the primary sources of law, this thesis will also analyse international treaties, conventions, agreements and organisations.

Legislation

The national legislation of each case study jurisdiction will be the principal source of law. These will be sourced from state run websites and law databases. As stated in relation to the parameters of the case studies, this research does not focus on US state law or the law of Australia's federal territories; the limitation on resources mean only national legislation is used.

Case Law

The three case study jurisdictions selected are common law jurisdictions, as such, relevant case law will be used to demonstrate the application of the law, however, it is accepted from the outset that the phenomenon of cryptocurrencies is such a recent development, very few relevant cases have been heard.

Sources of International Law

In addition to the law of the case study jurisdictions; international sources of law are used in this thesis. The principal sources of international law relevant to this thesis are treaties and conventions of the United Nations and the European Union. Soft law is also considered, such as the Recommendations of the FATF as this is a leading organisation in developing international standards in AML legislation and regulation.

Secondary sources

Journal articles and commentaries will make up the secondary legal sources; these will provide clarification from commenters and their interpretations of the development of the law, as well as highlight the current issues in the area. The use of these sources can remain within the general doctrinal method; using primary and secondary sources the legal rules can be analysed and provide "*a descriptive commentary on points of law.*"[186] However, in this research the use of secondary sources will embrace the socio-legal approach, as the secondary sources will not be limited to describing the law, but also seeking to critique its effectiveness. Furthermore, the secondary sources will not be limited to legal journals; relevant non-legal sources will be used, as the subject matter of this thesis naturally overlaps with economics, politics and sociology.

The sources used in this thesis are predominantly qualitative data, as the focus of this research is on the status and treatment of cryptocurrencies, which will not be found in quantitative data. Where relevant some statistics will be included; but this will be restricted to limited circumstances, such as justifying the research, the value of cryptocurrencies, and estimations as to the extent of money laundering in each of the jurisdictions, and globally. This element of the research will provide insight into the size and value of the industry that is being researched, which will provide justification for considering potential legal involvement. Castronova argues the size of the user base and the economies of virtual worlds justify a legal assessment of virtual worlds,[187] demonstrating the social importance of virtual worlds and as such the potential need for an assessment of the law's role. This research focuses on cryptocurrencies, which

[186] cf Mason and Mason (n181) at p.64
[187] cf Castronova (n11) at p.39.

form a broader phenomenon than virtual worlds as some virtual currencies can interact with the real-world economy. Law is reactionary and if such a great volume of people are participating in a behaviour, producing such a high value of economic worth, it is right for the law to address the problems that may exist and the potential problems that may develop. Analysing the impact of the law on cryptocurrencies will also provide insight into the way the law is administered and its effectiveness.

As well the economic considerations, societal considerations must be explored. Media coverage of cryptocurrencies in recent years will have influenced public opinion. It will be important to consider the portrayal of virtual worlds and virtual currency issues raised here. Contemporary methods of communication and sources of information are particularly important in such a fast-evolving area. Traditional sources of comment such as monographs and journals cannot be produced as fast or as efficiently as online news articles, direct publications to the internet, or publications through social networks. The research will utilise respectable online sources of information, such as reputable news sites and press releases from government authorities. However, where possible the research seeks to build on the seminal work of researchers in this area via monographs and journal papers.

2.5.2. Limitations to the research

Additional empirical socio legal work could and perhaps should be undertaken in this area, such as interviews with users of cryptocurrencies and regulatory authorities. It was not possible to use empirical methods due to difficulties in contacting relevant individuals, these individuals consenting to being interviewed, the available financial

resources to this research, and the ethical issues around such sources. If research were to be undertaken within virtual communities it will be difficult to ascertain or verify the identity of the individuals contacted, as such it would also be difficult to be sure of the age of the interviewees. This research is limited to a socio-political exploration of the concept of money, as it is a law PhD, and not an economics study. Similarly, it is not possible for this research to have produced the analytical tools recommended, but these are recommended for further research.

2.6. Chapter Summary

This literature review identifies that money laundering is an extensively researched area, but that the emergence of cryptocurrencies has not been fully addressed within academic literature. Trends in AML regulation have been observed, such as rise of the FATF and EU to take the place of the UN in leading global AML efforts, and the separation of money laundering from drug offences only for it to be combined with terrorist financing. This thesis focuses solely on money laundering, as it is distinguishable from the financing of terrorism. The existing legislation has been identified and it is clear that the UK is compliant with AML regulation of the traditional financial system, but it has fallen behind the US and Australia as it has yet to address the threats posed by cryptocurrencies. Current international guidance is observed to be a commendable first step to addressing the money laundering threat of cryptocurrencies, but this thesis argues that the guidance is ineffective as the majority of cryptocurrency transactions remain outside of AML regulation.

Before the relevant laws can be considered, the concept of cryptocurrencies and money laundering must be fully understood, therefore the next chapter explores the phenomenon of cryptocurrencies, defining and differentiating them from fiat currency. The chapter also analyses the concept of money and assesses whether cryptocurrencies are indeed money.

Chapter 3. Contextualisation

3.1. Chapter Outline

In this chapter, the subject matter of the thesis will be introduced and explained. The key terms which require explanation are; virtual worlds, virtual currencies, and cryptocurrencies. Once these have been defined, the concept of money will also be analysed, cryptocurrencies will be assessed against theories of money, and the functions of money. These discussions are necessary in order to consider the link between money laundering and cryptocurrencies; while it may not be possible to prove the extent to which cryptocurrencies are used to launder money, it will be shown that cryptocurrencies have the potential to be utilised in the money laundering process as demonstrated by convictions in the UK and US. The Financial Action Task Force (FATF) consider cryptocurrencies worthy of attention for this reason.[1]

Cryptocurrencies, and their characteristics, will be identified and assessed as to whether they can be defined as money, or as a type of money. This is necessary in order to establish that cryptocurrencies are a potential avenue to launder money. Cryptocurrencies have been prominent in the media in recent times, partly fuelled by the surges in price. The most well-known cryptocurrency is Bitcoin, partly due to its changeable value, its highest value being $19,447 in December 2017.[2] This chapter will identify Bitcoin as a cryptocurrency, which is a distinct type of virtual currency.

[1] Financial Action Task Force, 'Virtual Currencies – Key Definitions and Potential AML/CFT Risks' <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 27 October 2019.
[2] XE, 'USD per 1 XBT' <https://www.xe.com/currencycharts/?from=XBT&to=USD&view=2Y> accessed 19 March 2019.

In determining whether cryptocurrencies are money, theories of money must be analysed, five theories will be considered; orthodox, Marxist, state theory, social construction theory, and credit theory. Theories of money may be categorised into two broad groups; metallist and chartalist.[3] Metallist theories consider efficiency and market forces as the principle drivers in the formation of money, rather than the state.[4] Chartalists place the state in a much more prominent role in the creation of money,[5] creating money as tokens which have little value in themselves but have value as means of payment.[6] Orthodox and Marxist theories of money are categorised as metallist theories of money; as the intrinsic value of the thing being traded as money is paramount.[7] These theories may be contrasted with state theory and credit theory, which may be considered as chartalist theories of money. Cryptocurrencies will be assessed against the theories of money to determine their status in relation to money. Cryptocurrencies are not consistent with existing theories of money, but they are not wholly incompatible. It will be concluded that although cryptocurrencies are not currently able to perform the functions of money, it is possible for this to change with higher levels of acceptance. The Financial Conduct Authority (FCA) do not accept cryptocurrencies as currency or money,[8] and categorise cryptocurrencies as 'cryptoassets',[9] which is a broad term. The position of the FCA and the United Kingdom's (UK) response to cryptocurrencies will be analysed in chapter five.

---

[3] Both terms are defined later in this chapter, for further discussion see: S. Bell, 'The Role of the State and the Hierarchy of Money' (2001) 25 Cambridge Journal of Economics 149.
[4] D. C. North, Institutions, Institutional Change and Economic Performance (Cambridge University Press, 1990).
[5] A. Smith, *An Inquiry Into the Nature and Causes of The Wealth of Nations*, (The Cannon Edition, New York, The Modern Library, 1937).
[6] ibid.
[7] K. Menger, 'On Origins of Money' (1892) 2(6) Economic Journal 293.
[8] ibid at 2.7.
[9] Financial Conduct Authority, 'Guidance on Cryptoassets – Consultation Paper' <https://www.fca.org.uk/publication/consultation/cp19-03.pdf> accessed 19 March 2019 at 2.3.

The analysis in this chapter will focus on cryptocurrencies, the broader term virtual currencies will be considered, and alternative categories of virtual currency will be identified. However, as identified by the FATF,[10] cryptocurrencies will be identified as the focus of this thesis as they are considered to pose the highest money laundering risk.

Prior to the analysis of cryptocurrencies against the theories of money, the key concepts of this thesis must be introduced and defined. Cryptocurrencies must be distinguished from the wider term virtual currencies, as virtual currencies exist both within virtual world, and on the internet in general, therefore these terms need defining and contextualising.

3.2. Virtual worlds

Castronova identifies three defining features of virtual worlds: 'interactivity', 'physicality' and 'persistence'.[11] Users must be able to access the world remotely, it must be a simulation of a first-person physical environment, and finally it should continue to run whether anyone is using it or not.[12] Interactivity and persistence are the most important of these features. Persistence is particularly important as it distinguishes virtual worlds from computer games and simulations; the virtual world is always functioning, even when the user logs off, and it can be affected by an infinite

[10] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Currencies' <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf> accessed 19 March 2019 at p.32.
[11] E. Castronova, Virtual Worlds: A First Hand Account of Market and Society of the Cyberian Frontier, [2001] SSRN CESifo Working Paper Series No. 618.
[12] ibid.

number of users. Bell also defines virtual worlds by their attributes, echoing the 'persistence' requirement of the Castronova definition, but adding that the interaction should be 'synchronous',[13] as such the communication and interactivity should be in real time and not turn based.[14] The need for a virtual world to be synchronous is a demonstration of the development virtual worlds from early text based virtual worlds and role-playing games. The requirement of real time interaction incorporates Castronova's 'physicality' requirement. Bell also requires the program to be 'avatar-based'[15] in that users explore the world with their avatar; this can also be seen as an extrapolation of Castronova's 'physicality' criterion.

Virtual worlds may also be known as Massively Multiplayer Online Role-Playing Games (MMORPG) and their development may be traced to the development of role-playing games (RPGs). Role playing and simulation has been around for millennia, Lastowka dates simulation back as far as Ancient Greece.[16] The movement of RPGs to internet environments was not surprising and Brenner see the basis of many early RPGs stemming from the game *Dungeons and Dragons*.[17] These early games were known as Multi-User Dungeons (MUDs), these were largely text based and developed during the 1970s.[18] Also developing were non-game environments described as Multi Objected Oriented (MOO)[19] such as *LambdaMOO*.[20] Text based networks soon developed to become first-person graphical environments as computer graphics

[13] M. W. Bell 'Toward a Definition of "Virtual Worlds"' (2008) 1(1) Journal of Virtual Worlds Research 1 at p.3.
[14] ibid.
[15] ibid.
[16] G. Lastowka, *Virtual Justice: The New Laws of Online Worlds* (Yale University Press, 2010) at p.31.
[17] S. Brenner, 'Fantasy Crime' (2008) 11(1) Vand J Ent & Tech L 1 at p.20.
[18] ibid.
[19] B. J. Gilbert, 'Getting to Conscionable: Negotiating Virtual Worlds' End User License Agreements without Getting Externally Regulated' (2009) 4(4) JICLT 238.
[20] ibid.

improved, along with the ability of the internet to deal with increased traffic, especially with the increased access to broadband internet.[21]

The broadest categories of virtual worlds are 'game worlds' and 'open worlds'.[22] Game worlds provide users with objectives, they are competitive, and the user's aims include improving their characters 'level' and collecting items they can equip their character with. This is achieved though completing tasks often known as quests, many game worlds include a fighting element; users may fight each other and can take items from a defeated opponent. An example of a game world is World of Warcraft (WoW),[23] which is described as the biggest online game in the world,[24] peaking at over 10 million subscribers in December 2014.[25]

Open worlds are not objective orientated, they are merely simulations; be that of the real world or a fantasy world. Second Life is a prominent open world; users create an 'avatar' which they may customise and use to explore the virtual world. Users are free to do whatever they choose, hence the term open world, they may purchase land,

[21] R. Kennedy, 'Law in Virtual Worlds' (2009) 12(10) Journal of Internet Law 3.
[22] E. Castronova, 'The Right to Play' (2004) 49 NYL Sch L Rev 185.
[23] Blizzard, 'World of Warcraft: Game Guide' <http://eu.battle.net/wow/en/game/> accessed 11 June 2015.
[24] IGN, 'IGN Presents the History of World of Warcraft' <http://uk.ign.com/articles/2009/08/18/ign-presents-the-history-of-warcraft> accessed 11 June 2015.
[25] Forbes, <http://www.forbes.com/sites/erikkain/2014/11/19/world-of-warcraft-tops-10-million-subscribers-following-warlords-of-draenor-expansion/> accessed 11 June 2018. This has since dropped but accurate figures are not available as Blizzard, the game's developer, stopped releasing figures in 2015: E. Makuck, Gamespot <https://www.gamespot.com/articles/blizzard-will-no-longer-report-world-of-warcraft-s/1100-6431943/> accessed 29 March 2019.

create in world objects and trade amongst each other. Second Life[26] is an example of an open world which has over 1 million regular users.[27]

Virtual worlds may require payments from users in a number of ways, users may have to pay to access subscription or pay for additional content in 'freemium' worlds; a 'freemium' virtual world is one which may be played for free, but users may choose to pay a fee to access premium features.[28] Free-to-play virtual words are platforms that do not charge a subscription fee for user access, these worlds do not involve any financial transactions. Subscription based games are games which require the user to pay to access the virtual world, usually a monthly fee, such as WoW.[29] In 'freemium' virtual worlds, the platform is free to access but the user may pay to access premium content or accelerate their avatar's development. Second Life may be viewed as an example of a freemium virtual world; users may access Second Life for free, but they can pay to acquire a premium membership which gives the user land in Second Life, a stipend of in world currency (Linden Dollars) and access to premium items in world.[30] Alternatively, Second Life users may retain a free account but purchase Linden Dollars to acquire items in the Second Life marketplace.[31]

Trade is a common feature of most virtual worlds, predominantly via in-world currency. Users create or acquire objects, they often gain surpluses of common items and may

[26] Linden Labs, 'What is Second Life' <http://secondlife.com/whatis/> accessed 11 June 2015.
[27] Business Insider, 'Second Life Has Devolved into a Post-Apocalyptic Virtual World, And The Weirdest Thing Is How Many People Still Use It' <http://www.businessinsider.com/second-life-today-2014-7?op=1&IR=T> accessed 11 June 2015.
[28] BBC News, 'Video Games Embrace China's Freemium Model to Beat Piracy' <http://www.bbc.co.uk/news/technology-20899165> accessed 17 June 2015.
[29] Blizzard, 'Games and Subscriptions' <http://eu.battle.net/wow/en/shop/> accessed 11 June 2015.
[30] Linden Labs, 'Become a Second Life Premium Member' <https://secondlife.com/my/account/membership.php> accessed 11 June 2015.
[31] Linden Labs, 'Second Life Market Place' <https://marketplace.secondlife.com/?lang=en-US> accessed 11 June 2015.

lack rare ones. This, much like the development of real-world currency, requires a commodity with a standardised value which may be used as a medium of exchange; virtual world currencies are the medium of exchange in virtual worlds. Each virtual world will usually have its own virtual world currency, such as Linden Dollars in Second Life.

Virtual currencies of specific virtual worlds are issued and controlled by the developers, and they are not classified as cryptocurrencies. This thesis focuses on the risks posed by cryptocurrencies. It is important to identify and distinguish virtual world currencies from cryptocurrencies, as any recommended reforms will not be targeted towards virtual worlds.

3.3. Virtual Currencies

The term virtual currencies used alone refers to any currencies which exist solely in electronic form, having no official physical form. A virtual currency is defined by FATF as;

> "*a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status … It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency.*"[32]

[32] Financial Action Task Force, 'Virtual Currencies – Key Definitions and Potential AML/CFT Risks' <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 27th October 2019 at page 4.

The European Central Bank (ECB) views virtual currencies as 'schemes',[33] and in 2012 defined them 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*."[34] The position of the ECB was updated in relation to virtual currencies in 2015, the ECB stated that "*the word 'unregulated' should be deleted from the definition used in 2012,*"[35] as it recognised some jurisdictions had regulated virtual currencies.[36] The definition was therefore updated to a "*digital representation of value, not issued by a central bank, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money*."[37] The ECB do not recognised virtual currencies as money, but accept that they can be used as an alternative to money.

These definitions are deliberately generalised to apply to all virtual currencies, but there are important differences between types of virtual currencies. The ECB identify closed, unidirectional, and bidirectional virtual currencies; these are defined based on the way in which real economy money,[38] or fiat money may be exchanged for virtual currency.

In a closed virtual currency, no fiat money enters the system; the ECB state that there is "almost no link to the real economy"[39] and that these may also be known as "in-

[33] ECB, 'Virtual Currency Schemes' <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> accessed 02 June 2019.
[34] ibid at p13.
[35] ibid at p25.
[36] ibid.
[37] ibid.
[38] ibid at p13.
[39] ibid.

game only"[40] currencies. Users acquire this type of virtual currency via the virtual world they participate in; they may not use fiat money to purchase in-game currency. Unidirectional virtual currencies are currencies which may be purchased using fiat currency, but cannot be exchanged back; once converted the virtual currency must be spent within the relevant world or infrastructure. An example of this was Facebook Credits;[41] they could be purchased using fiat currency, but may only be spent on virtual goods offered by Facebook and associated applications.[42] The final category is bidirectional virtual currencies; these currencies allow the user to buy and sell the currency; Linden Dollars are the example provided by the ECB.[43] These types of currencies are "*similar to any other convertible currency with regard to its interoperability with the real world*."[44]

It can be seen that, the ECB classify virtual currencies based on the movement of fiat money into and out of the virtual currency's economy. The FATF also consider the transferability of the virtual currency into fiat currency, but also classify based on the organisational structure of the virtual currency. Figure 1 below demonstrates how the FATF categorises virtual currencies.

[40] ibid.
[41] Facebook, 'Where is my Facebook Credits?' <https://www.facebook.com/notes/molpoints/where-is-my-facebook-credits/439455502732806> accessed 02 October 2019.
[42] ECB, 'Virtual Currency Schemes' <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> accessed 02 June 2019 at p14.
[43] ibid.
[44] ibid.

Figure 1. FATF Categories of Virtual Currency[45]

	Centralised	Decentralised
Convertible	Linden Dollars (used in Second Life) are an example of a convertible virtual world currency; users may exchange their currency for US Dollars. The currency is centralised, Linden Labs (the developer of Second Life) act as administrators.	Examples of decentralised currencies include Bitcoin and Dogecoin. These are convertible for fiat currency but not controlled by a central administrator.
Non-Convertible	World of Warcraft (WoW) gold is non-convertible virtual world currency; users may not convert this into a fiat currency. WoW gold is controlled by the game developers, Blizzard	None exist.[46]

A virtual currency is convertible if it may be transferred into a fiat currency; if this is not possible, the currency is non-convertible. This may also be referred to as 'open' or 'closed' currencies; a non-convertible currency operates a 'closed' system, none of the currency may be transferred into fiat currency. The convertibility of a currency is not

[45] Financial Action Task Force, 'Virtual Currencies – Key Definitions and Potential AML/CFT Risks' <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 27th October 2019 at p.8.
[46] ibid.

fixed; it is observed that a virtual currency may become convertible, even via third party facilities, beyond the control of the currency's administrator.[47] In comparison to the ECB categories, both closed and unidirectional currencies would be viewed as non-convertible by the FATF classification. The values of these currencies are not fixed, they are dictated by market forces, which differentiates digital currencies from digital payment facilities, which have fixed exchange rates,[48] such as PayPal[49] or the now obsolete Liberty Reserve.[50]

As can be seen by Figure 1, the FATF also consider the structure of the virtual currency in order to categorise them. Structures are either centralised or decentralised. A virtual currency is centralised when it is controlled by a single administrating authority; examples of these are the currencies of virtual worlds. The degree of control exercised may vary according to the practices of the administrator and whether the currency is convertible or not. A decentralised currency has no central authority; these may be based on an algorithm or code which dictates the production of the currency.

In view of the aims of this research, it appears logical to adopt the FATF distinctions over that of the ECB; with regards to money laundering it is important to be able to convert the virtual currency back into fiat money in order to fully benefit from the criminal proceeds. As such virtual currencies fall into one of three categories; convertible centralised, non-convertible centralised, and convertible decentralised. No

[47] ibid at p.5
[48] For a detailed explanation of payment facilities see: C. Chambers Jones and H. Hillman, *Financial Crime and Gambling in a Virtual World: A new Frontier in Cybercrime* (Edward Elgar, 2014 at p139.
[49] PayPal, 'About PayPal' <https://www.paypal.com/uk/webapps/mpp/about> accessed 17 June 2018.
[50] BBC News, 'Liberty Reserve digital money service forced offline' <http://www.bbc.co.uk/news/technology-22680297> accessed 17 September 2019.

examples of non-convertible decentralised currencies have been identified by the FATF or the ECB. One further distinction which may be made relates to the usability of the virtual currency. A virtual currency is known as a virtual world currency when it is only accepted in a particular virtual world; this type of virtual currency is controlled by the developers of the virtual world and as such will be centralised. As demonstrated by the WoW gold and Linden Dollar comparison, virtual world currencies may be convertible or non-convertible; a virtual world currency may become convertible via a third party.

3.3.1. Bitcoin

Bitcoin warrants particular attention due to its value,[51] and because it is the forerunner to the growth cryptocurrencies.[52] Bitcoin is a virtual currency but is also be referred to as a cryptocurrency, a currency which uses cryptography to disguise or protect the users of the currency. Cryptocurrencies utilise cryptography techniques to conceal the identity of the sender and receiver of a message or transfer. Southall and Taylor[53] trace the technique used by Bitcoin, and many other cryptocurrencies, back to proposals made by Chaum in the early 1980's, who proposed sending private messages with a serial key system;[54] messages were sent using a public key, but only the sender and recipient could access the message using a private key. Chaum

[51] BBC News, 'Bitcoin Currency Hits New Record High' <https://www.bbc.co.uk/news/business-42135963> accessed 19 March 2019.
[52] Though widely considered the first cryptocurrency, the original paper proposing Bitcoin references a number of papers including previous proposals for web-based money such as: W. Dai, 'b-money' (1998) <http://www.weidai.com/bmoney.txt> accessed 13 October 2019.
[53] E. Southall and M. Taylor, 'Bitcoins' [2013] 19(6) Computer and Telecommunications Law Review 177.
[54] D. Chaum, 'Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms' [1981] 24(2) Communications of the ACM 84.

subsequently suggested the technique could be used to facilitate anonymous payments.[55]

Bitcoin is not the first digital currency; previous digital currencies existed but failed to persist. Examples of this include 'Beenz' which launched in 1999 and promised to create "a generation of e-millionaires"[56] but closed in 2001,[57] just weeks after rival currency 'Flooz'[58] also shut down. As is discussed later is this chapter,[59] numerous factors determine whether something is accepted as money, and as the demise of Beenz and Flooz demonstrates, early digital currencies failed to be accepted as money by a large enough community.

Bitcoin was created by Satoshi Nakamoto in 2009,[60] the true identity of Bitcoin's creator(s) is unknown as Satoshi Nakamoto is a pseudonym. It is not known if Satoshi Nakamoto is one person or a group of people as throughout the self-published paper proposing Bitcoins, the term 'we' is used to refer to the author, suggesting it may be more than one person. Bitcoins can be distinguished from early digital currencies, and subsequent digital currencies can be seen to have copied the characteristics of Bitcoin. Bitcoin operates using the process summarised below as it appeared in the original paper by Satoshi Nakamoto:[61]

[55] D. Chaum, 'Blind Signatures for Untraceable Payments' in D. Chaum. R.L. Rivest and A.T. Sherman (ed), '*Advances in Cryptology*' (Session III, Springer US, 1982) pp199-203.
[56] BBC News, 'Business: The Company File: Beenz means business' <http://news.bbc.co.uk/1/hi/business/297133.stm> accessed 12 June 2019.
[57] Commerce Times, 'Beenz.com Closes Internet Currency Business' <http://www.ecommercetimes.com/story/12892.html> accessed 12 June 2015.
[58] CNet, 'E-currency Site Flooz Goes Offline' <http://news.cnet.com/2100-1017-271385.html> accessed 12 June 2019.
[59] See 3.4 and 3.5.
[60] Bitcoin Wiki, 'Research' < http://bitcoin.org/bitcoin.pdf> accessed 10 October 2019.
[61] ibid.

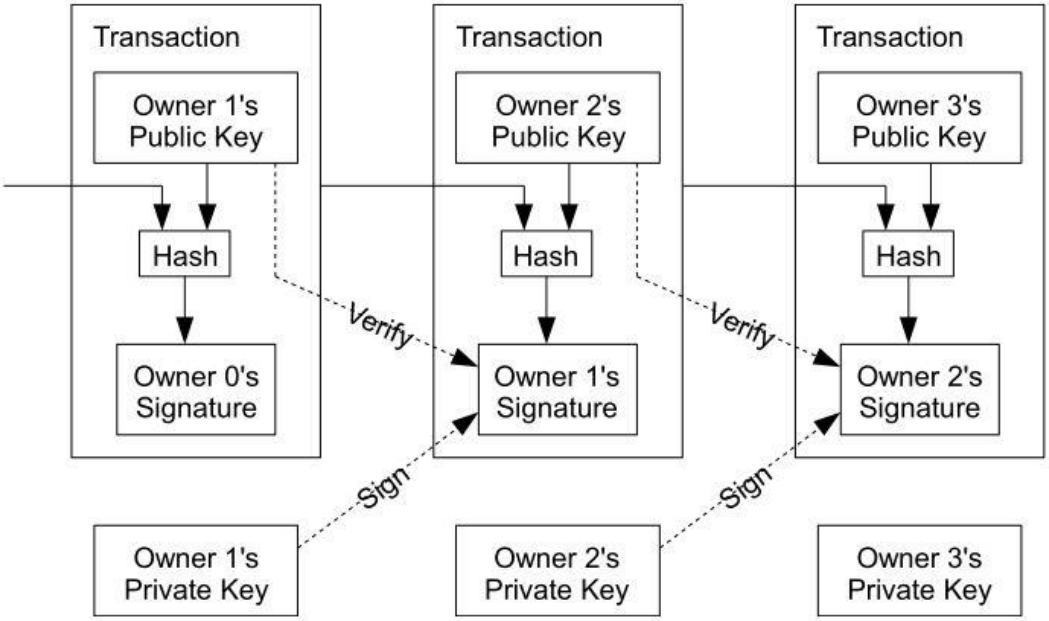
1) *New transactions are broadcast to all nodes.*
2) *Each node collects new transactions into a block.*
3) *Each node works on finding a difficult proof-of-work for its block.*
4) *When a node finds a proof-of-work, it broadcasts the block to all nodes.*
5) *Nodes accept the block only if all transactions in it are valid and not already spent.*
6) *Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.*[62]

Stage three introduces the concept of proof-of-work, this part of the process is known as mining, this involves a user's computer, known as a node, providing an answer which matches the solution the system is requesting in order to produce a 'block' with a 'proof-of-work' attached. Blocks are sets of data which are permanently recorded in the Bitcoin network, they are a record of Bitcoin transactions,[63] and known as the blockchain,[64] By finding the proof-of-work and completing the block the user then acquires some new Bitcoins, currently 6.25 Bitcoins.[65] Each block can only be produced once, and the Bitcoin reward goes to the miner who first produces the block, duplicates are not accepted. The alternative way to obtain Bitcoins is to purchase it via exchanges.[66]

[62] ibid at p.3.
[63] ibid at p.8.
[64] Bitcoin, 'How it Works' <https://bitcoin.org/en/how-it-works> accessed 13 October 2019.
[65] B. Bambrough, 'A Bitcoin Halvening Is Two Years Away - Here's What'll Happen To The Bitcoin Price' (Forbes, 29 May 2018) <https://www.forbes.com/sites/billybambrough/2018/05/29/a-bitcoin-halvening-is-two-years-away-heres-whatll-happen-to-the-bitcoin-price/#4bffecd05286> accessed 19 March 2019.
[66] Rates can be viewed here: Bitcoin Charts, 'Markets' <http://bitcoincharts.com/markets/> accessed 18 June 2015.

Users send messages to each other in order to send and receive Bitcoins; this process uses a cryptography technique similar to that proposed by Chaum. Each user has a Bitcoin wallet with a unique address, when one user sends another user some Bitcoins two keys are used. The first is the public key which tells the network of the transaction between the two keys, the second is a private key which is a signature from the sender which prevents the amounts being transferred from being altered by anyone else in the network.[67] This is shown below in Figure 2.

Figure 2. Bitcoin Transactions[68]



The use of keys rather than names allows all transactions to be public and verifiable, to ensure no Bitcoins are spent twice, but still ensure the anonymity of those making the transactions. This anonymity will be lost if the user's key were to become public,

[67] Bitcoin.org, 'How Does Bitcoin Work?' <http://bitcoin.org/en/how-it-works> accessed 19 January 2014.
[68] Taken from: Bitcoin Wiki, 'Research' <http://bitcoin.org/bitcoin.pdf> accessed 10 June 2015.

and then all transactions may be traced. The anonymity attached to cryptocurrencies is addressed by the United States Government Accountability Office in their 2014 report, which described such currencies as pseudonymous,[69] as the although the users name is not known, other details are published on the blockchain, such as their Bitcoin address, the time of the transaction, and the amount. Transactions of Bitcoins are confirmed by users of the network; confirmation ensures the sender has sufficient funds and that there are no double spends of Bitcoin. This confirmation occurs when the proof-of-work is found; at this point, the computer which solved the proof-of work verifies all of the transactions which took places since the last proof-of-work was produced.[70] In order to limit the number of Bitcoins being produced the difficulty proof-of-work problems increases to reduce the rate at which miners can complete blocks and obtain new Bitcoins.[71]

Bitcoin's model of coin production, transaction security, and transaction logging has been adopted by numerous subsequent cryptocurrencies, such as Ethereum,[72] Dogecoin[73] and LiteCoin.[74] The various currencies compete amongst each other by claiming to offer faster transaction speeds or increased security.[75] A key feature of cryptocurrencies is the use of a blockchain, also known as distributed ledger,[76] which

[69] United States Government Accountability Office, 'Virtual Currencies: Emerging Regulatory, Enforcement, and Consumer Protection Challenges' <http://gao.gov/assets/670/663678.pdf> accessed 16 December 2015 at p.6.
[70] Bitcoin Wiki, 'Research' <http://bitcoin.org/bitcoin.pdf> accessed 10 June 2015 at p.3.
[71] ibid.
[72] Ethereum, 'Learn about Ethereum' <https://www.ethereum.org/learn/> accessed 13 October 2019.
[73] Dogecoin, 'Dogecoin' <https://dogecoin.com/> accessed 13 October 2019.
[74] LiteCoin, 'LiteCoin' <https://litecoin.org/> accessed 13 October 2019.
[75] The Guardian, 'Nine Bitcoin alternatives for future currency investments' <http://www.theguardian.com/technology/2013/nov/28/bitcoin-alternatives-future-currency-investments> accessed 17 June 2015.
[76] Financial Conduct Authority, 'FCA publishes Feedback Statement on Distributed Ledger Technology' (15 December 2017) <https://www.fca.org.uk/news/press-releases/fca-publishes-feedback-statement-distributed-ledger-technology> accessed 13 October 2019.

is publicly available.[77] The accessibility of cryptocurrency blockchains can be further aided through the use of Application Programme Interfaces[78] (APIs) which allow for the creation of applications to analyse the transaction data published in the blockchain. The identity protection afforded by cryptocurrencies such as Bitcoin can also be challenged as Meiklejohn *et al*[79] "*were able to identify 1.9 million public keys with some real-world service or identity,*"[80] however, "*in many cases the identity was not a real name, but rather (for example) a username on a forum.*"[81] More recently, Juhász *et al* identified 22,363 users 1,797 associated IP addresses.[82] While difficulties will remain with determining which users require identification and investigation, Juhász *et al* argue their "*method is cheap in terms of resources,*"[83] and their "*algorithms are relatively easy to implement and can be combined with other Bitcoin-transaction related information.*"[84] The research of Meiklejohn *et al* and Juhász *et al* demonstrate that the anonymity of cryptocurrencies may be eroded by the aforementioned techniques, but more research is needed.

Bitcoin, and other cryptocurrencies, are exchanged globally and are referred to in similar terms as money; such as the term 'currency' within cryptocurrency, the term 'cash' in Bitcoin Cash, and the symbol used in Bitcoin's logo being akin to a monetary

[77] As demonstrated by: Blockchain, 'Block Explorer: Bitcoin' <https://www.blockchain.com/explorer> accessed 13 October 2019, Blockchain, 'Block Explorer: Ethereum' <https://www.blockchain.com/explorer?currency=ETH> accessed 13 October 2019, and Blockchain, 'Block Explorer: Bitcoin Cash' <https://www.blockchain.com/explorer?currency=BCH> accessed 13 October 2019.
[78] H. Henderson, 'application programming interface (API)' in Harry Henderson (ed) Encyclopaedia of Computer Science and Technology (3rd ed, Facts On File, 2017) <https://search-credoreference-com.ezproxy.uwe.ac.uk/content/entry/fofcomputer/application_programming_interface_api/0>
[79] Sarah Meiklejohn, et al, "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names," (2013) 38(6) ;Login: 10.
[80] ibid at p.14.
[81] ibid.
[82] P. L. Juhász, J. Stéger, D. Kondor and G. Vattay, 'A Bayesian approach to identify Bitcoin users' (2018) 13(12) PLoS ONE 1 at p.13.
[83] ibid at p.18.
[84] ibid.

symbol. Due to the connotations towards money, and cryptocurrencies representing such a novel and undefined phenomenon, an analysis of money is required, to determine whether cryptocurrencies are indeed money, or have the potential to become money.

3.4. Definition of Money

Definitions of a currency centre on the concept of a certain type of money being the legal tender of a country and controlled by the central bank of that country. The largest exception to this is the Euro which is the currency of a large number of countries across Europe and controlled by the ECB, the central bank of the European Union. A medium of exchange may still be viewed as money, despite not enjoying the status of legal tender in a particular jurisdiction. Fox states that the "*status of an asset as money is a social fact rather than a matter of legal fiat.*"[85] As such, "*an asset may circulate as a generally accepted medium of exchange, without also enjoying the status of legal tender in that state.*"[86] Fox gives the example of the US dollar which is accepted as payment in numerous countries where it is not legal tender. It would therefore seem sensible to establish whether cryptocurrencies are in fact money; as such the question must be asked, what is money?

3.4.1. Theories of Money

Debates over the origins on money have existed for millennia;[87] subsequently a number of theories have been developed. Five theories will be discussed here;

[85] D. Fox, *Property Rights in Money* (OUP, 2008) at p17.
[86] ibid.
[87] Aristotle considered the nature of money in: Aristotle, Politics, Book 1, Ch.9 (384-322 BC).

orthodox, Marxist, state theory, social construction theory, and credit theory. Orthodox and Marxist theories of money are metallist theories of money; this school of thought places intrinsic value on the thing being traded as money.[88] Metallist theories consider efficiency and market forces as the principle drivers in the formation of money, rather than the state.[89] These theories may be contrasted with state theory and credit theory, which are chartalist theories of money. Chartalists place the state in a much more prominent role in the creation of money,[90] the state creates money as tokens which have little value in themselves but have value as means of payment.[91] The social construction theory will also be considered, this does not necessarily conform to either category of theory, as it focuses on the differing situations money is used in order to determine what is meant by money. A hierarchy of money will then be analysed; this will demonstrate that money is not fixed, and numerous things may be money to varying extents. Cryptocurrencies will be placed on the hierarchy. It is argued that by being able to satisfy some functions of money, cryptocurrency are illustrated as capable of being utilised as a money laundering tool.

3.4.2. Metallist and Chartalist Theories

As it has already been stated, theories of money may be divided into two categories, metallist and chartalist, and individual theories of money will be considered within their category, beginning with metallist theories. Marxist and orthodox theories of money are metallist theories, as both of these theories view money as having intrinsic value, which means that the item used as money is valuable even when not being used as money. The Marxist theory considers money to be a measure of value for labour; gold

[88] cf Menger (n7).
[89] cf North (n4).
[90] cf Smith (n5).
[91] ibid.

is used to measure the labour required to produce the item being purchased. Likewise, in the orthodox theory, the commodity used as money is a commodity which is used as a measure of the value of other commodities. The metallist theories view money as being created by society and merchants; the state has a minor role, supporting the system through contract and property law.[92] The state theory of money and credit theory are chartalist theories of money; these theories place the state in a much more prominent role in the creation of money. Chartalist theories also differ from metallist in their view over the value of money; chartalist theories consider money to be valuable as tokens of credit, the thing used as money may not have any value in itself, it gains value through being usable. Money is then the mechanism by which debts is accepted and repaid. Metallist theories view the asset used as money as having intrinsic value.

Orthodox Theory of Money

The orthodox theory suggests that money evolved out of the inefficiencies of barter, principally, as identified by Jones, the issue of requiring double wants.[93] For example, A must find someone, B, with the commodity they require, who in turn requires what A is offering in return. As Jones observes, this in inefficient because the chances of this occurring are low, and the relevant commodities may be of differing values.[94] A further issue with barter is that not everyone offers commodities, some people may provide services, and difficulties may arise in valuing services against commodities. Menger raises these issues, as well as the issue of transporting goods, or commodities restricted to specific times of the year.[95] Feldman and Jones recognise barter is *quid*

[92] cf North (n4).
[93] R. A. Jones, 'The Origin and Development of Media of Exchange' (1976) 84 (4, Part 1) August Journal of Political Economy 757 at 757.
[94] cf Jones (n93) at 759.
[95] cf Menger (n7) at 242-243.

pro quo[96] and that money is the item which all market participants keep in supply.[97] Feldman states that all market participants will hold a "*positive quantity of one good (which we will call 'money')*",[98] which will be accepted in lieu of wanting to directly swap goods, and Jones interprets this as a "*good which everyone desires.*"[99] In determining the good which will be used as money, Menger notes that precious metals are best suited because "*their saleableness is far and away superior to that of all other commodities.*"[100] 'Saleableness is determined by a number of factors; demand, supply, divisibility, status, and market speculation.[101] Saleableness appears to have the same meaning as value; in essence precious metals are used because they are valuable. Precious metals are not always the basis of money, Radford observes that in prisoner of war (P.O.W) camps cigarettes took the role of money and were traded at standard values for inter-prisoner trade.[102] The exact commodity which becomes money may vary, but it will have value itself; as well as be divisible, durable and portable, traits identified by Menger[103]

The orthodox theory attributes very little to the role of the state; Radford's assessment of P.O.W camps demonstrates the development of an economy without the control of the state. Menger argues that money "*has not been generated by law,*"[104] but that it is

[96] A. M. Feldman, 'Bilateral Trading Processes, Pairwdse Optimality and Pareto Optimality'(1973) 40(4) Review of Economic Studies 463 at 463, and R. A. Jones, 'The Origin and Development of Media of Exchange' (1976) 84 (4, Part 1) August Journal of Political Economy 757 at 757.
[97] A. M. Feldman, 'Bilateral Trading Processes, Pairwdse Optimality and Pareto Optimality'(1973) 40(4) Review of Economic Studies 463 at 463.
[98] ibid.
[99] cf Jones (n93) at 759.
[100] cf Menger (n7) at p.252.
[101] ibid at p.246.
[102] R. A. Radford, 'The Economic Organisation of a P.O.W. Camp' (1945) November Economica, 189 at 191.
[103] cf Menger (n7).
[104] ibid at p.255.

a "*social, and not a state-institution.*"[105] North takes a similar position and argues that the law plays a facilitating role, protecting rights through property and contract law.[106] The orthodox theory of money puts forward the argument that money developed independently, as a social tool to facilitate trade. It suggests the commodity used as money should have value; and that this commodity by durable, divisible and portable. The role of the state is not prominent; it should simply take the role of enforcing the effects of money and protecting users.[107]

Applying the orthodox theory of money to cryptocurrencies, it can be seen that the limited role of the state is true in cryptocurrencies. In applying saleableness, as identified by Menger,[108] cryptocurrencies are divisible, and the process of mining provides a steady supply. However, while cryptocurrencies have been in high demand, the levels of market speculation have caused huge swings in value,[109] and this reduces the usability of cryptocurrencies as money. The key characteristic of the orthodox theory which cryptocurrencies do comply with is the role of the state being minimal.

Marxist Theory of Money

The Marxist theory is, like the orthodox theory, a metallist theory of money. Karl Marx, an eminent philosopher of the 19th Century and his writings are the foundations of

[105] ibid.
[106] cf North (n4).
[107] ibid.
[108] cf Menger (n7) at 246.
[109] Coverage of bitcoin and cryptocurrencies show that the relative values have been falling from the highs of 2017: BBC News, 'Bitcoin' <https://www.bbc.co.uk/news/topics/c734j90em14t/bitcoin> accessed 05 March 2019.

modern communism.[110] His theory of money is based on the concept of labour; money is quantified in terms of units of labour. Commodities have a value in money, which in turn places a value on the labour time required to produce that commodity. Money itself also has value, the gold used as money must be mined and minted; the price of gold acts as the price of labour.[111] Marx identifies money as the unit of account; everything may be measured in terms of labour, and in turn in terms of money. The role of the state and the law is a reduced one, money is a product of society. The Marxist theory identifies money as a cover for relations of domination; if money did not exist it would simply appear that people were under the control of other people.[112]

It might be that Marxist concepts of labour best apply to the mining process of cryptocurrencies, but nothing of intrinsic value is produced; just code which represents Bitcoins. Due to the computing power required to complete the mining process,[113] it is likely that those mining Bitcoin in particular, are having to use lots of fiat money in order to produce cryptocurrency, which is most probably not the 'labour' Marx was referring to when formulating his theory of money.

Metallist theories appear unworkable in modern monetary systems, particularly as the gold standard has been abandoned, so there is no solid commodity which paper notes represent; however, metallist theories do suggest that money existed before the state which would appear logical as humans formed into groups before forming into organised countries. Though metallist theories better explain money prior to the

[110] D. Mclellan, *Karl Marx* (London, Harper Collins, 1975).
[111] K. Marx, *Capital: Vol 1* (London, Penguin, 1976).
[112] ibid.
[113] The Guardian, 'Energy cost of 'mining' bitcoin more than twice that of copper or gold' <https://www.theguardian.com/technology/2018/nov/05/energy-cost-of-mining-bitcoin-more-than-twice-that-of-copper-or-gold> accessed 05 March 2019.

existence of states, the theories still fail to provide a satisfactory account of how the concept of money came into existence, chartalist theories may better explain money in the modern day. As surmised by Bell, chartalist theories treat money as a token rather than as a valuable commodity in itself,[114] and place the state at the centre of the operation of money,[115] which is a contrast to the role attributed by metallist theories of money. The state theory of money will demonstrate how chartalist theories consider the state's power to demand payment and the form the payment takes.[116] Credit theory will also be considered as this chartalist theory of money demonstrates that the role of wider society is not immaterial in shaping money and identified by Innes.[117]

State Theory of Money

As the name suggests, the state theory of money places the state at the centre of the creation of money; prominent proponents of this theory include Knapp[118] and Hurst.[119] Knapp argues that money is whatever the state understands as money, and what it understands as money is clear from what it will accept in payment of debts.[120] This money then acquires value in the community because it may be used to settle such debts. Smith provides the analogy of a prince who chooses to accept a proportion of taxes in paper money; this paper has then been given a certain value.[121] An important factor in the attribution of value in state theory is usability; the money has value because it is useful; it can be used to pay debts to the state. In turn this will encourage

[114] S. Bell, 'The Role of the State and the Hierarchy of Money' (2001) 25 Cambridge Journal of Economics 149 at p.154
[115] ibid.
[116] ibid.
[117] A. M. Innes, 'What is Money' (1913) 30 Banking LJ 377.
[118] G. F. Knapp, *The State Theory of Money* (Macmillan, 1924).
[119] J. W. Hurst, *A Legal History of Money in the United States 1774-1970* (University of Nebraska Press, 1973).
[120] cf Knapp (n118).
[121] cf Smith (n5).

the citizens of the state to trade in what the state understands as money; because the citizens will seek to collect this money in order to be able to meet their obligations to the state, this position was supported by Minsky.[122] Under the state theory of money value is assigned to money, and the value they are given is upheld by the state's acceptance of them at that value. Despite this the state is not the sole force, Mann recognises the influence the public may have on what is used as money, the State may be influenced by what the community already accepts as money.[123] Knapp claims that the state will make it clear what they will accept, regardless of whether it is legal tender.[124]

The role of the state is central to this theory of money; this is a clear contrast to the role of the state in the two previous theories. A further contrast is the way in which money is valued and the role of precious metals; in state theory the amount of precious metal in a coin is not relevant to its indicated value, whereas orthodox and Marxist approaches deem money to have value as a commodity. It is not possible to apply state theory to Bitcoin; there is no state associated with Bitcoin, and it is not possible to settle state debts in Bitcoins in any of the case study jurisdictions.

The decentralised nature of cryptocurrencies makes them antonymous to the state theory of money, with the state having little to no control. It is also difficult for cryptocurrencies to conform to the chartalist concept of money being a token, as the relative value of the token is constantly changing. While it is not impossible for the

[122] H. P. Minsky *Stabilising An Unstable Economy* (Yale University Press, 1986) at p231.
[123] Charles Proctor (ed), *Mann on the Legal Aspects of Money* (7th Edition, Oxford University Press, 2005).
[124] cf Knapp (n118).

state to adopt cryptocurrencies as payment for taxes, there is nothing to suggest this is likely to happen in the near future.

Credit Theory

Credit theory places credit and debt relationships at the heart of the creation of money; credit and debt are explained by Innes:

> *"What* A owes to B is A's debt to B and B's credit on A. A is B's debtor and B is A's creditor. The words 'credit' and 'debt' express a legal relationship between two parties, and they express the same legal relationship seen from two opposite sides."[125]

Debt cannot exist without someone else being in credit, credit is the opposite of debt but, as noted by Innes, credit may exist without debt; this is money.[126] Keynes makes similar arguments to Innes, seeing money as coming into existence on the creation of debt.[127] Bell interprets this further, viewing money as "*representing a promise or IOU held as an asset by the creditor.*"[128] Bell also comments on the claim by Minsky that "*everyone can create money; the problem is to get it accepted,*"[129] Bell sees this as slightly inaccurate; Bell accepts that anyone may try to create a money but that it cannot be created until acceptance has occurred.[130]

The concept of credit and debt correlating at all times, with the exception of money being credit alone, can be applied quite simply. Only money is its physical form may

[125] cf Innes (n117) at p.392.
[126] ibid.
[127] J. M. Keynes, *A Treatise on Money* (Harancourt Brace, 1930).
[128] cf Bell (n114) at p.150.
[129] cf Minsky (n122) at p228
[130] cf Bell (n114) at p.150.

be solely credit, all other money is in a credit-debt relationship. An example of the credit theory in practise is that of a demand deposit with the bank; the money which A may have in the bank is credit they have with the bank, at the same time that money is a debt owed by the bank to A. If A were to withdraw the money and hold it in a physical format, then the credit debt relationship has been neutralised and the money held by A is then purely credit.

Cryptocurrencies satisfy the contention of Minsky, they have been created, and users seek its acceptance from others. Bell's requirement of acceptance is difficult to judge, cryptocurrencies are not universally accepted, but there is a degree of acceptance, as can be demonstrated by Coinmap, which is a website recording where users of Bitcoin can spend their cryptocurrency.[131] As of March 2019, 14,413 Bitcoin venues are recorded on the site, considering French supermarket chain Carrefour has 12,300 shops worldwide,[132] it is not feasible to argue Bitcoin has achieved acceptance to the level required to satisfy the credit theory of money.

Social Construction Theory

The social construction theory is argued by Zelizer;[133] and suggests that money may be different in different situations. Grounding for this comes from historical references to cultures where male and female money were physically different commodities; Zelizer gives the example of the south-western Pacific island of Rossel where lower value coins are reserved for women.[134] On a summary reading of this theory, it would

[131] Coin Map 'World View' <https://coinmap.org> accessed 05 March 2019.
[132] Carrefour, 'Carrefour stores worldwide' <http://www.carrefour.com/content/carrefour-stores-worldwide> accessed 05 March 2019.
[133] V. A. Zelizer, 'The Social Meaning of Money: "Special Monies"' (1989) 95(2) 342.
[134] ibid 342.

immediately appear outdated; in modern civilisations a single currency is used by all members of a community, but this currency may be used in different ways depending on the circumstances. Zelizer looks at the spending habits of married women from 1870-1930 and finds that the use of 'domestic money' differs from the use of 'real money';[135] once money enters the household it is subject to different rules, distinct from the rules of the market. The exact uses of 'domestic money' may differ between households but the principle argument of Zelizer that the money of the housewife is very different from the salary of the husband; the size of a housewife's stipend may remain the same, even if the salary of the husband increases.[136] This concept is now outdated, with greater gender equality, but it may still apply in the sense of disposable income;[137] spending habits have been seen to change when levels of disposable income decrease.[138] This may show that when the money is seen as being disposable, or as spending money, it is spent with greater ease than when the money is needed to meet liabilities, such as rent or bills. This supports the essence of the social construction theory; that money may be treated differently in different situations, and a different form of payment may be used. Money which has already been designated for a particular purpose may be spent more liberally than money which is being saved for the future.

The social construction theory does not necessarily fit into either type of theory; this is because the social construction theory instead looks at the different uses of money

[135] ibid at 367.
[136] ibid at 368.
[137] Personal income that remains after direct taxes and government charges have been paid: Financial Times, 'Lexicon: Definition of Disposable Income' <http://markets.ft.com/research/Lexicon/Term?term=disposable-income> accessed 18 June 2015.
[138] Barclays, 'Where's Britain spending? The Barclaycard Consumer Spending Report Q3 2014' http://www.barclaycard.com/content/dam/bcardpublic/FinalContent/NewsandViews/2014/q3spendreport/Barclaycard_Spend_Report_Q3_2014.pdf> accessed 17 June 2015.

instead of its origins. This means that the social construction theory could be applied within the other theories as it seeks to explain a different phenomenon. Social construction theory may be relevant to cryptocurrencies, the use of cryptocurrencies as a payment mechanism is limited by the number of retailers willing to accept it, but in terms of settling payments between individuals, cryptocurrencies have potential as they can be used easily between two users.

The social construction theory, along with all of the discussed theories, can be assessed alongside the hierarchy of money considered by Bell,[139] which incorporates a number of theories of money to consider how different types of money are ranked according to the ease with which they are accepted.

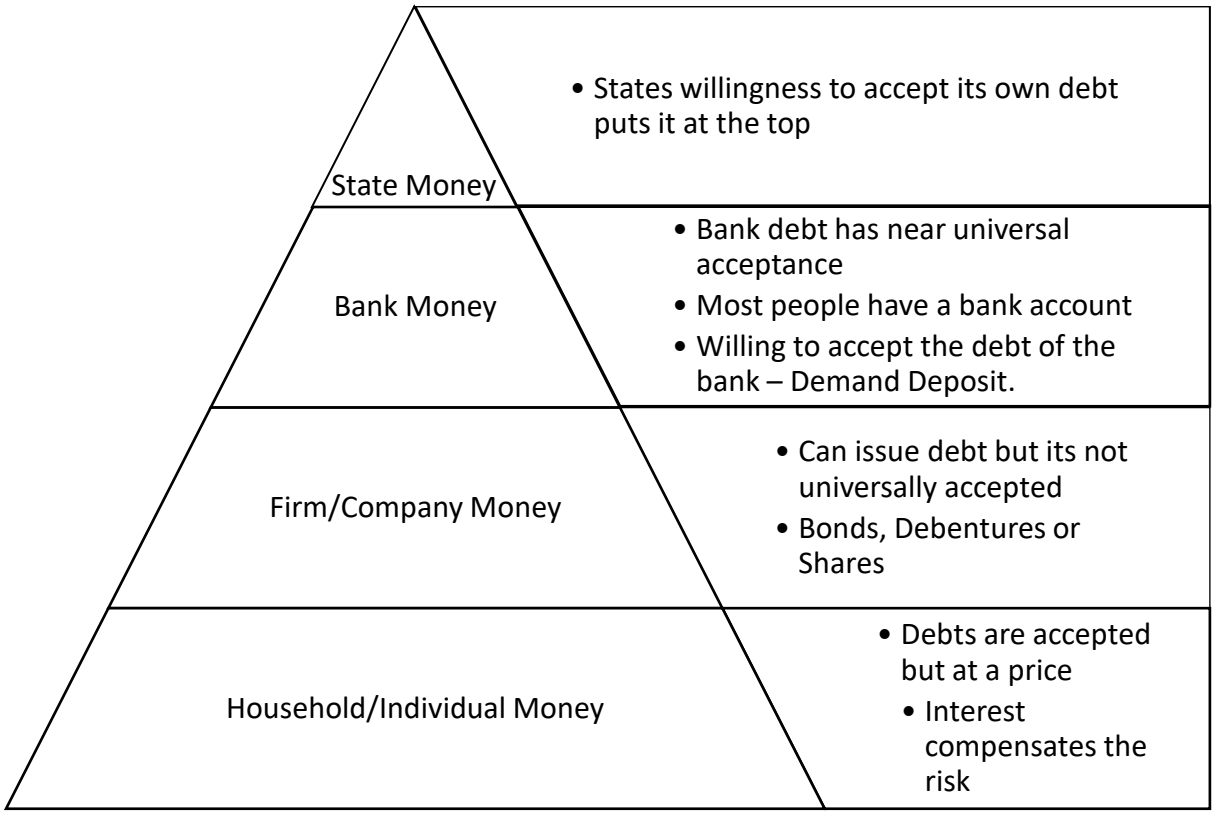
3.4.3. Bell's Hierarchy of Money

Bell analyses a hierarchy based on the works of economists, such as Minsky,[140] Foley[141] and Wray.[142] The hierarchy is formulated around chartalist theories of money; but Bell also assesses metallist theories,[143] and finds them to be a poor fit for modern forms of money. Bell traces metallist theory back to the functions of money identified by Aristotle, of which the medium of exchange function is the considered the most important, as this replaced barter, though Bell questions whether barter economies ever existed.[144] The principle issue identified by Bell is that paper money is not metal

[139] cf Bell (n107) .
[140] cf Minsky (n122).
[141] D. Foley, 'Money in Economic Activity' in M. Milgate and P. Newman (eds) *The New Palgrave: Money* (W.W. Norton, 1987).
[142] L. R. Wray, *Money and Credit in Capitalist Economics: The Endogenous Money Approach* (Edward Elgar, 1990).
[143] cf Bell (n114) at p.149.
[144] cf Bell (n114) at p.151.

backed which is contrary to metallist theory. Money has now become fiat money; money which will never be used as a commodity, as described by Kiyotaki and Wright.[145] As such, the metallist position is a difficult one to maintain. The hierarchy focuses on debt relationships; the further up the pyramid the more freely that type of debt is accepted.

Figure 3. Hierarchy of Money[146]



As Figure 3 demonstrates that the acceptability of debt increases the higher up the pyramid the money is. A pyramid is used here as this represents the decreasing number of parties which are active, the higher up the hierarchy they sit; only the state

[145] N. Kiyotaki and R. Wright, 'Acceptability, Means of Payment and Media of Exchange' in J. Eatwell, M. Milgate and P. Newman (eds) *The New Palgrave: Money* (W.W. Norton, 1987).
[146] Produced based on: S. Bell, 'The Role of the State and the Hierarchy of Money' (2001) 25 Cambridge Journal of Economics 149.

is present at the top of the hierarchy, whereas the population as a whole is at the bottom. The state is at the top, because all those below will accept state money. This is because state money is fiat money; this is money issued by the state, and in turn accepted by the state in payment of debts. As argued by the chartalist approach, the willingness of the state to accept its own money gives that money value through its usability. In accordance with credit theory, state money is the only money in the pyramid capable of being purely credit.

Bank money is second in the hierarchy; it is in this position because the acceptance of bank debt is near universal. The majority of people in the Western world have a bank account,[147] usually a demand deposit, and in doing so they accept the debt of the bank. State money takes the top place in the hierarchy, but the acceptability of bank debt is also near universal. The usability of bank money is also nearly that of state money; wherever card payment or cheques are accepted, bank money can be used, which is an ever-increasing number of places.

The third level of the hierarchy is labelled as firm or company money, this level of the hierarchy represents the debt of companies. In this level of the hierarchy the debt is significantly less usable than the top two levels; in order to spend, or redeem, credit held against a company, the holder would need the company to be able to repay the debt or find another buyer. It would be unusual for shares in a company to be used as a medium of exchange; at this level of the hierarchy the assets have a much lower liquidity than the higher levels.

[147] In 2010 it was estimated that 1 million people in the UK did not have a bank account: BBC News, ‘One million adults 'do not have a bank account' <http://www.bbc.co.uk/news/10277151> accessed 29 May 2015.

The lowest level of the hierarchy is household or individual money; this is personal debt. This level is the least liquid of the hierarchy and of the least value; in order for this debt to be accepted, interest is usually charged, and security sought in return. The theories of money may be applied to the hierarchy, while the hierarchy is produced predominately using chartalist theories,[148] metallist theories can be applied, and non-money assets may also be placed on the hierarchy. The hierarchy is particularly useful when it is difficult to identify something as state money; by providing a tiered system, commodities, assets, or concepts, which are not yet money, can be considered on the scale, against other similar assets. The hierarchy supports the idea that money is not a fixed concept and assets which are not money may become money if their usability increases, or the state begins to accept said asset as money.

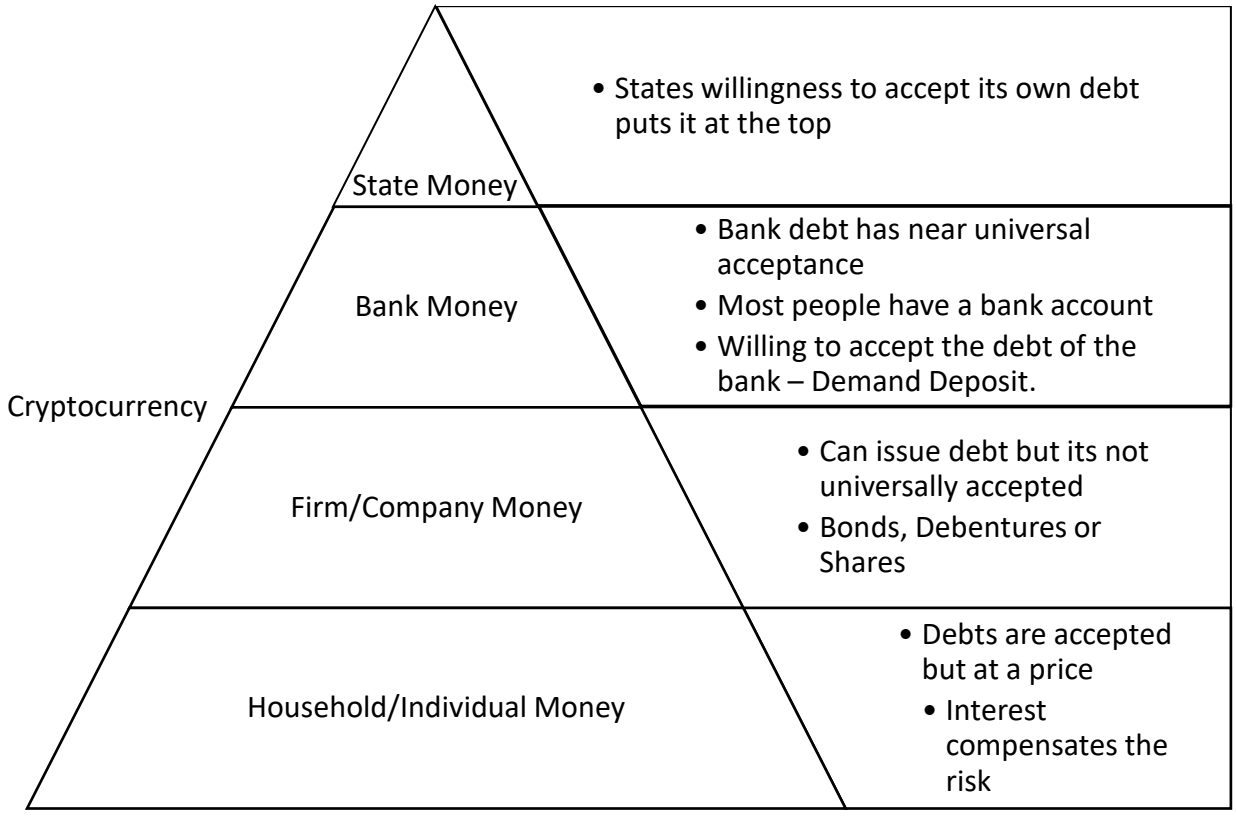
Chartalist theories of credit and debt relationships can clearly be seen, each level has a different class of debt, which may be used differently. There is a clear resemblance to the state theory of money as the state is at the top due to its ability to declare what it will accept as money, and give this value by accepting it in payment of debts. The social construction theory may be also be applied to the hierarchy and may also demonstrate how money may differ depending on the social situation. All money is valued in the currency dictated by the state, but the relative value of the money decreases as it progresses down the hierarchy and it is treated in a very different way.

[148] cf Bell (n114).

3.4.4. Placing Cryptocurrencies on the Hierarchy of Money

Cryptocurrencies satisfy of some of the functions of money, but not all of them, so they may near the middle of Bell's hierarchy, as approximated in Figure 4 below.

Figure 4. Placing Cryptocurrency on Bell's Hierarchy of Money[149]



Cryptocurrencies have no state to act as the driver of the money, there are no state debts to pay with cryptocurrencies. Therefore, cryptocurrencies cannot be placed as high on the pyramid as state money. Cryptocurrencies may be best placed as either company money or bank money. The level of usage and acceptance is not high enough to meet all of the criteria of bank money; it is not held by most people and cannot be said to have near universal acceptance, but it has the capacity to increase

[149] Produced based on: S. Bell, 'The Role of the State and the Hierarchy of Money' (2001) 25 Cambridge Journal of Economics 149.

in levels of acceptance as more people start to use it. Cryptocurrencies may be viewed as having higher liquidity than company money as it may be used as a medium of exchange in some circumstances. The liquidity of cryptocurrencies is higher than a bond or share, as a cryptocurrency is not linked to a company in the way a share or bond is, and can be bought as sold very quickly, without the need to produce share certificates and go through the required procedures with Companies House.[150] The most appropriate place on the pyramid for cryptocurrencies would be a low form of bank money or a high form of company money due to its limited acceptance, and its current use as an investment tool rather than as money.

3.5. Identifying Money

While theories of money attempt to explain what money is, they do not provide a clear mechanism for identifying money. The aim of this chapter is to consider whether cryptocurrencies, such as Bitcoins, are actually money. To determine this a variety of approaches may be taken. Using the state theory, it might first be appropriate to determine whether or not the state accepts the item as money, this would be the clearest indication; if the state says that it is money, or accepts it in payment of debts, then it is money. The second approach may then be to apply credit theory; a creditor and debtor relationship may be found in many situations, but in order for money to have been created, acceptance of the resulting credit must be high. As stated above, theories of money may be helpful in explaining money, but identifying it and tracing its origins still remains difficult, as such money is often determined by its principle functions.

[150] The reporting requirements regarding shareholders are found at: Companies Act 2006, ss112-144.

3.5.1. Function Based Definition

Hudson begins with Aristotle's three principles of money; a means of exchange, a measure of value, and a store of value.[151] Something is a means of exchange when it is used as consideration in a contract; most histories of money trace its roots back to being a solution to the shortfalls of bartering. One party may not always have an item, or service, that the other party wants in return for an item, or service; or the parties may bring items, or services, of different values. Money provides a solution to this; the person wishing to acquire an item may give money to the other party in return for that item. Money then also completes the second function, a measure of value, or unit of account; money is used to value items. Purchasing a cow for £100 demonstrates both of these functions; the £100 is used as the medium of exchange and the £100 also represents the value of the cow. Finally, value can be stored in money; an individual may gather and store their wealth in the form of money; £100 today will still be worth £100 in 10 years, the cow may have perished in this time.

3.5.2. Money in the eyes of the law

Legal definitions of money may differ from socio-economic definitions. The principle concern for the law is to identify what money is, and the rights the holder of money has; though there will obviously be some cross over, the theories discussed thus far seek to understand the development of money and provide an explanation for that development. While an understanding of the development of money is important to educate legal decisions; the principle concern of the law is to identify and provide

[151] A. Hudson, *The Law of Finance* (Sweet and Maxwell, 2013) at p.40.

guidelines, so as to ensure confidence and certainty for those that seek to rely on it.[152] Arora and Hudson both point to the case of *Moss v Hancock*[153] in which money is defined as:

> "*That which passes freely from hand to hand throughout the community in final discharge of debts and full payment for commodities, being accepted equally without reference to the character or credit of the person who offers it and without the intention of the person who receives it to consume it or apply it to any other use than in turn tender it to others in discharge of debts or payment for commodities.*"[154]

It is clear that money is not a fixed concept; *Moss v Hancock*[155] notably seeks to define money by its functions. Economists also seek to do this, but identify a few additional functions of money. While the law is primarily concerned with the medium of exchange, socio-economics recognises this as the main function, but also considers money as a store of value, and a unit by which value is determined. The function-based approach adopted by the law allows it to be flexible; the law does not prescribe what money is, and as such cryptocurrencies may have the potential to become money.

The EU definition of money is focused on the concept of legal tender, which the Euro is clearly identified as within the Treaty of the Functioning of the European Union[156] (TFEU), in which Article 128(1) stipulates the legal tender status of euro banknotes.[157]

---

[152] J. van Dunné 'On a clear day, you can see the continent - the shrouded acceptance of good faith as a general rule of contract law on the British Isles' (2015) 31(1) Const. L.J. 3.
[153] [1899] 2 QB III.
[154] ibid 116.
[155] ibid.
[156] Consolidated Version Of The Treaty On The European Union [2012] OJ C326/25.
[157] Article 128(1), Consolidated Version Of The Treaty On The European Union [2012] OJ C326/25.

The European Commission state that "*in the absence of an agreement of the means of payment, the creditor is obliged to accept a payment made in euro*"[158] but that "*contractual parties are free to use other official foreign currencies with legal tender status in the state of issuance*."[159] Additionally the Commission directly address 'virtual currency schemes', which includes cryptocurrencies, stipulating that although "*these are not official currencies and have no legal tender status, parties can agree to use them as private money without prejudice to the official currency*."[160] By categorising cryptocurrencies as private money, the EU makes it clear that cryptocurrencies will not be covered by monetary law,[161] so individuals use cryptocurrencies at their own risk and are not afforded the same protections as when using money.

3.5.3. Is Bitcoin Money?

As theories of money do not appear to be compatible with Bitcoin, a function-based analysis is adopted. The primary function of money, a medium of exchange, is satisfied in part; it is possible to purchase goods using Bitcoins, but they are not universally accepted. Universal acceptance, at least in a particular community, is a clear requirement identified in *Moss v Hancock.*[162] Taking the word 'community'; it is arguable that Bitcoin is accepted by an online community,[163] and therefore, for that community Bitcoin is a medium of exchange. This argument may be viewed as tenuous, it is potentially difficult to determine when a group of people form a

[158] European Commission, 'The euro as legal tender' <https://ec.europa.eu/info/business-economy-euro/euro-area/euro/use-euro/euro-legal-tender_en> accessed 10 October 2019.
[159] ibid.
[160] ibid.
[161] ibid.
[162] [1899] 2 QB III.
[163] B. Weber, 'Bitcoin and the legitimacy crisis of money' (2016) 41 Cambridge Journal of Economics 17 at 18.

community. For Bitcoin to be a form of money in the UK it would need to pass "*freely from hand to hand throughout the community*",[164] this is currently not the case; currently only 341 outlets accept Bitcoin in the UK. The counter argument to the issue of limited usability at present is that Bitcoin is still a developing concept, and that as it grows, acceptance will grow too. Society is not stationary, things change over time, and as Fox observes, the "*status of an asset as money is a social fact*"[165] and it is possible that Bitcoin may grow into a recognised from of money.

Bitcoin also faces issues when other functions of money are considered; it is difficult to argue that Bitcoin serves as a store of value, or a unit of account, due to its inconsistent value in relation to fiat currencies. Bitcoin is a store of value in that 1 Bitcoin will always be worth 1 Bitcoin, but the value of Bitcoin in relation to other currencies, such as the US Dollar, will mean that the real value of that Bitcoin may vary considerably. It is accepted that all currencies will vary in value, the exchange rates are determined by market forces,[166] but the size of these value changes are often small; the changes in the value of Bitcoin are often much more extreme. This is clear when Bitcoin is compared to major fiat currencies. In January 2013, 1 Bitcoin was worth US$13.28,[167] but by 4th December 2013, Bitcoin reached a then record high value of $1230.69 per Bitcoin.[168] By 18th December, half of that value had been lost and 1 Bitcoin was worth $553.48.[169] Despite recovering to $995.83 by 11th January

[164] *Moss v Hancock* [1899] 2 QB III at 116.
[165] cf Fox (n85) p17.
[166] C. A. E. Goodhart, 'What is the essence of money?' 2005 29 Cambridge Journal of Economics 817 at 823.
[167] XE, 'USD per 1 XBT' <http://www.xe.com/currencycharts/?from=XBT&to=USD&view=2Y> accessed 24 September 2019.
[168] ibid.
[169] ibid.

2014,[170] Bitcoin steadily lost value over 2014 and the first 5 months of 2015, it was worth just $229.24 on 1st June 2015.[171] The latter half of 2015 saw Bitcoin regain value, finishing the year at $432.40,[172] and 2016 saw Bitcoin retain its value until May before rising to $763.54 in June, then falling sharply to $503.48 in August. Bitcoin continued to increase in value for the rest of 2016, finishing at $963.50. 2017 saw Bitcoin surpass its record value of 2013, reaching $1275 on 3rd March, dipped to £929.38 by 24th March and then began to rise to new highs, reaching $2381.55 in May, and then steadily rising to its record value of $19,783 in December 2017.[173] Over 7 years the value of Bitcoin varied from $13.28 to $19,783, a difference of $19,769.72 with many abrupt changes up and down. In the same period, the GBP experienced a low value of $1.20 in April 2015[174] and a high value of $1.72 in July 2014,[175] a difference in value of $0.52. Similarly, to GBP, the Euro only varied in value by $0.35.[176] The swings in value prevents Bitcoin from acting as a store of value; it is not possible to be confident about which direction the value will move, or how quickly it will change.

The functions of money do not operate independently; for something to be a functioning unit of account it must also be a store of value, or that measure of value will be inconsistent. The unit of account function allows for the value of an item to be immediately identified; for example, a jumper is worth £10, the pounds are serving as a measure of the value of that jumper. In the case of Bitcoin this is not reliable as the

[170] ibid.
[171] ibid.
[172] ibid.
[173] D. Morris, 'Bitcoin Hits a New Record High, but Stops Short of $20,000' (Fortune.com, 17 December 2017) <https://fortune.com/2017/12/17/bitcoin-record-high-short-of-20000/> accessed 29 July 2020.
[174] XE, 'USD per 1 GBP' <http://www.xe.com/currencycharts/?from=GBP&to=USD&view=5Y> accessed 23 September 2019.
[175] ibid.
[176] ibid.

value of goods in Bitcoins will constantly changes as the value of Bitcoin changes. An issue for Bitcoin in being a store of value is its lack of backing; Bitcoin is not valued against anything, whereas currencies such as the British Pound are valued against a national economy. The value of the pound rises and falls based on the success of the UK economy, amongst other things;[177] there is no such economy which Bitcoin is valued against, it is simply based on trust. While the supporters of Bitcoin will point to the inability to control Bitcoin being an assurance for its users,[178] the majority of individuals do not understand Bitcoin, so their trust would have to be blind; this is not common when money is concerned.

As Bitcoin does not satisfy all of the functions of money, it is difficult to conclude that it is money in same way as fiat money is money; based on the hierarchy of money it would not be possible to have Bitcoin at the top. It may be more appropriate to view Bitcoin as company money or bank money; it could be considered a company money of relatively high liquidity, or a bank money with comparably low liquidity; with the potential to become as usable as other bank money as acceptability increases. This analysis has focused on Bitcoin as it is the most prominent cryptocurrency, the shortfalls in Bitcoin being money are applicable to all cryptocurrencies. In many cases, the limitations preventing Bitcoin being money are even more evident in alternative cryptocurrencies, with even lower levels of acceptance and more volatile changes in value.

[177] The value of GBP may rise and fall based on events on the national and international platform, changes of government or announcements of budgets may influence the value of GBP as this may stimulate certain trading.
[178] Coin Desk, 'What is Bitcoin' <http://www.coindesk.com/information/what-is-bitcoin/> accessed 23 June 2015.

3.6. Chapter Summary

Cryptocurrencies require unique attention due to their popularity, and the levels of anonymity they provide. This chapter identifies cryptocurrencies as a specific class of virtual currencies, their key characteristics being that they are decentralised, as they rely on cryptography and blockchain technology, and they are capable of being exchanged for fiat currencies. Other forms of virtual currencies, such as those within virtual worlds, are not without legal issues, but the value of cryptocurrencies and their interaction with the traditional financial system makes them the most attractive form of virtual currency for money laundering, as will be demonstrated in chapter four, and thus the focus of this thesis.

Theories of money fail to provide a definitive answer to the question of whether cryptocurrencies are money, but these theories do demonstrate that money is clearly not a static concept; it is subject to change and is developed by states and society. Chartalist theories of money appear to best describe modern fiat money, and these theories have some application to cryptocurrencies, but it is not a perfect fit, as the state's role is nearly completely removed in cryptocurrencies. The reduced role of the state in metallist theories of money is present in cryptocurrencies, but there is no intrinsic value to cryptocurrencies, as is required by both orthodox and Marxist theories of money. Assessing cryptocurrencies against the functions of money provides a useful indication of whether something may be money, but this is not conclusive as although cryptocurrencies act as a medium of exchange, the volatility in value means cryptocurrencies cannot act as a store of value or a unit of account. Considering that money is a social concept and is subject to change, the hierarchy of money proposed by Bell is a useful measure of where an asset sits in relation to state money, which is

universally accepted credit. An asset's position on the hierarchy is also not static and may be subject to change as its usability increases or decreases. Based on cryptocurrencies current usage and acceptance, cryptocurrencies cannot be placed as high as state money, nor can it be as high as bank money. Due to being more readily accepted than company shares or vouchers, cryptocurrencies sit towards the top of 'company money', with the potential to move up the hierarchy depending on future treatment in society.

Although not accepted as money, the transferability of cryptocurrencies, into fiat currencies, means there is potential for money laundering to take place. It would most likely take place during the layering stage of the money laundering process; a launderer may purchase Bitcoins using US$, and then be able to undertake a number of transactions via Bitcoin wallets which will be difficult to trace as only serial keys are published in the blockchain. The next chapter analyses the history of money laundering and efforts to combat it, by observing the development of this area of law, predictions and recommendations can be made as to how best address the threat posed by cryptocurrencies.

Chapter 4. Money Laundering

> *"Crime has become increasingly international in scope, and the financial aspects of crime have become more complex due to rapid advances in technology and the globalization of the financial services industry.*"[1]

4.1. Outline

In this chapter the crime of money laundering will be defined, the history of the term will be considered, as will the concept of money laundering, and what criminals aim to achieve from the practice. In defining money laundering, the process by which money is laundered will be explained, and various techniques will be outlined. It is clear from successful prosecutions in the United Kingdom (UK) and the United States (US), that money launderers are utilising cryptocurrencies. In order to understand the likely trajectory of anti-money laundering (AML) regulation, a short history of AML measures will be provided, where themes are identified in the development of AML regulation, introducing the key developments, legislation, and international bodies as they become relevant. The chapter goes on to analyse the responses of international organisations to the money laundering threat posed by cryptocurrencies, specifically the UN, the Financial Action Task Force (FATF), and the European Union (EU). It is observed that the role of the UN in relation to setting international best practice for AML regulation has receded, as the FATF and the EU have taken the lead role in the 21st century. The FATF and the EU both propose the AML regulation of cryptocurrency

[1] J. McDowell and G Novis, 'The Consequences of Money Laundering and Financial Crime' (2001) 6(2) Economic Perspectives 6.

service providers at the point of intersection with fiat currencies and the traditional financial system, which is a first step in addressing the money laundering threat of cryptocurrencies, but ignores the wealth of information available through publicly available blockchains.

4.2. Concept of Money Laundering

Money laundering is the process by which the proceeds of crime are made to look legitimate; "[m]*ost simply, it is the process by which criminals cleanse the fruits of their criminal labours.*"[2] Stokes refers to Lilly's definition; "*the process whereby the identity of dirty money that is the proceeds of crime and the real ownership of these assets is transformed so that the proceeds appear to originate from a legitimate source.*"[3] The aim of money laundering is to conceal, hide and disguise the origins of the illicit money, and to enable the money launderer to enjoy the benefits of it without reproach. Money laundering simply refers to concealing the source of money due to its criminal origins. As the task is such a broad one, money laundering may take many forms and may utilise anything that has value.[4]

Claimed to be the third biggest industry in the world by Robinson;[5] money laundering is an international problem, but estimating the extent of the issue has proven

[2] R. Stokes, 'Virtual money laundering: the case of Bitcoin and the Linden dollar' (2012) 21(3) Journal of Money Laundering Control 221 at 222.
[3] P. Lilley, *Dirty Dealing: The Untold Truth about Global Money Laundering* (London, Kogan Page, 2006).
[4] N. Ryder, 'The Financial Services Authority and Money Laundering: A Game of Cat and Mouse' (2008) 67(3) Cambridge LJ 635.
[5] J. Robinson, *The Laundrymen* (London, Pocket Books, 1995).

complicated and produced conflicting results. For example, the United Nations Office on Drugs and Crime (UNODC) estimated 2.7% of global GDP[6] (or US$1.6 trillion) was being laundered in 2009,[7] which is the figure the FATF use.[8] This correlates with the International Monetary Fund (IMF)[9] estimate in 1998, which suggested money laundering could be valued at 2-5% of global GDP.[10] These estimates differ from other global estimates collated by Unger,[11] who found wide ranging estimates, such as $45 and $280 billion by Reuter and Greenfield,[12] to $2.85 billion by Walker and Unger.[13] As well as global estimations, the individual jurisdictions in the case studies of this thesis also attempt to estimate the value of illegal money laundered their respective territories. The Australian Transaction Reports and Analysis Centre (AUSTRAC) estimates "*AUD200 billion is laundered in the Asia-Pacific region*";[14] in the UK the Financial Conduct Authority (FCA) estimate that "*£10billion of illicit funds*"[15] passes through the UK financial system; and in the United States (US) the Treasury believes "*about $300 billion is generated annually in illicit proceeds.*"[16] While these estimations

[6] Gross Domestic Product: "*an aggregate measure of production equal to the sum of the gross values added of all resident, institutional units engaged in production (plus any taxes, and minus any subsidies, on products not included in the value of their outputs).*" Organization for Economic Co-operation and Development, 'Gross Domestic Product' <http://stats.oecd.org/glossary/detail.asp?ID=1163> accessed 15 June 2015.
[7] United Nations Office on Drugs and Crime, 'Illicit Money: How Much is Out There?' <http://www.unodc.org/unodc/en/frontpage/2011/October/illicit-money_-how-much-is-out-there.html> accessed 15 June 2015.
[8] Financial Action Task Force, 'About Us' <http://www.fatf-gafi.org/pages/aboutus/whatwedo> accessed 09 June 2015.
[9] International Monetary Fund, 'Money Laundering: The Importance of International Countermeasures' <http://www.imf.org/external/np/speeches/1998/021098.htm> accessed 15 June 2015.
[10] ibid.6
[11] B. Unger, 'Can Money Laundering Decrease?' (2013) 41(5) Public Finance Review 658 at p.663.
[12] P. Reuter and V.A. Greenfield, 'Measuring Global Drug Markets: How Good Are the Numbers and Why Should We Care about Them?' (2001) 2(159) World Economics 73.
[13] J. Walker and B. Unger, 'Estimating Money Laundering: The Walker Gravity Model' (2009) 5(821) Review of Law and Economics 53.
[14] AUSTRAC, 'Introduction to Money Laundering' <https://michaelsmithnews.typepad.com/files/money-laundering.pdf> accessed 5 September 2019.
[15] Financial Conduct Authority, 'Anti-Money Laundering Annual Report 2012/13' <http://www.fca.org.uk/static/documents/anti-money-laundering-report.pdf> accessed 15 June 2015.
[16] United States Treasury, 'National Money Laundering Risk Assessment' <https://www.treasury.gov/resource-center/terrorist-illicit-

may be helpful in justifying a concerted effort to combat money laundering, each of these estimations is likely to be inaccurate. This is because each calculation has been produced using a different methodology and based on different definitions of the key terms. Further to this, the secretive nature of money laundering means reliable records are unavailable, and each study dedicated to calculating the extent of money laundering will make different assumptions from the data available to them. Unger and Busuioc identify that differing definitions of money laundering, the proceeds of different predicate offences being included, and the use of different statistical methods, lead to "*controversy between the purists, people who want to measure and model precisely, and the innovators – those who try to measure the immeasurable, even if they run the risk of being criticised.*"[17] Writing as a purist under Unger's distinction, Thomas criticised money laundering measurements, and other measurements from the criminal economy,[18] as "*measurement without theory.*"[19] Estimations have provided larger and larger figures, which Unger puts this partly down to the number of predicate offences increasing as AML laws have developed.[20] Increasing the number of offences counting as a predicate offence for money laundering will naturally lead to a larger amount of money in illicit gains being produced, and needing to be laundered. The issues in quantifying the extent and impacts of money laundering are not limited to monetary terms, other impacts should be considered, money laundering is not a victimless crime. Unger notes that while there are no direct victims of money

finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf> accessed 5 September 2019.

[17] B Unger, *The Scale and Impacts of Money Laundering* (Edward Elgar, Cheltenham, 2007) at p.32

[18] There is no agreed term for the criminal economy; it may also be referred to as the 'black economy', or the 'hidden economy'. It refers to transactions completed in secret to avoid detection by the relevant authorities.

[19] J. Thomas, 'Quantifying the Black Economy: 'Measurement Without Theory' Yet Again?' (1999) 109(456) The Economic Journal 381 at p.381.

[20] cf Unger (n11) at p661-662.

laundering, "*there are always secondary victims such as family, friends, acquaintances, and society at large.*"[21]

4.3. Impacts of Money Laundering

McDowell and Novis identify the money laundering has both economic and social consequences.[22] As the scale of money laundering is impossible to calculate, it is also impossible to discern the impacts, as some of the impacts are also naturally difficult to measure, and may be impacted by other factors, such as damage caused to the reputation of an economy. Reputational damage may lead to the reduced investment from legitimate businesses, which do not wish to be associated with such an economy, and an increase in those wishing to launder their money in the effected economy, as they see such an economy as an appealing place to do so. Both of these potential consequences are effects which cannot be measured, are therefore impossible to quantify accurately. Further impacts of money laundering include legitimate businesses being unable to compete with those funded by illegal money, as the front businesses may have substantial illicit funds behind them and allowing them to offer goods and services at lower prices than legitimates businesses.[23]

Money laundering reduces the integrity of the financial services industry; money launderers may move their money unexpectedly and this may cause liquidity strains for financial institutions. McDowell and Novis highlight that the BCCI and Bearings

[21] B. Unger & D. v.d. Linde, *Research Handbook on Money Laundering* (Edward Elgar, Cheltenham, 2013) at p.20
[22] cf McDowell and Novis (n1).
[23] cf McDowell and Novis (n1).

Bank scandals in the 1990s "*had significant criminal or fraud components*"[24] as causal factors, and such scandals persist to the present day, as the 2012 US senate investigation into HSBC demonstrates.[25]

Privatisation of services may be affected by money laundering;[26] should one of the companies bidding for government contracts be backed by illicit funds it will hold an advantage over the legitimate bidder. Tax revenues will also be reduced by money laundering which negatively affects taxpayers.[27] Given the estimates of the scale of money laundering McDowell and Novis also argue that the control of economic policy may also be reduced,[28] money laundering may distort markets and increase the threat of monetary instability.

The prevalence of money laundering may increase the occurrence of other crimes; it provides "*fuel for drug dealers, terrorists, illegal arms dealers, corrupt public officials, and others to operate and expand their criminal enterprises*."[29] Morris-Cotterill noted in 1996 that "*governments and society are recognising their inability to control drug abuse and that the only way to stop or reduce the rate of increase of crime is to try to prevent the criminal spending his or her money*."[30] An increase in corruption has a generally detrimental effect on society; in "*extreme cases, it can lead to the virtual*

[24] cf McDowell and Novis (n1) at p.7.
[25] US Senate, 'HSBC Exposed U.S. Financial System to Money Laundering, Drug, Terrorist Financing Risks' <https://www.hsgac.senate.gov/subcommittees/investigations/media/hsbc-exposed-us-finacial-system-to-money-laundering-drug-terrorist-financing-risks> accessed 05 August 2016.
[26] cf Unger and Linde (n21) at p.20
[27] M. M. Gallant, 'Money Laundering Consequences: Recovering Wealth, Piercing Secrecy, Disrupting Tax Havens and Distorting International Law' (2014) 17(3) JMLC 296.
[28] cf McDowell and Novis (n1).
[29] cf McDowell and Novis (n1).
[30] N. Morris-Cotterill, 'The International Effect of Money Laundering Laws' (1996) 4(1) Journal of Financial Regulation & Compliance 67 at 68.

take-over of legitimate government."[31] The impacts of money laundering are "*magnified in emerging markets*."[32] The prevalence of money laundering may make organised crime more appealing and lead to increases in such crime, at present this may lead to increased people smuggling, in light of social unrest and the migrant crisis facing the EU, the importance of investigating the finances of such criminals is argued by Kluczyński.[33]

A further justification for combatting money laundering, is that the money, or assets, may be evidence of the predicate crimes; a key piece of evidence in securing a conviction for a crime might be the possession of the proceeds of that crime. As has already been stated, money laundering is the process of disguising the origins of illicit money, the purpose of this is not only to be able to enjoy the use of the money, it is also to distance the criminal from the original offences. If this money can be identified, and traced back to the offender then it will not only serve to aid in a money laundering conviction, but also aid in obtaining a conviction for the original offence which produced the illegal assets.

4.4. Can Cryptocurrencies Be Used to Launder Money?

Cryptocurrencies are being used to launder money, as demonstrated by examples from the UK and the US, such as the conviction of Ross Ulbricht for his role in creating

[31] cf McDowell and Novis (n1).
[32] cf McDowell and Novis (n1).
[33] M. Kluczyński, 'Prevention of Money Laundering in the Fight Against Human Trafficking and Smuggling of Migrants' (2013) 5(2) Internal Security 83.

Silk Road.[34] Ulbricht is not the only individual to have be convicted for money laundering using cryptocurrencies, numerous convictions have been announced through US Department of Justice press releases with cases varying from international gangs[35] to one-man operations.[36] The appeal of using cryptocurrencies was assessed by Irwin et al,[37] who considered the factors a money launderer may consider when deciding how to clean their money. The key factors considered were; ease, time, amount laundered, cost, risks mitigated, and chances of detection.[38] The ideal scenario for a money launderer would be for the proceeds of a crime to be quickly and easily cleaned, without reducing the value and avoiding detection, this is unrealistic, and each method for laundering money will involve a balancing of these factors.[39] Irwin *et al* found that each money launderer will have their own preferences in their techniques, but that "*the more techniques that are used, the more cash can be successfully laundered or concealed*."[40] Cryptocurrencies provide an additional technique to launder the proceeds of crime, which is clearly being utilised by criminals.

In terms of ease, using cryptocurrencies does not require any great expertise, basic computer literacy and access to a cryptocurrency exchange being the only hurdles to

[34] United States v. Ulbricht, 858 F.3d 71, 82–83 (2d Cir. 2017).
[35] Department of Justice, U.S. Attorney's Office Western District of Washington, 'Multi-State International Drug Trafficking Organization Targeted in 18-Month Investigation' (Washington, United States, 6 December 2018) <https://www.justice.gov/usao-wdwa/pr/multi-state-international-drug-trafficking-organization-targeted-18-month-investigation> accessed 04 September 2019.
[36] Department of Justice, U.S. Attorney's Office Central District of California, '"Bitcoin Maven" Sentenced to One Year in Federal Prison in Bitcoin Money Laundering Case' <https://www.justice.gov/usao-cdca/pr/bitcoin-maven-sentenced-one-year-federal-prison-bitcoin-money-laundering-case> accessed 04 September 2019.
[37] A. S. M. Irwin, R.K.K. Choo, and L. Liu, 'An analysis of money laundering and terrorism financing typologies' (2012) 15(1) JMLC 85.
[38] ibid at 100.
[39] ibid at 99.
[40] ibid at 105.

overcome to make use of cryptocurrencies.[41] Once using cryptocurrencies, the level of difficulty does not increase, making transfers simply requires knowing the address of the intended recipient.[42] Cryptocurrencies are also very fast, Bitcoin transactions take approximately 10 minutes on average,[43] as this is the time between blocks being created.[44] Blocks are created when the proof-of work is completed, at which point all transactions since the previous the block was created are verified.[45] While it takes up to 10 minutes to verify a transaction, this does not preclude a user from making more than one transaction in the same 10-minute time frame. In theory, many transactions could take place in a very short period of time, distancing the money from its origin. Transactions in cryptocurrencies incur small fees which go to the miner who produced the block, and some fees may be incurred when using a cryptocurrency exchange, similar to that incurred when exchanging fiat currencies.[46]

Using cryptocurrencies does come with some risks, while the speed of the transactions and the potential lack of dependency on others to assist in operation both reduce the risks, the biggest risk in using cryptocurrencies is the volatility in value. If the value of a cryptocurrency crashes while the launderer has their funds in that currency, they will suffer losses to the value of their assets when they convert the money back into a fiat currency.

---

[41] Numerous guides exist online to assist beginners such as : Bitcoin, 'Getting started with Bitcoin' <https://bitcoin.org/en/getting-started> accessed 14 October 2019 and Cryptorunner, 'How to Get Started with Bitcoin' <https://cryptorunner.com/get-started-with-bitcoin/> accessed 14 October 2019.
[42] Bitcoin, 'Getting started with Bitcoin' <https://bitcoin.org/en/getting-started> accessed 14 October 2019.
[43] Bitcoin Wiki, 'Research' <http://bitcoin.org/bitcoin.pdf> accessed 10 June 2015.
[44] The details of the how Bitcoin works, and transaction times is set out in the initial paper: Bitcoin Wiki, 'Research' <http://bitcoin.org/bitcoin.pdf> accessed 10 June 2015.
[45] Bitcoin Wiki, 'Research' <http://bitcoin.org/bitcoin.pdf> accessed 10 June 2015 at p.8.
[46] Information on potential fees can be found through the exchange or platform used.

Accurate estimates of the amount of money laundered through cryptocurrencies are not available, but Europol have predicted that 3-4% of the £100bn in illicit proceeds in Europe is through cryptocurrencies, and that is "*growing quite quickly*."[47] By using a cryptocurrency, the chances of detection may be reduced as the majority of cryptocurrency transactions are not be subject to reporting requirements. The only cryptocurrency transactions which are subject to reporting requirements are those that go through cryptocurrency exchanges, as stipulated by FinCEN in the US,[48] and in accordance with the Anti-Money Laundering and Counter-Terrorism Financing Act 2006[49] in Australia. Currently no reporting requirements are implemented in the UK, but this will change in 2021 once amendments to the 2017 Money Laundering Regulations, enacted to comply with the 5th Anti-Money Laundering Directive, come into force.[50] It is unclear exactly how the UK will implement the regulation required by the Directive, but the FCA has stated it will go further than the requirements of the Directive,[51] which is in line with the insights that can be drawn from the way the UK

[47] BBC News, 'Criminals hide 'billions' in crypto-cash – Europol' (12 February 2018) <https://www.bbc.co.uk/news/technology-43025787> accessed 08 October 2019 and Hannah Murphy, 'Europol meets cryptocurrency exchanges to thwart criminals' *Financial Time* (London, 19 June 2018) <https://www.ft.com/content/9430a3b0-73d4-11e8-b6ad-3823e4384287> accessed 14 October 2019.

[48] FinCEN, 'Guidance - FIN-2013-G001 - Issued: March 18, 2013 - Subject: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies' <https://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf> accessed 06 August 2019 at p2.

[49] Anti-Money Laundering and Counter-Terrorism Financing Act 2006.

[50] Regulatory Policy Committee, 'Transposition of the Fifth Anti-Money Laundering Directive HM Treasury' (London, 16 January 2020) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/863735/2020-01-16-RPC-HMT-4432_1_-Transposition_of_the_Fifth_Anti-Money_Laundering_Directive.pdf> accessed 28 July 2020.

[51] T. Chambers, 'Unstable coins: cryptoassets, financial regulation and preventing financial crime in the emerging market for digital assets' (Financial Conduct Authority, London, 06 March 2020) <https://www.fca.org.uk/news/speeches/unstable-coins> accessed 10 November 2020.

has implemented AML measures that have been developed domestically and internationally since the 1960s.

4.5. History of Anti-Money Laundering Law

Here the development of AML law will be chronicled, dating AML measures back to the UN's attempts to combat the international drugs trade. It is important to understand the development of AML laws so as to better understand the current law, and to be able to better predict the potential future developments of AML laws. By tracing the developments of the fight against money laundering, themes may be observed and the motivations for the developments may also be considered by assessing the key events from the time. Once the development of AML laws has been assessed, and the factors that influenced this development have also been considered, it will be possible to discuss whether the risks posed by cryptocurrencies will lead to reforms of AML laws. Each decade, from the 1960s onwards, is taken in turn so that the key developments in national and international approaches can be seen.

4.5.1. 1960s

Leading on from the 1939 League of Nations Convention, the UN's Single Convention on Narcotic Drugs 1961[52] remained focussed on the production, and trade of drugs. Article 37 stipulated that "drugs, substances and equipment"[53] should be confiscated, but does not explicitly mention money, or money laundering. While the UN was still

[52] Single Convention on Narcotic Drugs (adopted 30 March 1961, entered into force 13 December 1964) 520 UNTS 151 (Single Convention on Narcotic Drugs).
[53] ibid art.37.

focussed on drugs, the US was concerned about money laundering. Doyle dates the beginning of US attempts to tackle money laundering to the late 1960's;[54] citing a Department of Justice guide to the Bank Secrecy Act[55] which identifies strong bank secrecy laws of foreign jurisdictions creating "a legal climate that is optimal for the laundering of "dirty" money."[56]

4.5.2. 1970s

In 1970 the US enacted the Bank Secrecy Act 1970 (BSA 1970) which Ryder identifies as the "*central tenant of the US AML policy*,"[57] as it introduced record keeping requirements on financial institutions and introduced obligatory currency transaction reports where the transaction value exceeded $10,000.[58] As the name suggests the BSA 1970 was introduced to tackle the bank secrecy concerns which developed in the late 1960's. The aim of the Act "*was to deter and prevent the use of secret foreign bank accounts for tax fraud and their use to screen from view a wide variety of criminally related financial activities, and to conceal and cleanse criminal wealth.*"[59] Also enacted in 1970 was the Racketeering Influenced and Corrupt Organizations Act 1970 (RICO 1970),[60] which aimed to "*restrict the growth of criminal enterprises and,*

[54] T. Doyle, 'Cleaning Up Anti-Money Laundering Strategies: Current FATF Tactic Needlessly Violate International Law' (2002) 24 Houston Journal of International Law 297.
[55] Bank Secrecy Act, Pub. L. 91–508
[56] C. W. Blau Et Al., Investigation and Prosecution of Illegal Money Laundering: A Guide to The Bank Secrecy Act, U.S. Department of Justice, Criminal Division (1983) at p.124.
[57] N. Ryder *Money Laundering - An Endless Cycle?: A Comparative Analysis of the Anti-Money Laundering Policies in the United States of America, the United Kingdom, Australia and Canada* (Routledge, London, 2012) at p.41.
[58] ibid.
[59] Statement of Eugene T. Rossides Former Assistant Secretary of the Treasury for Enforcement and Operations Senate Hearing on Foreign Bank Secrecy June 9, 1970 available: FinCEN, 'Annual Report 2010' <https://www.fincen.gov/news_room/rp/files/annual_report_fy2010.pdf> accessed 22 September 2019 at p.16.
[60] Pub. L. 91-452, 18 USC Part 1 Chapter 96 §1961-1968.

secondly, to thwart the reintegration of their proceeds of crime,"[61] and was part of the Organized Crime and Control Act 1970. The BSA 1970 and the RICO 1970, while closely linked to money laundering, were not directly concerned with combatting money laundering. The reporting requirements of the BSA 1970 did not apply to money laundering as noted by Ryder, and the offence of money laundering[62] was not created by the BSA 1970 or the RICO 1970. However, the BSA does represent the first measures attempting to identify money laundering, even if it was via bank secrecy law; this is significant, as by seeking to identify money laundering the US demonstrated a will to pursue criminal gains, rather than simply enact offences. Reporting requirements may be viewed as the origins of detecting and combatting money laundering in the US. Additionally, the RICO 1970 attempted to widen the concept of 'proceeds of crime', this was subsequently limited in the US Supreme Court in *United States v Santos*,[63] but demonstrated the willingness of the US to broaden money laundering law to crimes not involving drugs, despite not yet coining the term 'money laundering'.

1971 saw the creation of the UN Convention on Psychotropic Substances[64] which, along with the Single Convention on Narcotic Drugs 1961, was criticised for being ineffective as it did not target the benefits of the drugs trade or punish those involved.[65] The weaknesses of the 1961 and 1971 Conventions are laid out by Sproule and St-

[61] cf Ryder (n57) at p.65
[62] cf Ryder (n57) at p.41.
[63] 128, S. Ct. 2020, 2025, 2031 (2008) affirming 461 F. 3d 886 (7th Cir. 2006)
[64] Convention on Psychotropic Substances (adopted 21 February 1971, entered into force 16 August 1976) 520 UNTS 1019 (Convention on Psychotropic Substances)
[65] D. P. Stewart, 'Internationalizing the War on Drugs: The UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances' (1990) 18 Denver Journal of International Law and Policy 387 at p.390.

Denis, who state that, despite the UNs "*aim of reducing the drug trafficking problem, they are inadequate instruments to confront the various aspects of the problem*"[66] that existed. Comparing the UN's approach to the US, it can be seen that the US created offences but also put in place measures by which the offences may be utilised. The US recognised that in order to combat money laundering, there needed to be prescribed measures for financial institutions to follow in order to detect criminal activity; law enforcement agencies are not in a position to detect and pursue money laundering without information from financial institutions. In recommending offences, the UN was only half addressing the problem, the offences were "*inadequate instruments to confront the various aspects of the problem*"[67] because they did not provide a framework for detecting and enforcing the offences.

The UN was not the only international body concerned by money laundering, the EU, formerly known as the European Economic Community, began addressing the issue of money laundering in the 1970's. The EU began addressing money laundering through the European Committee on Crime Problems (CDPC), which created a Select Committee to assess the transfer of criminal proceeds between Member States.[68] The recommendations of the CDPC Select Committee were not published until 1980.

[66] D. W. Sproule and P. St-Denis, 'The UN Trafficking Convention: An Ambitious Step' (1989) 27 Canadian Yearbook of International Law 263 at p.265.
[67] ibid.
[68] cf Ryder (n57) at p.18.

4.5.3. 1980s

The EU Committee of Ministers approved of the recommendations of the CDPC Select Committee in 1980, these recommendations included the introduction of identity checks when customers open accounts, rent safe deposits, or when large cash and inter-bank transactions take place.[69] This would have been an innovative move at the time; such measures are commonplace in modern day, but the EU did not adopt the recommendations.[70] Gilmore states that despite the fact that many of the proposed measures are "*now generally regarded as central aspects of any comprehensive anti-money laundering programme, the 1980 initiative failed to find a receptive audience*"[71] and as such were not implemented at that time. This was a missed opportunity by the EU to greatly improve AML approaches. In 1981 Australia made its first attempt to address the issue of international drug trafficking through the Stewart Royal Commission, which was completed in 1983,[72] it was officially called the Royal Commission of Inquiry into Drug Trafficking,[73] thus it was focussed on the drugs trade instead of solely on money laundering.[74]

[69] Council of Europe, Committee of Ministers Measures against the transfer and the safekeeping of funds of criminal origin – recommendation no. R (80) 10. This was adopted by the Committee of Ministers of the Council of Europe on 27 June 1980 available: Council of Europe, 'Resolutions and recommendations elaborated under the authority of the CDPC' <https://www.coe.int/en/web/cdpc/resolutions-recommendations > accessed 25 September 2019.
[70] cf Ryder (n57) at p.18.
[71] W. Gilmore, *Dirty Money – The Evaluation of International Measures to Counter Money Laundering and the Financing of Terrorism* (Council of Europe, Brussels, 2004) at p161.
[72] E. Hunter, 'Australia', in M Simpson, N Smith and A Srivastava (eds), *International Guide to Money Laundering Law and Practice* (Haywards Heath, Bloomsbury Professional, 2010) at p.255.
[73] D. G. Stewart, *Royal Commission of Inquiry into Drug Trafficking*, (Canberra, Australia Government Printing Services, 1983).
[74] cf Hunter (n72)at p.255.

1986 saw the UK and the US make money laundering a criminal offence; the US was first with the Money Laundering Control Act 1986,[75] followed by the UK by virtue of the Drug Trafficking Offences Act 1986[76] (DTOA 86). The DTOA 86 was enacted in light of decision in *R* v *Cuthbertson*[77] which highlighted the limitations of the Misuse of Drugs Act 1971,[78] which restricted confiscation to the "*physical items used to commit the offence*",[79] demonstrating that the law needed wider drafting to address the reality of organised crime. In light of the Cuthbertson decision, the Hodgson Committee recommended a broadening of what should be considered the proceeds of crime, and therefore the way in which money laundering was addressed.[80] The Drug Trafficking Offences Act 1986 can be seen as the birthplace of suspicious activity reports as it created the offence of "*assisting another to retain the benefit of drug trafficking*"[81] which made assisting someone while "*knowing or suspecting*"[82] them to be an offender, and failing to report it, a criminal offence. The introduction to suspicious activity reports is important as it demonstrates the origins of preventative measures requiring the expertise of professionals from industries vulnerable to money laundering. Until this point the common approach had been centred on criminalisation, this was a solely reactive approach, the crime and the money laundering had to have been committed before any action could be taken. Suspicious activity reports were the first measures that were preventative, attempting to capture money laundering before

[75] Money Laundering Control Act Pub. L. 99-570.
[76] Drug Trafficking Offences Act 1986.
[77] *R* v *Cuthbertson* [1981] A.C. 470 HL.
[78] Misuse of Drugs Act 1971.
[79] ibid s.27.
[80] A detailed discussion of the recommendations of the Hodgson Committee can be found in: N. Ryder, 'To Confiscate or not to Confiscate? A Comparative Analysis of the Confiscation of the Proceeds of Crime Legislation in the United States and the United Kingdom' [2013] 8 JBL 767 at 786.
[81] Drug Trafficking Offences Act 1986 s.24.
[82] ibid s.24(1).

is occurred; from this point AML developments may be categorised as further criminalisation or preventive measures.

In the same year as the UK and the US enacted targeted legislation towards money laundering, the EU still failed to act through legislation. In 1986 European ministers did instruct the CDPC to consider the issue "*in light inter alia of the work of the United Nations,*"[83] but the work of the CDPC did not lead to any legislation until 1990. Australia implemented its first money laundering offences in 1987, passing the Proceeds of Crime Act 1987,[84] and in 1988 the UN also began to address the proceeds of crime more directly through the UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances,[85] commonly referred to as the Vienna Convention 1988. Alford notes that the Vienna Convention "*evolved from two previous multilateral agreements;"*[86] the 1961 and 1971 Conventions, which as Sproule and St-Denis stated*, "focused primarily on limiting the supply of narcotic drugs and psychotropic substances to […] prevent their diversion into illicit traffic.*"[87] Alford sees this as a weakness of the earlier conventions; as "*they were primarily regulatory in nature and did not provide for punishment of drug traffickers, these conventions were not effective against the drug problem in the 1980s*."[88] It is important to note that combatting the drugs trade was still the main driver behind money laundering legislation in the 1980s, as the Vienna Convention and commentators' analysis illustrate. Ryder observes that

[83] cf Gilmore (n71) at p161.
[84] Proceeds of Crime Act 1987.
[85] Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (adopted 20 December 1988, entered into force 11 November 1990) UNTS 1582 (Vienna Convention 1988)
[86] D. Alford, 'Anti-Money Laundering Regulations: A Burden on Financial Institutions' (1994) 19(3) North Carolina Journal of International Law and Commercial Regulation 437 at 441-442.
[87] cf Sproule and St-Denis (n66) at p.265
[88] cf Alford (n86) at 441-442.

while the Vienna Convention requires signatories to criminalise the laundering of drug proceeds,[89] confiscate said proceeds,[90] facilitate extradition,[91] and improve mutual legal assistance;[92] these obligations are initially limited as the "*Vienna Convention was limited to the laundering of the proceeds of crime from the manufacturing and sale of narcotics.*"[93]

In 1989 the FATF was created, "*in response to mounting concern over money laundering.*"[94] The FATF "*was established by the G-7 Summit that was held in Paris in 1989*"[95] to address "*the threat posed to the banking system and to financial institutions*."[96] The creation of the FATF is a particularly important one in the history of AML initiatives as it demonstrated a shift away from the drugs trade, and towards treating money laundering as a standalone issue.

4.5.4. 1990s

The FATF issued 40 Recommendations, "*intended to provide a comprehensive plan of action needed to fight against money laundering*"[97] for its initial 16 members to comply with, the first edition of these Recommendations was published in April 1990.[98]

[89] Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (adopted 20 December 1988, entered into force 11 November 1990) UNTS 1582 (Vienna Convention 1988) art.3.
[90] ibid art.5.
[91] ibid art.6.
[92] ibid art.7.
[93] cf Ryder (n57) at p.15.
[94] Financial Action Task Force, 'History of the FATF' <http://www.fatf-gafi.org/about/historyofthefatf/> accessed 27 September 2019.
[95] ibid.
[96] ibid.
[97] ibid.
[98] Financial Action Task Force, 'Financial Action Task Force on Money Laundering: Report' <http://www.fatf-gafi.org/media/fatf/documents/reports/1990%20ENG.pdf> accessed 27 September 2019.

Despite the creation of the FATF as a body to address money laundering as an independent issue, the first Recommendation was for members to "*fully implement the Vienna Convention*,"[99] which, as has already been made clear, remained focussed on the issue of the drugs trade. Also in 1990 the Council of Europe adopted the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime[100] (1990 Council of Europe Convention), which was open for both member states and non-member states to sign.[101] Gilmore notes that the 1990 Council of Europe Convention was not widely adopted when it was first created, but that by 2004 it had 44 signatories.[102] The reasons for the poor uptake are not clear. Gilmore observes that the drafters were keen to "*protect the advances which had so recently been made*"[103] by the Vienna Convention 1988. The Council of Europe convention goes further than the Vienna Convention 1988, notably signatories were required to criminalise money laundering generally, rather than specifically in relation to drug trafficking.[104] Ratification of the Council of Europe Convention was slow, but it was another sign that the fight against money laundering was being decoupled from drug trafficking and being considered as a financial crime of its own.

In 1991, the First Money Laundering Directive was passed by the EU,[105] which created numerous obligations for financial institutions, the most important of which included

[99] ibid Recommendation 1.
[100] Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (adopted 08 August 1990, entered into force 01 September 1993) ETS 141 (1990 Council of Europe Convention).
[101] Council of Europe, 'Details of Treaty No.141' <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/141> accessed 27 September 2019.
[102] cf Gilmore (n71) at p162.
[103] ibid.
[104] ibid.
[105] 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 L166/77.

identifying customers, record keeping, refraining from tipping off customers being investigated, and a proactive duty to report suspicious transactions to the competent national authorities.[106] Article 14 stated that Member States were to "*determine the penalties to be applied for infringement of the measures*"[107] by financial institutions. Mitsilegas and Gilmore considered the Directive inadequate as it was not specific enough; the "*Directive did not contain any provisions regarding the nature, functions and powers of*"[108] the domestic authorities to oversee the measures. The lack of specificity of the Directive led to Member Stares implementing the directive in different ways, which hindered cooperation between Member States.[109]

In the US, the Annunzio-Wylie Money Laundering Act 1992[110] amended the BSA 1970, notably introducing suspicious activity reporting requirements for financial institutions.[111] Reporting requirements were extended further by the Money Laundering Suppression Act 1994.[112] It can be seen that suspicious activity reports were a key development of the AML approaches in the 1990s. An important development in the UK was the Criminal Justice Act 1993,[113] which amended the Criminal Justice Act 1988[114] to include money laundering offences for all crimes, not just drugs.[115] The 1993 amendment also criminalised "[a]*ssisting another to retain the*

[106] V. Mitsilegas and B. Gilmore, 'The EU legislative framework against money laundering and terrorist finance: a critical analysis in light of evolving global standards' (2007) 56(1) International and Comparative Law Quarterly 119 at 120.
[107] 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 L166/77 art.14.
[108] cf Mitsilegas and Gilmore (n106) at 120.
[109] ibid.
[110] Annunzio–Wylie Money Laundering Act 1992.
[111] ibid §1571.
[112] Money Laundering Suppression Act 1994.
[113] Criminal Justice Act 1993.
[114] Criminal Justice Act 1988.
[115] ibid ss.29-32, Adding ss.93A-D to the Criminal Justice Act 1988.

benefit of criminal conduct"[116] which, along with the drug crime related offence within the Drug Trafficking Offences Act 1986,[117] represents an important development in the crime of money laundering. Since the Criminal Justice Act 1993, money laundering has become an offence in itself; an offender would be found guilty of dealing with the proceeds of a crime without having committed the original crime.

International cooperation can be seen to be continually developing in the 1990s; by 1992 the membership of the FATF had increased to 28 members,[118] and in 1995 the Egmont Group of Financial Intelligence Units formed; an "*informal network of FIUs for the stimulation of international co-operation.*"[119] The FATF Recommendations required members to create financial intelligence units (FIU), which serve as a "*national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and financing of terrorism, and for the dissemination of the results of that analysis*."[120] An FIU should be in a position to co-ordinate a country's intelligence relating to money laundering and aid investigations by law enforcement agencies. The UK's FIU is the National Crime Agency (NCA), the Financial Crimes Enforcement Network (FinCEN) and the Australian Transaction Reports and Analysis Centre are the respective FIUs of the US and Australia. While the Egmont group and the expansion of the FATF demonstrates an international move towards separating money laundering from the

[116] Criminal Justice Act 1988 s.93A.
[117] Drug Trafficking Offences Act 1986 s.24
[118] Financial Action Task Force, 'History of the FATF' <http://www.fatf-gafi.org/about/historyofthefatf/> accessed 27 September 2019.
[119] The Egmont Group of Financial Intelligence Units, 'About' <http://www.egmontgroup.org/about> accessed 27 September 2019.
[120] The Egmont Group of Financial Intelligence Units, 'Financial Intelligence Units (FIUs)' <http://www.egmontgroup.org/about/financial-intelligence-units-fius> accessed 27 September 2019.

drugs trade in the 1990s, the UN was still focussed primarily on drugs, and in 1997 the United Nations Office on Drugs and Crime (UNODC) was created.[121] The UNODC was the result of the United Nations Drug Control Programme and the Centre for International Crime Prevention merging. The UNODC mandate is to assist UN Member States in combatting drugs and crime, but the inclusion of drugs in the title of the organisation, and the Conventions adopted up to this point, indicates the focus remained on drugs at the time of its creation.

4.5.5. 2000 to Present

The turn of the century saw the creation of the Wolfsberg Group, a group of banks which collectively develop guidance for banks in developing AML policies,[122] this demonstrates that money laundering was beginning to warrant attention in the private sector as well as from governments. In 2000 the UN extended the criminalisation of money laundering with the UN Convention against Transnational Organised Crime,[123] known commonly as the Palermo Convention 2000. This was an important development in the UN's approach to money laundering as it finally decoupled the fights against drugs and money laundering; the Palermo Convention 2000 required signatories to extend money laundering offences to include the proceeds of "*serious crimes,*"[124] not just drug related crime. Serious crimes were defined as "*conduct*

[121] Established through the merging of United Nations Drug Control Programme and the Centre for International Crime Prevention: United Nations Office on Drugs and Crime, 'About the UNODC' <https://www.unodc.org/unodc/en/about-unodc/index.html?ref=menutop> accessed 02 September 2019.
[122] Wolfsberg Group, 'Mission' <https://www.wolfsberg-principles.com/about/mission> accessed 14 October 2019.
[123] Convention against Transnational Organised Crime (adopted 15 November 2000, entered into force 29 September 2003) UNTS 2225 (Palermo Convention 2000).
[124] ibid art.6.

constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty."[125] Zagaris cites a key aim of the Palermo Convention 2000 as strengthening the "*power of governments to combat serious crimes by providing a basis for stronger common action against money laundering through synchronized national laws.*"[126] This may be contrasted with the criticisms of the first EU Directive on money laundering,[127] which produces an inconsistent approach from Member States and created uncertainty. The Palermo Convention 2000 provides a clear model for governments to follow and its definitions were adopted by the FATF.[128]

Also in 2000, the UK passed the Terrorism Act 2000,[129] which introduced the concept of laundering terrorist property. Alexander distinguishes terrorist financing from the common concept of money laundering; money laundering "*concerns property which is derived from crime and efforts to combat it therefore focus on its origin",*[130] whereas with terrorist financing, *"the focus is not on the where the property has come from but where it is destined: its ultimate purpose.*"[131] Roberge also argues for a disentangling of the two concepts due to their differing aims and ideology.[132] The Terrorism Act 2000 represents the point at which the UK confused money laundering with a different issue

[125] ibid art.3.
[126] B. Zagaris, *International White Collar Crime: Cases and Materials* (New York: Cambridge University Press, 2010) p.64.
[127] 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 L166/77.
[128] Financial Action Task Force, 'FATF Recommendations – 2003' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202003.pdf> accessed 28 September 2019 Recommendation 1.
[129] Terrorism Act 2000.
[130] R. Alexander, Insider Dealing and Money Laundering in the EU: Law and Regulation (Aldershot: Ashgate, 2007) at p.173.
[131] ibid.
[132] Ian Roberge, 'Misguided Policies in the War on Terror? The Case for Disentangling Terrorist Financing from Money Laundering' (2007) 27(3) Political Studies Associations 196.

to the drugs trade, and can be seen as a backwards step by a country which could be viewed as being ahead of the international approach in the 1990's by criminalising money laundering for all crime. Coupling money laundering and terrorism financing is confusing as the processes are different; as can be seen from the Alexander distinction above, the processes operate in opposite directions and so use different techniques, and while there may be some common ground, the two issues require separate approaches. The UK also enacted the Financial Services and Markets Act 2000,[133] which gave the newly created Financial Services Authority responsibility for reducing financial crime,[134] and powers to create rules in relation to preventing money laundering.[135] In 2002, the UK passed the Proceeds of Crime Act 2002[136] (POCA 2002), which is where the current UK money laundering offences are found, the applicability of the offences to cryptocurrencies is analysed in chapter five.

Countering terrorist financing was further integrated into AML approaches in the wake of the 11th September attacks, as the US introduced reforms to money laundering legislation to address terrorist financing. The Uniting and Strengthening America by Providing Appropriate Tools to Restrict, Intercept and Obstruct Terrorism Act 2001[137] (PATRIOT Act 2001), which, along with paying too much attention being paid to the acronym the title produced, amended the BSA 1970 reporting requirements to cover terrorist financing. The PATRIOT Act 2001 was also the first time the US legislated against money laundering with extra-territorial effect.[138] The amended version of the

[133] Financial Services and Markets Act 2000.
[134] ibid s.6.
[135] ibid s.146.
[136] Proceeds of Crime Act 2002.
[137] Uniting and Strengthening America by Providing Appropriate Tools to Restrict, Intercept and Obstruct Terrorism Act 2001.
[138] cf Ryder (n57) at p.44.

BSA 1970 is the principal current source of US AML law and is considered in detail in chapter six. The incorporation of counter terrorist financing legislation has led to the term 'reverse money laundering', which Cassella defines as the "*process of conducting financial transactions with clean money for the purpose of concealing or disguising the future use of that money to commit a criminal act.*"[139] The development of the US AML approach, similarly to the UK, has become confused as it tries to combat terrorist financing; as a result the US and the UK may now be criticised for coupling money laundering to a relatable offence, much like the UN did with the drugs trade before 2000. The FATF also reacted to the 11th September attacks by conflating money laundering and terrorist financing, initially through Eight Special Recommendations in October 2001.[140]

In 2001, the EU passed the Second Money Laundering Directive,[141] which amended the First Directive, extending the preventative measures to non-financial institutions.[142] Notably the Second Directive required any potentially new Member States to adopt the Money Laundering Directives as a prerequisite of entry.[143] The First and Second Directives were then merged into the Third Directive in 2005;[144] Ryder states that the

[139] S. D. Cassella, 'Reverse money laundering (2003) 7(1) Journal of Money Laundering 92 at pp.92-93.
[140] Financial Action Task Force, 'History of the FATF' <https://www.fatf-gafi.org/about/historyofthefatf/> accessed 14 October 2019.
[141] 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 [2001] OJ L.344/76.
[142] Many non-financial institutions may be susceptible to money laundering due to the services that proved; lawyers, estate agents and art dealers for example are not financial institutions but may be approached by those wishing to launder money.
[143] cf Ryder (n57) at p.34.
[144] 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 [2005] OJ L.309/15.

EU Directives require Member States to adopt a risk-based approach, prioritising institutions, individuals or services that are most at risk to money laundering. The risk-based approach is also recommended by the FATF as of the 2003 iteration of the FATF Recommendations.[145] The EU has also amended the 1990 Council of Europe Convention with the 2005 by the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism,[146] and took similar action to the UK and the US, combining money laundering with counter terrorist financing, the treaty currently has 28 ratifications and a further 12 signatories not followed by ratification.[147] The FATF also added an additional ninth special Recommendation for combatting terrorist financing in 2004.[148]

2003 saw the UN adopt the UN Convention on Corruption.[149] Corruption is a complex and broad issue, which overlaps with money laundering. Article 14 of the Convention contains measures to prevent money laundering, which are notably similar to the Recommendations of the FATF. Article 14 requires Party States to regulate entities which pose money laundering risks,[150] and to enable the cooperation of the relevant

[145] Financial Action Task Force, 'FATF Recommendations – 2003' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202003.pdf> accessed 28 September 2019.
[146] Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (adopted 16 May 2005, entered into force 01 May 2005 CETS 198 (2005 Council of Europe Convention).
[147] Council of Europe, 'Chart of signatures and ratifications of Treaty 198' <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/198/signatures?p_auth=7ynMkkvx> accessed 28 September 2019.
[148] Financial Action Task Force, 'IX Special Recommendations' <http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Standards%20-%20IX%20Special%20Recommendations%20and%20IN%20rc.pdf> accessed 28 September 2019.
[149] Convention against Corruption (adopted 21 October 2003, entered into force 14 December 2005) 43 ILM 37.
[150] ibid Art 14(1)(a).

authorities.[151] Cash is specifically mentioned as requiring monitoring,[152] and the convention specifically mentions remittance services as being included in the entities which are required to identify the originator of funds, maintain information, and query any incomplete data sets.[153] It is notable that remittance services are mentioned, as US regulator FinCEN specifically identifies cryptocurrency exchanges as money transmitters,[154] regardless of whether the currency being remitted is fiat or not. Carr praises the comprehensiveness of the Convention,[155] arguing it is "*very difficult to fault*",[156] but notes that the biggest weakness with the Convention, which is true of most UN measures, is that international legislation alone is not the solution. Carr does not criticise the convention itself, but the will of countries to utilise it. In "*countries where politicians turn a blind eye to corruption to ensure or maintain their status, there is unlikely to be legislative interference*"[157] on corrupt practices. The UK is a signatory to the Convention, as are the US and Australia.[158] In the UK in particular the Convention was implemented by the Bribery Act 2010,[159] this legislation is not specifically targeted towards money laundering, due to the UK addressing this in other pieces of legislation, and therefore the Bribery Act 2010 will not be focused on in this thesis.

---

[151] ibid Art 14(1)(b).
[152] ibid Art 14(2).
[153] ibid Art 14(3)
[154] FinCEN, 'Guidance - FIN-2013-G001 - Issued: March 18, 2013 - Subject: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies' <https://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf> accessed 16 December 2015.
[155] I. Carr, 'Fighting corruption through the United Nations Convention on Corruption 2003: a global solution to a global problem?' (2005) 11(1) Int. T.L.R. 24 at p.29.
[156] ibid.
[157] ibid.
[158] United Nations Office on Drugs Crime, 'Signature and Ratification Status' <https://www.unodc.org/unodc/en/corruption/ratification-status.html> accessed 10 June 2019.
[159] Bribery Act 2010 c.23. For more on the level of compliance achieved by the UK see: Transparency International-Bond Anti-Corruption Group, 'Report on the UK's Compliance with the UN Convention Against Corruption' <https://www.transparency.org.uk/wp-content/plugins/download-attachments/includes/download.php?id=901> accessed 10 June 2019.

The Money Laundering Regulations 2007[160] codified the preventive measures of the UK in order to comply with the 3rd Anti-Money Laundering Directive, this has since been superseded by the 4th and 5th Anti-Money Laundering Directives.[161] The Money Laundering Regulations 2007 have subsequently been replaced by the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.[162] The UK has amended the 2017 regulations to implement the 5th Anti-Money Laundering directive.[163] The current legislation of the UK analysed in detail in chapter five. Similarly, Australia's most recent money laundering legislation is the Anti-Money Laundering and Counter-Terrorism Financing Act 2006,[164] which is considered in the Australia case study in chapter eight.

4.5.6. Summary of Anti-Money Laundering Regulation

Money laundering has developed from being a secondary consideration to the War on Drugs to a standalone issue of international concern. The 1980s and 1990s saw money laundering separated from drug offences, but from the early 2000s it has been conflated with countering the financing of terrorism. It is clear from the timeline of AML

[160] The Money Laundering Regulations 2007 S.I. 2003/3075.
[161] Directive 2015/849/EU 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 [2015] OJ L.141/73 and Council Directive 2018/843/EU 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 L 156/43.
[162] Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 S.I. 2017/692.
[163] The Money Laundering and Terrorist Financing (Amendment) Regulations 2019, SI 2019/1511.
[164] Anti-Money Laundering and Counter-Terrorism Financing Act 2006.

development than the UK, the US, and Australia have each been early adopters of international best practice, and also gone further than the international minimum requirements. Each of the three jurisdictions are considered developed countries[165] and therefore have developed economies which are vulnerable to money laundering. Based on the previous behaviour of each of the case study jurisdictions it is likely that they will implement international best practice in relation to cryptocurrencies. This has already occurred in the United States, which is analysed in chapter six, and in Australia, which is analysed in chapter seven. The UK is expected to keep pace with international best practice, and it is legally bound to implement EU directives while it remains a member of the EU. The EU response to cryptocurrencies is analysed below at 4.11, and the UK has legislated to implement the 5th Anti-Money Laundering Directive. Due to the global importance of AML regulation, the threat posed by cryptocurrencies has been addressed by international organisations, the next section of this chapter will assess the response of the UN, the FATF and the EU. It will be seen that the EU and the FATF continue to pursue their prescriptive approach to setting international best practice and providing guidance on regulating cryptocurrencies.

4.6. International Response to Money Laundering Threat Posed by Cryptocurrencies

Given the development global of AML standards during the latter half of the 1990s and the early 2000s, there are a number of international organisations which provide domestic jurisdictions with model legislation and guidance relating to combatting the

[165] United Nations Development Programme, 'Human Development Reports: 2018 Statistical Update' (14 December 2018) <http://hdr.undp.org/en/2018-update> accessed 14 October 2019.

board and complex issue of money laundering. The organisations involved differ greatly; in their legal authority, in their size of membership, and in how high AML is in their overall objectives. Therefore, the aim on this section is to identify the relevant international organisations, ascertain their influence over the case study jurisdictions and to analyse their AML measures, with specific reference to their responses to the money laundering risks posed by cryptocurrencies. The organisations which will be assessed are the United Nations (UN), the FATF, and the EU. The reasons for the selection of these organisations are as follows. All of the case study jurisdictions are UN members, and the UN has been instrumental in developing AML legislation at an international level since the 1960s. The FATF can be seen as the present-day world leading AML organisation, set up in 1989, providing comprehensive recommendations and also counting all three case study jurisdictions as members. The EU is considered in this thesis due to its unique nature, which means its AML measures are applicable across the bloc, and has directly impacted on the development of AML in the UK. As identified in the money laundering timeline, the EU has been addressing money laundering since the 1970s. Building on the history of money laundering and AML analysed above, it will be seen in this section that the international position in relation to money laundering is still lacking harmony, but the FATF Recommendations form the basis of international standards. The importance these international organisations to the case study jurisdictions varies according to membership rules, but, as seen above, each of the case study jurisdictions are early adopters of international AML standards so would likely continue to comply with such measures. It will also be seen that the FATF and the EU both seek to regulate cryptocurrencies in some form but only at the periphery of the cryptocurrency networks, where they interact with the traditional financial system. This is inadequate, and the relevant international

organisations should take more of a lead in understanding cryptocurrencies, their networks, and how best to adapt the current measures to apply to cryptocurrencies, rather than simply transposing existing measures which are incompatible with cryptocurrency transactions.

4.7. United Nations

The UN was formed in 1945,[166] it was created in the wake of World War Two, replacing the defunct League of Nations.[167] Both the League of Nations and its replacement, the UN, were created in the aftermath of world wars, and therefore maintaining peace was high on the initial agenda.[168] The modern-day UN has 193 Member States, including the three case study jurisdictions; the UK, the US, and Australia. The UN lists its main organs as the General Assembly,[169] the Security Council,[170] the Economic and Social Council,[171] the Trusteeship Council,[172] the International Court of Justice,[173] and the Secretariat.[174] The UN is a unique international organisation with the power to "*take*

[166] United Nations, '1945: The San Francisco Conference' <http://www.un.org/en/sections/history-united-nations-charter/1945-san-francisco-conference/index.html> accessed 01 March 2019.
[167] BBC, 'The League of Nations and the United Nations' (17 February 2011) <http://www.bbc.co.uk/history/worldwars/wwone/league_nations_01.shtml> accessed 02 March 2019.
[168] United Nations, 'History of the United Nations' <http://www.un.org/en/sections/history/history-united-nations/index.html> accessed 01 September 2019 and BBC, 'The League of Nations and the United Nations' (17 February 2019) <http://www.bbc.co.uk/history/worldwars/wwone/league_nations_01.shtml> accessed 02 September 2019.
[169] United Nations, 'Functions and powers of the General Assembly' <http://www.un.org/en/ga/about/background.shtml> accessed 01 March 2019.
[170] United Nations, 'What is the Security Council' <http://www.un.org/en/sc/about/> accessed 02 March 2019.
[171] United Nations, 'About Us' <https://www.un.org/ecosoc/en/about-us> accessed 02 March 2019.
[172] United Nations, 'Trusteeship Council' <http://www.un.org/en/sections/about-un/trusteeship-council/index.html> accessed 02 March 2019.
[173] United Nations, 'International Court of Justice' <http://www.icj-cij.org/court/index.php?p1=1> accessed 01 March 2019.
[174] United Nations, 'Secretariat' <http://www.un.org/en/sections/about-un/secretariat/index.html> accessed 02 March 2019.

action on the issues confronting humanity,"[175] of which money laundering has been accepted as global issue, as the International Monetary Funds (IMF) estimations of 2-5% of global GDP demonstrates.[176]

In relation to money laundering the United Nations Office on Drugs and Crime (UNODC) is the most relevant body; and as argued in the money laundering timeline, this is indicative of the UN's approach to money laundering being part of its measures to combat the international drugs trade, rather than independent financial crime. The UN's role with regard to AML is less prominent in the 21st century due to the development of the FATF, and the current UN conventions do not address cryptocurrencies

4.7.1. Anti-Money Laundering Policy

As seen through the history of AML, the UN's AML policy can be traced back to the 1960's when the confiscation of the proceeds of drug related crime was included in the Single Convention on Narcotic Drugs 1961.[177] This did not directly address the issue of money laundering, however, it recognised that preventing criminals from enjoying the benefits of crime is an important step to reducing the appeal of criminal activity. As Stewart identifies,[178] the first attempts of the UN to address money

[175] United Nations, Overview' < http://www.un.org/en/sections/about-un/overview/index.html> accessed 01 March 2019.
[176] International Monetary Fund, 'Money Laundering: The Importance of International Countermeasures' <http://www.imf.org/external/np/speeches/1998/021098.htm> accessed 15 October 2019.
[177] Single Convention on Narcotic Drugs (adopted 30 March 1961, entered into force 13 December 1964) 520 UNTS 151 (Single Convention on Narcotic Drugs).
[178] cf Stewart (n65).

laundering focussed on the drugs trade, and this continued for the proceeding decades; as Ryder observes, the "*Vienna Convention was limited to the laundering of the proceeds of crime from the manufacturing and sale of narcotics.*"[179] The Vienna Convention required signatories to criminalise the laundering of drug proceeds,[180] confiscate said proceeds,[181] facilitate extradition,[182] and improve mutual legal assistance;[183] but, as identified in the money laundering timeline, the continued link with the drugs trade left many crimes outside of the remit of the convention. It was not until the Palermo Convention 2000[184] that the UN decoupled money laundering from drug related offences, and criminalised money laundering of the proceeds of all "*conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty.*"[185]

The UN Convention on Corruption was adopted in 2003 and entered into force in 2006.[186] The convention addresses money laundering, but it is not the focus of the Convention as corruption is a wider and more complex issue which overlaps with many financial crimes. Article 14 of the convention contains measures to prevent money laundering, which are notably similar to the Recommendations of the FATF. While independent of each other, the UN endorses the FATF Recommendations, notably in

[179] cf Ryder (n57) at p.15.
[180] Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (adopted 20 December 1988, entered into force 11 November 1990) UNTS 1582 (Vienna Convention 1988) art.3.
[181] ibid art.5.
[182] ibid art.6.
[183] ibid art.7.
[184] Convention against Transnational Organised Crime (adopted 15 November 2000, entered into force 29 September 2003) UNTS 2225 (Palermo Convention 2000).
[185] ibid art.3.
[186] Convention against Corruption (adopted 21 October 2003, entered into force 14 December 2005) 43 ILM 37.

2005, UN Security Council Resolution 1617 "[s]*trongly urges all Member States to implement*" FATF Recommendations.[187]

4.7.2. Policy towards cryptocurrencies

The relevant UN conventions were adopted before the creation and development of cryptocurrencies, as such the conventions makes no mention of cryptocurrencies. However, the UN, particularly through the UNODC, has recognised cryptocurrencies, and makes recommendations to Member States for the detecting and preventing money laundering through cryptocurrencies. The UNODC is the principle UN organisation in this area as it has responsibility for the UN's Global Programme against Money-Laundering, Proceeds of Crime and the Financing of Terrorism,[188] with the UNODC's mandate coming from the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988.[189]

The UNODC published guidance on virtual currencies in 2014.[190] This document is training manual, which covers 4 areas; identifying virtual currencies, the risks posed, methods for detecting money laundering through virtual currencies, and methods for seizing virtual currencies. The manual echoes the guidance from the FATF, identifying

[187] United Nations Security Council, 'Resolution 1617 (2005)' <http://unscr.com/en/resolutions/doc/1617> accessed 10 June 2019 at para 7.
[188] United Nations Office on Drugs and Crime, 'UNODC on Money Laundering and Countering the Financing of Terrorism' <https://www.unodc.org/unodc/en/money-laundering/index.html?ref=menuside> accessed 03 March 2019.
[189] United Nations Office on Drugs and Crime, 'UNODC on Money Laundering and Countering the Financing of Terrorism' <https://www.unodc.org/unodc/en/money-laundering/index.html?ref=menuside> accessed 03 September 2019.
[190] United Nations Office of Drug Control, 'Basic Manual on the Detection and Investigation of the Laundering of Crime Proceeds Using Virtual Currencies' <https://www.imolin.org/pdf/imolin/FULL10-UNODCVirtualCurrencies_final.pdf> accessed 10 June 2019.

similar challenges that cryptocurrencies pose. Namely that regulations should be applied where intersections between the traditional financial system and cryptocurrencies occur, "*they should be licensed or registered, and subject to effective systems of monitoring and ensuring compliance with national AMF/CFT requirements.*"[191] With regard to gaps in the guidance of the FATF, the UNODC notes the difficulties in regulating cryptocurrencies as their decentralised nature means there is "*no financial institution providing a service of money or value transfer, or of money or currency changing*"[192] to apply regulations to.

The UNODC make some basic proposals for tackling cryptocurrency money laundering, they suggest international harmonisation, and the adoption on the FATF Recommendations.[193] The UNODC also propose the creation of "*specialised financial investigative units* [that] *can draw on their experience investigating laundering crime proceeds using more traditional methods*."[194] This is a commendable suggestion, while cryptocurrencies are a new phenomenon, the concept of money laundering is not, and the end goal for launders remains the same. As stated already, the aim of money laundering is not disputed, taking Stokes summation, money laundering is "*the process whereby the identity of dirty money that is the proceeds of crime and the real ownership of these assets is transformed so that the proceeds appear to originate from a legitimate source.*"[195] A logical step proffered by the UNODC is to utilise existing

[191] ibid at 5.4 at p.64.
[192] ibid.
[193] ibid at 5.4 at p.120.
[194] ibid.
[195] cf Lilley (n3).

expertise on money laundering, and cooperate with those who understand the complexities of cryptocurrencies.

4.7.3. Summary of the UN's Approach to risks of Money Laundering using Cryptocurrencies

The UN has developed AML conventions which have a high level of ratification, all of the case study jurisdictions comply with UN AML provisions. The UN does provide some guidance on cryptocurrencies and their regulation through the basic manual, but this has no legal force and it is not well publicised. Additionally, it does not provide any specific measures for cryptocurrencies, the guidance is limited in relation to applying or developing AML provisions to address cryptocurrencies. The UN frequently refers to the guidance of the FATF rather than developing AML provisions of its own.

4.8. Financial Action Task Force

The FATF was created in 1989, following the G-7 Summit that was held in Paris that year.[196] All of the case study jurisdictions of this research are members.[197] The FATF describes itself as "*an inter-governmental body,*"[198] which is to "*set standards and promote effective implementation of legal, regulatory and operational measures*"[199] specifically towards money laundering and terrorist financing, but it will consider wider

[196] Financial Action Task Force, 'History of the FATF' <http://www.fatf-gafi.org/about/historyofthefatf/> accessed 05 May 2019.
[197] Financial Action Task Force 'Who We Are' <http://www.fatf-gafi.org/about/> accessed 02 February 2019.
[198] ibid.
[199] ibid.

related threads to the international financial system.[200] The role of the FATF is as "*a "policy-making body" which works to generate the necessary political will to bring about*"[201] change to Member States AML legislation. In this capacity, the FATF issues 40 Recommendations which it states are the "*International Standards on Combating Money Laundering.*"[202] While the FATF was created to address money laundering as an independent issue, the first Recommendation was for members to "*fully implement the Vienna Convention*,"[203] which remained focussed on the issue of the drugs trade. The Recommendations were first published in 1990,[204] they have been amended regularly, but most notably in 1996, 2001, 2003, and 2012.[205] The biggest change to the Recommendations came in 2001 when eight 'special Recommendations' were introduced to combat terrorist financing following the terrorist attacks in September 2001.[206] A ninth special Recommendation was added in 2004,[207] and all nine have subsequently been incorporated into the most recent set of 40 Recommendations.[208] With the inclusion of terrorist financing provisions, the approach towards money

[200] ibid.
[201] Financial Action Task Force 'Who We Are' <http://www.fatf-gafi.org/about/> accessed 02 September 2019.
[202] Financial Action Task Force, 'The FATF Recommendations' <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/internationalstandardsoncombatingmoneylaunderingandthefinancingofterrorismproliferation-thefatfrecommendations.html> accessed 05 February 2019.
[203] Financial Action Task Force, 'Financial Action Task Force on Money Laundering: Report' <http://www.fatf-gafi.org/media/fatf/documents/reports/1990%20ENG.pdf> accessed 27 July 2019 Recommendation 1.
[204] Financial Action Task Force, 'The Forty Recommendations of the Financial Action Task Force on Money Laundering 1990' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%201990.pdf> accessed 01 April 2019.
[205] Financial Action Task Force 'Who We Are' <http://www.fatf-gafi.org/about/> accessed 02 February 2019.
[206] Initially eight, but amended to nine in October 2004: Financial Action Task Force, 'FATF IX Special Recommendations' <http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Standards%20-%20IX%20Special%20Recommendations%20and%20IN%20rc.pdf> accessed 02 April 2019.
[207] ibid.
[208] Financial Action Task Force, 'The FATF Recommendations' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf> accessed 04 April 2019.

laundering is slightly confused, as identified in the money laundering timeline, money laundering was originally integrated into drug offences and took decades to be considered an offence in itself, it is a step backwards to merge money laundering and terrorist financing together when they should be considered separately.

4.8.1. Anti-Money laundering policy

The FATF was created *in response to mounting concern over money laundering*",[209] and the 40 Recommendations represent the FATF's money laundering policy, to address "*the threat posed to the banking system and to financial institutions*."[210] The 40 Recommendations are *"intended to provide a comprehensive plan of action needed to fight against money laundering",*[211] which its 35 members are to comply with.

The FATF promotes a 'risk-based approach' to preventing and detecting money laundering.[212] A risk-based approach means "*enhanced CDD measures have to be taken*"[213] in higher risk circumstances. The FATF provides guidance for determining such circumstances; customer risk factors include whether "*the business relationship is conducted in unusual circumstances*",[214] if the customers from foreign jurisdictions, cash intensive businesses, or businesses which are "*excessively complex given the*

[209] Financial Action Task Force, 'History of the FATF' <http://www.fatf-gafi.org/about/historyofthefatf/> accessed 27 July 2019.
[210] ibid.
[211] ibid.
[212] Financial Action Task Force, 'The FATF Recommendations' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> accessed 05 July 2019 at p62.
[213] ibid.
[214] ibid.

nature of the company's business."[215] The FATF also consider country or geographic risk factors such as countries identified as not having adequate AML systems, countries subject to sanctions, or countries identified as having significant levels of corruption or other criminal activity.[216] Finally, in relation to high risk activity, specific services or transactions are deemed to increase the money laundering risk, such as private banking, anonymous transactions, non-face-to-face business relationships or transactions and payments received from unknown or un-associated third parties.[217]

The FATF also identifies situations which are of a lower risk and in such circumstances the FATF states it is "*reasonable for a country to allow its financial institutions to apply simplified CDD measures*."[218] Situations where a simplified CDD measures can be applied typically involve recognised financial institutions, government bodies or situations where AML measures will already have been applied; such as financial institutions "*where they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations*".[219] Other risk lowering circumstances include customers which are publicly listed companies or public administrations. While the country a transaction come from may raise the risk, no countries are listed as lowering risk of money laundering. The FATF states that products and services with low risks include life insurance policies with low premiums, pensions "*where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the*

[215] ibid.
[216] ibid at p63.
[217] ibid.
[218] ibid.
[219] ibid at p64.

scheme",[220] and "[f]*inancial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes*."[221]

Adopting a risk-based approach can be applied in a specific manner as above, but the importance of the risk-based approach is in a more general sense; Recommendation 1 of the 40 Recommendations is that Member States are "[a]*ssessing risks & applying a risk-based approach.*"[222] The FATF states that the risk based approach "*should be an essential foundation to efficient allocation of resources across the anti-money laundering and countering the financing of terrorism (AML/CFT) regime and the implementation of risk based measures throughout the FATF Recommendations*."[223] Member States are required to perform regular risk assessments, as money launderers will utilise whatever methods they can, and will naturally target weaknesses.[224] The risk-based approach accepts that it is not possible to pursue money laundering without being targeted towards circumstances which are most likely to be used for money laundering.

Alexander notes that despite the Recommendations of the FATF being "*non-binding in a legal sense, some of the 40 Recommendations have become mandatory.*"[225] Examples of mandatory Recommendations are criminalising money laundering and

[220] ibid.
[221] ibid.
[222] ibid at p.4.
[223] ibid at p.9.
[224] As identified earlier in this chapter at 4.5.
[225] K Alexander, 'The International Anti-Money-Laundering Regime: The Role of the Financial Action Task Force' (2001) 4(3) JMLC 231 at p.240.

implementing 'know your customer' protocols.[226] The FATF strengthens the status of the Recommendations through sanctions. Alexander outlines the FATF sanctions regime as "*a series of graduated steps designed to pressure members to enact the necessary reforms to achieve compliance*."[227] Sanctions available to any international organisation are limited; as such the punitive measures of the FATF start with relatively soft pressure with a letter from the President of the FATF, this step was issued to Turkey in 1996.[228] The non-compliance of Turkey as a member of the FATF prompted the FATF to formalise its sanctions regime; if a jurisdiction fails to adequately respond to the FATF President's letter, then Recommendation 19 requires all members to "*apply enhanced due diligence measures to business relationships and transactions with natural and legal persons, and financial institutions, from countries for which this is called for by the FATF.*"[229] The strongest sanction the FATF can impose on a member is to expel them from the organisation, which to date has not been taken. Recommendation 19 demonstrates that the key power the FATF will utilise is public shaming, Alexander notes that the public shame created when the FATF instructed its members to scrutinise transactions with Turkey was enough to prompt Turkey to comply where the letter from the President had failed.[230] The power of the FATF to shame jurisdictions is only as effective as the jurisdiction's desire to be seen positively by the international community; public shaming will likely have little effect on

[226] ibid at 231.
[227] ibid at 240.
[228] Financial Action Task Force, 'Annual Report 1995-1996' <http://www.fatf-gafi.org/media/fatf/documents/reports/1995%201996%20ENG.pdf> accessed 03 June 2019 at para 61.
[229] Financial Action Task Force, 'The FATF Recommendations' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> accessed 03 June 2019.
[230] cf Alexander (n225) at 241.

jurisdictions such as North Korea where international condemnation does not appear to deter the government or force change.

The sanction regime for Non-Member States is similar to that of Member States, while there is no official sanctioning power, Recommendation 19 is not limited to Member States. The FATF treatment of jurisdictions which are not members and not adhering to international money laundering standards has been described by Stessens as 'blacklisting'.[231] The FATF categorise 'high-risk and non-cooperative jurisdictions' as either those requiring a 'call for action', and 'other monitored jurisdictions'.[232] Those that are subject to a 'call to action' are North Korea, which faces a "*FATF call on its members and other jurisdictions to apply counter-measures,*"[233] and Iran, which is subject to a "*FATF call on its members and other jurisdictions to apply enhanced due diligence measures proportionate to the risks arising from the jurisdiction*."[234] The 'call for action' list serves as the FATF blacklist, intended to shame jurisdictions into complying; the approach will also cause economic pressure as globalisation has meant countries are increasingly dependent on international trade. The blacklisting approach is still reliant on the subject jurisdiction being influenced by public shame, which has limited impact on isolated jurisdictions such as North Korea. An important element to any sanctions regime is to also act as a deterrence; this can be demonstrated by the effect of threatening sanctions on the Seychelles. The FATF

[231] G. Stessens, 'The FATF 'Black List' of Non-Cooperative Countries or Territories' (2001) 14 Leiden Journal of International Law 199.
[232] Financial Action Task Force, 'High-risk and non-cooperative jurisdictions' <http://www.fatf-gafi.org/countries/#high-risk> accessed 03 September 2019.
[233] Financial Action Task Force, 'Public Statement - 23 June 2017' <http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/documents/public-statement-june-2017.html> accessed 03 July 2019.
[234] ibid.

criticised a proposed law in the Seychelles in 1996,[235] and Alexander notes that the threat of sanctions along with the negative media attention was enough to dissuade the Seychelles from passing the law.[236]

Additionally to the blacklist, the FATF also maintains a list of 'other monitored jurisdictions', which are "jurisdictions that have strategic AML/CFT deficiencies for which they have developed an action plan with the FATF."[237] The current list consists of Bosnia and Herzegovina, Ethiopia, Iraq, Syria, Uganda, Vanuatu and Yemen.[238] The purpose of this category of jurisdictions is to aid the jurisdictions to become compliant; the FATF states that "[w]*hile the situations differ among each jurisdiction, each jurisdiction has provided a written high-level political commitment to address the identified deficiencies.*"[239]

The FATF identifies its money laundering objective as to "*set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering*".[240] As part of this objective the FATF undertakes "peer reviews of

[235] George Graham, 'Seychelles 'haven for money laundering'' Financial Times (London 2 February 1996) 3.
[236] cf Alexander (n225) at 242.
[237] Financial action Task Force, 'Improving Global AML/CFT Compliance: On-going Process - 23 June 2017' <http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/documents/fatf-compliance-june-2017.html> accessed 04 July 2019.
[238] ibid.
[239] ibid.
[240] Financial Action Task Force 'Who We Are' <http://www.fatf-gafi.org/about/> accessed 02 September 2019.

each member on an ongoing basis to assess levels of implementation of the FATF Recommendations".[241]

4.8.2. Policy towards cryptocurrencies

The FATF has been the most proactive international organisation in attempting to address the money laundering threats posed by cryptocurrencies; publishing three guidance documents on the issue, and two reports.[242] In June 2014, the potential risks of cryptocurrencies were considered,[243] and in June 2015 a follow up paper was published as a guide for Member States in applying the risk-based approach to cryptocurrencies.[244] In June 2019, the FATF published "*Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*",[245] in which the terminology used was broad, addressing virtual assets as a whole, rather than specifically advising on cryptocurrencies.

[241] Financial Action Task Force, 'Topic: Mutual Evaluations' <http://www.fatf-gafi.org/publications/mutualevaluations/?hf=10&b=0&s=desc(fatf_releasedate)> accessed 04 September 2019.
[242] Financial Action Task Force, 'Publication Search: Virtual Currencies' <https://www.fatf-gafi.org/publications/?hf=10&b=0&q=virtual+currencies&s=desc(fatf_releasedate)> accessed 25 June 2019.
[243] Financial Action Task Force, 'Virtual Currencies – Key Definitions and Potential AML/CFT Risks' <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 27 November 2019.
[244] Financial Action Task Force, 'Guidance for a Risk-Based Approach – Virtual Currencies' <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf> accessed 04 March 2019.
[245] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2019.

The June 2014 paper, 'Virtual Currencies – Key Definitions and Potential AML/CFT Risks'[246] provides a definition of virtual currencies which focusses on the three functions of money. The FATF define a virtual currency as a "*digital representation of value*"[247] which is not legal tender, is "*not issued nor guaranteed by any jurisdiction,*"[248] and only fulfils the functions of money by agreement of the relevant community of users.[249] As identified in chapter three, in addition to providing a general definition of virtual currencies, the FATF also provide a breakdown of virtual currency types, as shown in Figure 5 below.

[246] Financial Action Task Force, 'Virtual Currencies – Key Definitions and Potential AML/CFT Risks' <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 27 November 2019.
[247] ibid at p4.
[248] ibid.
[249] ibid.

Figure 5. FATF Categories of Virtual Currency[250]

	Centralised	Decentralised
Convertible	Linden Dollars (used in Second Life) are an example of a convertible virtual world currency; users may exchange their currency for US Dollars. The currency is centralised, Linden Labs (the developer of Second Life) act as administrators.	Examples of decentralised currencies include Bitcoin and Dogecoin. These are convertible for fiat currency but not controlled by a central administrator.
Non-Convertible	World of Warcraft (WoW) gold is non-convertible virtual world currency; users may not convert this into a fiat currency. WoW gold is controlled by the game developers, Blizzard	None exist.[251]

As discussed in chapter three, a convertible virtual currency can be transferred into a fiat currency; if this is not possible, the currency is non-convertible. The distinction between centralised and decentralised currencies is that a centralised currency is controlled by a single administrating authority, whereas a decentralised currency has

[250] ibid.
[251] ibid.

no central authority. Fiat currencies are centralised, typically the administrating authority is a central bank, but in virtual currencies the central authority might be the developer of the virtual world the currency is used in. For decentralised virtual currencies, no central bank entity exists, instead these may be based on an algorithm or code which dictates the production of the currency. The focus of the FATF is on convertible virtual currencies, as is the focus of this thesis, known as cryptocurrencies.[252] The FATF state that "[c]*onvertible virtual currencies that can be exchanged for real money or other virtual currencies are potentially vulnerable to money laundering*"[253] and that "[d]*ecentralised systems are particularly vulnerable to anonymity risks*.[254] This thesis adopts the term cryptocurrencies, as all known decentralised convertible currencies utilise cryptography.[255]

2015 Guidance on applying the Risk-Based Approach to Virtual Currencies

In 2015 FATF published a follow up to the 2014 paper, providing guidance on applying the risk based approach to virtual currencies,[256] the focus of 2015 Guidance is on *"convertible virtual currency exchangers which are points of intersection that provide gateways to the regulated financial system*".[257] The guidance is based on how to follow the FATF Recommendations, advising on two areas; applying the FATF

[252] This thesis uses the term cryptocurrency to refer to convertible decentralised virtual currencies and uses the term 'virtual currencies' as a much wider term, as explained in chapters 1,2 and 3.
[253] Financial Action Task Force, 'Virtual Currencies – Key Definitions and Potential AML/CFT Risks' <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 27 November 2019 at p.9.
[254] ibid.
[255] As explained here: Bank of England, 'What are cryptoassets (cryptocurrencies)?' <https://www.bankofengland.co.uk/knowledgebank/what-are-cryptocurrencies> accessed 14 October 2019.
[256] Financial Action Task Force, 'Guidance for A Risk-Based Approach to Virtual Currencies' <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf> accessed 01 August 2016.
[257] ibid at p.4.

Recommendations to countries and authorities,[258] and guidance on applying FATF Recommendations to virtual currency exchanges.[259]

Guidance to countries and competent authorities begins at Recommendation 1; the FATF expect countries to adopt a risk-based approach, and in order to do this countries should "*identify, assess, and understand the money laundering and terrorist financing risks for the country.*"[260] Higher risk activities will then be subject to the strongest AML measures, and in relation to cryptocurrencies the FATF recommend the "*application of enhanced due diligence measures*"[261] due to the levels of anonymity provided to users. With regard to national cooperation and coordination, the FATF recommends education of the relevant authorities to understand the money laundering risks of cryptocurrencies and to consider engaging with the cryptocurrency sector.[262] FATF Recommendation 14 requires 'money or value transfer services'[263] to become licensed, and subject to the relevant guidance in the FATF Recommendations.[264] The 2015 guidance from FATF states that "*requirements of Recommendation 14 apply to domestic entities providing convertible VC exchange services between VC and fiat currencies*."[265] This is a notable step as it shows the FATF are opening up to the concept of cryptocurrencies being akin to money. Additionally, Recommendation 15 is

[258] ibid at p.7.
[259] ibid Section IV at p.12.
[260] Financial Action Task Force, 'The FATF Recommendations' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> accessed 03 September 2019, Recommendation 1 at p.9.
[261] ibid at para 23 at p.8.
[262] ibid at para 30 at p.9.
[263] Financial Action Task Force, 'The FATF Recommendations' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> accessed 03 September 2019, Recommendation 14 at p.15.
[264] ibid.
[265] Financial Action Task Force, 'Guidance for A Risk-Based Approach to Virtual Currencies' <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf> accessed 01 August 2016, para 33 at p.10

clearly applicable as it requires countries to assess risks concerning "*the development of new products and new business practices, including new delivery mechanisms*,"[266] and "*the use of new or developing technologies for both new and pre-existing products*."[267] The guidance reminds countries of Recommendation 39 which requires countries to have an appropriate sanction regime,[268] and Recommendation 40 which promotes international cooperation.[269]

Section IV of the FATF guidance applies to any "*entities that act as nodes where convertible VC activities intersect with the regulated fiat currency financial system*."[270] As with the advice to countries in Section III, the first Recommendation is for entities to "*identify, assess, and take effective action to mitigate*"[271] their money laundering risks, and apply a risk-based approach. The principle advice from the FATF is for entities to apply customer due diligence, suspicious activity reporting, and record keeping requirements to cryptocurrencies. The guidance advises compliance with Recommendation 10[272] which states that regulated entities "*should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names,*"[273] and that entities "*should be required to undertake customer due diligence*."[274] The guidance

[266] Financial Action Task Force, 'The FATF Recommendations' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> accessed 03 September 2019, Recommendation 15 at p.15.
[267] ibid.
[268] ibid at Recommendation 39 at p.27.
[269] ibid at Recommendation 40 at p.27.
[270] Financial Action Task Force, 'Guidance for A Risk-Based Approach to Virtual Currencies' <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf> accessed 01 August 2016, para 40 at p12.
[271] ibid at para 41 at p12.
[272] ibid at para 42 at p12.
[273] Financial Action Task Force, 'The FATF Recommendations' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> accessed 03 September 2019, Recommendation 10 at p.17.
[274] ibid.

states that record keeping and suspicious activity reporting requirements should apply to entities involved in exchanging cryptocurrencies. The guidance here is not detailed; it states that "*information available on the blockchain provides a beginning foundation for record keeping, provided institutions can adequately identify their customers*".[275] As identified in chapter three, the use of public keys rather than more orthodox personal details, led to cryptocurrencies being described as pseudonymous, and thus are appealing to money launderers.[276] Pseudonymous is an important distinction from anonymous, as if an individual's details are matched to a cryptocurrency address then transactions can be traced on the blockchain. Some success has been achieved in identifying cryptocurrency users, Meiklejohn *et al*[277] "*were able to identify 1.9 million public keys with some real-world service or identity,*"[278] although in many cases the identity discovered was not genuine.[279] More recently Juhász *et al* identified 22,363 users 1,797 associated IP addresses.[280] While difficulties will remain with determining which users require identification and investigation, Juhász *et al* argue their method is economical[281] and their "*algorithms are relatively easy to implement and can be combined with other Bitcoin-transaction related information.*"[282] The research of Meiklejohn *et al* and Juhász *et al* demonstrate that the anonymity of cryptocurrencies may be eroded by the aforementioned techniques, but more research is needed.

[275] Financial Action Task Force, 'Guidance for A Risk-Based Approach to Virtual Currencies' <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf> accessed 01 August 2016, para 49 at p13.
[276] United States Government Accountability Office, 'Virtual Currencies: Emerging Regulatory, Enforcement, and Consumer Protection Challenges' <http://gao.gov/assets/670/663678.pdf> accessed 16 December 2015 at p.6.
[277] Sarah Meiklejohn, et al, "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names," (2013) 38(6) ;Login: 10.
[278] ibid at p.14.
[279] ibid.
[280] P. L. Juhász, J. Stéger, D. Kondor and G. Vattay, 'A Bayesian approach to identify Bitcoin users' (2018) 13(12) PLoS ONE 1 at p.13.
[281] ibid at p.18.
[282] ibid.

2019 Guidance on Applying Risk Based Approach to Virtual Assets and Virtual Asset Service Providers.

The 2019 guidance issued by the FATF is more comprehensive than the 2015 guidance, but it provides broadly similar advice. The FATF have widened their terminology to 'Virtual Assets' (VAs)[283] and they recommend that its members interpret terms "*such as "property," "proceeds," "funds," "funds or other assets," and other "corresponding value," as including VAs*."[284] This clearly brings cryptocurrencies within the remit of what the FATF recommend should be regulated for AML purposes.

The 2019 guidance terms a VA as a "*digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes.*"[285] The definition specifically discounts digital representations of fiat currencies.[286] The FATF use the term 'Virtual Asset Service Provider' (VASP),[287] to describe businesses providing services for cryptocurrency users, and the definition of the term is wide. The 5 activities are:

I. Exchange between virtual assets and fiat currencies;
II. Exchange between one or more forms of virtual assets;
III. Transfer of virtual assets on [behalf of another natural or legal person]
IV. Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets;

[283] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2019 Acronyms at p3.
[284] ibid at para 33 at p13.
[285] ibid.
[286] ibid.
[287] ibid at Acronyms at p3.

V. Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.[288]

This set of activities will encompass those who provide cryptocurrency services, but it will not require individual users to be regulated, which is in keeping with the regulation of fiat currencies; the financial institutions are regulated, not the individual users of a currency. The FATF approach appears to be to recommend the regulation of the entities which can be regulated, accepting that the cryptocurrency networks cannot be regulated, due to their decentralised nature. The 2019 guidance shows a departure from exclusively regulating at the intersections of cryptocurrencies and fiat currencies, which was recommended in 2015. The FATF stress that the new VASP definition "*includes both virtual-to-virtual and virtual-to-fiat transactions or financial activities or operations*."[289] The 2019 guidance goes on to state that countries should address money laundering risks "*both where those activities intersect with the regulated fiat currency financial system*"[290] and also where the activities "*consist only of "virtual-to-virtual" interactions*."[291] This is a commendable step as the previous approach was leaving potentially suspicious transactions unreported. The guidance makes specific reference to maintaining flexibility, attempting to remain "*technology neutral*"[292] and aims to encompass future developments in VAs, without specific terms being recognised.[293]

[288] ibid at para 33 at p13-14.
[289] ibid.
[290] ibid at para 52 at p18.
[291] ibid.
[292] ibid at para 49 at p17.
[293] ibid.

The 2019 guidance from the FATF demonstrates a commitment to take cryptocurrencies seriously, there is a recognition that "[a]*lmost all of the FATF Recommendations are directly relevant*"[294] to addressing the money laundering risks posed by cryptocurrencies. In keeping with previous advice from the FATF, the risk-based approach is central to the FATF guidance.[295] In applying the risk-based approach the FATF recommends that cryptocurrencies and VASPs be treated as higher risk due to the levels of anonymity allowed by cryptocurrency systems.[296] Identifying an activity as high risk means the enhanced due diligence measures are required of the regulated entity.[297]

To assist members in continuing to adhere to the FATF Recommendations, guidance is provided on the specific Recommendations which are directly relevant to cryptocurrencies. Recommendation 1 concerns countries undertaking a risk assessment and applying the risk-based approach,[298] which the 2019 guidance states should now include VAs and VASPs. The assessment should identify the relevant authorities that should regulate VAs and VASPs, and the treatment of these products and services should be consistent.[299] With regards to Recommendations 3, 4, and 6,

[294] ibid at para 55 at p19.
[295] ibid at para 58 at p19.
[296] ibid.
[297] See recommendation 10 and the relevant explanatory note: Financial Action Task Force, 'The FATF Recommendations' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> accessed 04 April 2019.
[298] See Recommendation 1 and the relevant explanatory note: Financial Action Task Force, 'The FATF Recommendations' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> accessed 04 April 2019.
[299] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2019 para 58 at p19.

which concern creating appropriate offences,[300] enacting a confiscation regime,[301] and asset freezing,[302] the 2019 guidance makes it clear that "*all funds or value-based terms in the Recommendations*"[303] should be interpreted as including VAs.[304] While this guidance is clear it is difficult to put into practice, confiscating cryptocurrency is extremely difficult given that assets are not stored in financial institutions, and for the same reason asset freezing will be impossible without access to an individual's cryptocurrency wallet.

Perhaps the most pertinent of the Recommendations is Recommendation 15 which requires institutions to be aware of, and continue to assess the money laundering risks posed by new products and new business practices.[305] This Recommendation has been updated to specifically mention VASPs, which are to be regulated for AML purposes,[306] which is reiterated in the 2019 guidance.[307] Recommendations 26 and 27 are highlighted in the 2019 guidance, requiring adequate regulatory authorities to be identified and given adequate powers to supervise regulated entities.[308]

[300] See Recommendation 3 and the relevant explanatory note: Financial Action Task Force, 'The FATF Recommendations' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> accessed 04 April 2019.
[301] See Recommendation 4 and the relevant explanatory note: ibid.
[302] See Recommendation 6 and the relevant explanatory note: ibid.
[303] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2019 para 65 at p20.
[304] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2019 para 65 at p20.
[305] FATF Recommendations' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> accessed 28 June 2019 at p15.
[306] ibid.
[307] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2019 para 86 at p23.
[308] ibid at para 86 at p23.

Recommendation 33 requires countries to gather relevant statistics pertaining to their AML systems,[309] the 2019 guidance instructs countries to widen their data gathering to include regulation of VASPs and VA activities. Such statistics include the practice of suspicious activity reporting and reporting transactions over a specified threshold.[310]

Recommendation 10 requires regulated entities to complete customer due diligence (CDD),[311] the 2019 guidance expands this to VASPs,[312] this is consistent with the advice given in 2015.[313] The extension of CDD requirements to VASPs is a logical step, as it is not possible to apply regulation to the cryptocurrency networks, but by applying CDD requirements to exchanges, this theoretically removes the anonymity of the users. This is only true for users that use regulated cryptocurrency exchanges, and the data captured will be limited if the user uses multiple wallets and only registers one with the exchange. The FATF state that the CDD process includes "*understanding the purpose and intended nature of the business relationship, where relevant, and obtaining further information in higher risk situations*."[314] As already identified with the classification of cryptocurrencies as high risk, the CDD required will be enhanced to reflect the risk. The regulated entities will be required to obtain the identity of "*the customer and, where applicable, the customer's beneficial owner*"[315] and verify this information.[316] These requirements may deter some users from using regulated

[309] See Recommendation 33: FATF Recommendations' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> accessed 28 June 2019 at p24.
[310] See Recommendations 10 and 20: ibid.
[311] See Recommendation 10: ibid.
[312] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2019 para 91 at p24.
[313] ibid at para 42 at p12.
[314] ibid at para 91 at p24.
[315] ibid at para 91 at p24.
[316] ibid.

exchanges, due to the data being gathered. VASPs will also be expected to submit SARs where relevant, and per Recommendation 20,[317] have risk management systems in place, adhering to Recommendation 12,[318] and share information with FIUs, compliant with Recommendation 29.[319]

The FATF recommends a licensing system to VASPs, the registration is required to take place "*in the jurisdiction(s) where they are created*."[320] Registration should include records of who operates the VASP, so if owned by a company then the registration should require reference to the relevant register of companies for that jurisdiction.[321] The register should be the responsibility of a designated authority.[322] The 2019 guidance stresses that the "*authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in, a VASP*."[323]

The FATF promote the increasing understanding of cryptocurrencies, the 2019 guidance recommends that in order to develop a deeper understanding, investment is needed in training personnel.[324] This Recommendation mirrors that of the UNODC,

[317] ibid at para 124 at p31.
[318] ibid at para 104 at p27.
[319] ibid at para 129 at p32.
[320] ibid at para 77 at p22.
[321] ibid at para 78 at p22.
[322] ibid at para 77 at p22.
[323] ibid at para 82 at p23.
[324] ibid at para 144 at p35.

which also recommends education.[325] VASPs operate in a different way to existing financial institutions, but many of their functions are also similar.[326]

The FATF provides guidance on how supervisors and authorities can adjust their approach. Examples given by the FATF are that "*supervisors should employ both offsite and onsite access to all relevant risk and compliance information*",[327] vary the frequency of visits, both periodical and ad hoc and issues arise,[328] and regulate to the perceived risks.[329] However these Recommendations are still lacking in detailed guidance to the supervisors, the guidance from the FATF is too vague. The guidance also suggests an intensive response from regulators, which will cost significant amounts of money to train staff and empower supervisors. Given that AML regulation is already criticised by the British Bankers Association for costing its members £5bn per year collectively,[330] it is likely that excessive regulation will deter VASPs from being compliant and make operating outside of the regulation more appealing.

The 2015 FATF guidance recognises that cryptocurrencies provide compliance challenges, and suggests, "*Actors in the VC space should seek to develop technology-*

[325] United Nations Office of Drug Control, 'Basic Manual on the Detection and Investigation of the Laundering of Crime Proceeds Using Virtual Currencies' <https://www.imolin.org/pdf/imolin/FULL10-UNODCVirtualCurrencies_final.pdf> accessed 10 June 2019 at 5.4 on p120.
[326] Examples include: exchange of one asset for another, acting as a broker for buyers and sellers, and holding stock of types of asset so as to provide a market.
[327] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2019 para 153 a) at p37.
[328] ibid at para 153 b) at p37.
[329] ibid at para 153 c) at p37.
[330] British Bankers Association, 'Response to Cutting Red Tape Review, The Effectiveness of The UK's AML Regime' <https://www.bba.org.uk/download-file/?f=eyJ1cmwiOiJodHRwczpcL1wvd3d3LmJiYS5vcmcudWtcL3dwLWNvbnRlbnRcL3VwbG9hZHNcLzIwMTVcLzExXC9CQkEtcmVzcG9uc2UtdG8tQ3V0dGluZy1SZWQtVGFwZS1SZXZpZXctRWZmZWN0aXZlbmVzcy1vZi10aGUtVUtzLUFNTC1SZWdpbWUucGRmIiwibmVlZGxvZ2luIjpmYWxzZSwidXNlciI6ZmFsc2V9> accessed 28 June 2019 at p.2.

based solutions that will improve compliance";[331] such as application, programming interfaces (APIs) to provide identification information.[332] This Recommendation of the FATF highlighted a key weakness in the 2015 FATF guidance, it only applies to situations where cryptocurrencies intersect with fiat currencies, at which point it may be difficult to ascertain the origin of the money as the previous transactions will have taken place inside the cryptocurrency network, and thus outside of the regulated sector. This weakness has been partly addressed in the 2019 guidance, recognising that VASPs providing cryptocurrency exchange services will convert between cryptocurrencies as well as from fiat to cryptocurrency.

The FATF emphasises the importance of intelligence in combatting money laundering, particularly through the requirement for countries creating and coordinating their reporting regime via an FIU, and the record keeping requirements placed in regulated entities. The recommended approach to cryptocurrencies will only monitor the edges of the cryptocurrency networks, key information will not be collected. Despite the shortcomings in the FATF guidance, it has been the proactive international body with regards to addressing the money laundering risks posed by cryptocurrencies.

4.8.3. Summary of the FATF's Approach to risks of Money Laundering using Cryptocurrencies

The FATF guidance is not binding on its members; all of the case study jurisdictions are members, but they are not compelled to follow the advice. The status of the

[331] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2019 para 51 at p14.
[332] ibid at para 52 at p14.

Recommendations is that they too are advisory as they are soft law, members of the FATF are expected to comply with them, but no member of the FATF is fully compliant. As observed by Alexander, the FATF has been a powerful driver of reform, giving the example of mandatory suspicious transaction reports, which were *virtually non-existent before the FATF came into being, are in place in all but one of the FATF member jurisdictions.*[333] It is observed that the present advice of the FATF is that states should apply a risk-based approach to cryptocurrencies, regardless of their specific legal treatment of them. This advice has been developed in 2019 to recommend the regulation of VASPs, and the remit of the regulation has been broadened to some transactions which do not involve fiat currencies, such as from one cryptocurrency to another. The weakness of the FATF advice is that it is still using its existing Recommendations, and applying them to cryptocurrencies, and the advice amounts to designating all VASPs as high risk and applying the highest level of regulation possible, which is likely to cause backlash from VASPs. The FATF should heed its own guidance and seek a deeper understanding of cryptocurrencies. As Recommendation 36 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation' states, international harmonisation is required, and through the FATF's position this may be the way this is achieved. Another body which may achieve harmonisation, on a European scale, is the EU.

[333] cf Alexander (n225) at p244.

4.9. European Union

The EU is a unique, supranational organisation; "*Member States of the European Union have agreed, as a result of their membership of the EU, to transfer some of their powers to the EU institutions in specified policy areas*."[334] The initial aims of the EU were to *foster economic cooperation*[335] between six countries: Belgium, Germany, France, Italy, Luxembourg and the Netherlands.[336] The EU now has 28 members;[337] although the UK is in the process of leaving the EU, until the process has been organised and completed, "*the United Kingdom remains a full member of the EU and rights and obligations continue to fully apply in and to the UK*.[338] As well as its size, the nature of the EU has changed considerably since its inception; it has developed into a single market and a "*unique economic and political union*"[339] which has the power to prescribe legislation to its Member States.

4.9.1. Anti-Money laundering policy

The EU began combatting money laundering in the 1970s[340] through the European Committee on Crime Problems (CDPC),[341] which created a Select Committee to assess the transfer of criminal proceeds between Member States,[342] and first

[334] European Parliament, 'Supranational decision-making procedures' <http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuId=FTU_1.4.1.html> accessed 05 September 2019.
[335] The European Union, 'The EU in Brief' <https://europa.eu/european-union/about-eu/eu-in-brief_en> accessed 26 August 2016.
[336] ibid.
[337] EUROPA, 'Countries' <https://europa.eu/european-union/about-eu/countries_en#28members> accessed 03 September 2019.
[338] ibid.
[339] The European Union, 'The EU in Brief' <https://europa.eu/european-union/about-eu/eu-in-brief_en> accessed 26 August 2016.
[340] cf Ryder (n57) at p.18.
[341] Council of Europe, 'European Committee on Crime Problems' <http://www.coe.int/en/web/cdpc> accessed 03 September 2019.
[342] cf Ryder (n57) at p.18.

published its findings in 1980.[343] Prior to legislating through directives, the EU adopted the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime[344] (1990 Council of Europe Convention), which was open for members and non-member states to sign.[345] The 1990 Council of Europe Convention was not widely adopted when it was first created,[346] the reasons for the poor uptake are not clear. Gilmore states that the drafters were keen to "*protect the advances which has so recently been made*" [347] by the Vienna Convention 1988. The Council of Europe convention went further than the Vienna Convention 1988, as signatories were required to criminalise money laundering generally, rather than specifically in relation to drug trafficking.[348] The first EU AML legislation was the 1991 First Money Laundering Directive;[349] measures included identifying customers, record keeping, refraining from tipping off customers being investigated, and a proactive duty to report suspicious transactions to the competent national authorities.[350] Mitsilegas and Gilmore criticised the Directive as it was not specific enough,[351] which led to Member States implementing the directive in different ways, and hindered cooperation across the EU. This demonstrates an issue with directives which is borne out of the flexibility they provide, Member States are allowed to devise the best solution for their jurisdictions, and those solutions may be too different to achieve harmony. Money

[343] Council of Europe 'Council of Europe Committee of Ministers Recommendation No. R (80) 10' <https://rm.coe.int/16804f6231> accessed 01 September 2019.
[344] Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (adopted 08 August 1990, entered into force 01 September 1993) ETS 141 (1990 Council of Europe Convention).
[345] Council of Europe, 'Details of Treaty No.141' <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/141> accessed 27 September 2019.
[346] cf Gilmore (n71)at p162.
[347] ibid.
[348] ibid.
[349] 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 L166/77.
[350] cf Mitsilegas and Gilmore (n106) at 120.
[351] ibid.

laundering is a common problem which may be addressed differently in different jurisdictions, it is an example where Craig and de Búrca's observation is particularly true; "*Member States have differing legal systems, and there are variations in the political, administrative, and social arrangements within the Member States.*"[352] The task for EU legislators is therefore to devise legislation which is flexible enough to allow Member States to devise appropriate measures for their jurisdictions, but also be prescriptive enough to provide consistency across the EU. The 1st Directive was amended by the 2nd Directive in 2001,[353] and required any potentially new Member States to adopt the Money Laundering Directives as a prerequisite of entry.[354] In 2005 the First and Second Directives were then merged into the Third Directive;[355] the EU approach to AML mirrors that of the FATF Recommendations, Ryder states that the EU Directives require Member States to adopt a risk-based approach; prioritising institutions, individuals, or services that are most at risk to money laundering. Also in 2005, the EU amended the 1990 Council of Europe Convention with the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism.[356] As observed in the AML timeline,[357] the 2005 Convention coupled money laundering with terrorist financing which confuses the issue and undoes the progress made in the 1990's to recognise money

[352] P Craig and G. de Búrca, EU Law: Text Cases and Materials (6th edn, Oxford University Press, 2015). at p.108.
[353] 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 [2001] OJ L.344/76.
[354] cf Ryder (n57) at p.34.
[355] 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 [2005] OJ L.309/15.
[356] Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (adopted 16 May 2005, entered into force 01 May 2005 CETS 198 (2005 Council of Europe Convention).
[357] See 4.7 above.

laundering as an issue in itself. The present AML legislation of the EU is contained in Directive 2018/843,[358] known as the 5th AML Directive, which amends Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing,[359] known as the 4th Directive.

4.9.2. The 4th Money Laundering Directive

As discussed already, directives set a minimum standard for Member States to attain, the; directives are goal driven, and the Member States can reach that goal through passing their own laws. Fortson notes that, as with the earlier directives, "[m]*uch of the 4th Directive restates pre-existing measures*";[360] this is because each of the money laundering directives replaces the previous one. The preamble to the 4th Directive highlights the international nature of money laundering, and that the "*measures adopted by the Union in that field should therefore be compatible with, and at least as stringent as, other actions undertaken in international fora*"[361] in light of this the Directive seeks to be aligned with the Recommendations of the FATF.[362]

[358] Council Directive 2018/843/EU 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 L 156/43.
[359] Directive 2015/849/EU 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 [2015] OJ L.141/73.
[360] R. Fortson, 'Intensifying anti-money laundering laws - the last 30 years' (2016) 4 Arch Rev 6
[361] Directive 2015/849/EU 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 [2015] OJ L.141/73 preamble para 4.
[362] ibid.

The intended correlation between the EU approach and the FATF is clear from the first requirement of the Directive, which is for Member States is to criminalise money laundering.[363] Article 4 then makes it clear that the risk based approach should be adopted in applying the Directive to "*activities which are particularly likely to be used for the purposes of money laundering.*"[364] In pursuing the risk based approach, the Commission will conduct an assessment of the money laundering risks affecting both internal and cross border activities.[365] Member States will conduct their own risk assessments,[366] and regulated institutions should also complete their own assessments.[367] Chapter 2 of the Directive covers customer due diligence (CDD) requirements,[368] namely when CDD measures should be applied and what details should be gathered. Circumstances where CDD is to be applied include; when establishing a new business relationship,[369] when transactions values meet certain thresholds,[370] where money laundering is suspected,[371] or the previously obtained information is questioned.[372] Article 13 outlines what CDD consists of, such as obtaining the verified identify of the customer,[373] the nature of the business relationship,[374] and the beneficial owner of the money or goods being transferred.[375] The Directive is clear that the CDD procedures should take place before the respective business relationship is established, or transaction takes place.[376] The Directive is

[363] ibid at Article 1(2).
[364] ibid at Article 4(1).
[365] ibid at Article 6(1).
[366] ibid at Article 7(1).
[367] ibid at Article 8(1).
[368] ibid at Chapter II: Customer Due Diligence.
[369] ibid at Article 11(a).
[370] ibid at Article 11(b)-(c).
[371] ibid at Article 11(e).
[372] ibid at Article 11(f).
[373] ibid at Article 13(1)(a).
[374] ibid at Article 13(1)(c).
[375] ibid at Article 13(1)(b).
[376] ibid at Article 14(1).

committed to the risk based approach, and Section 2 Chapter 2 makes it clear that in low risk circumstances a simplified CDD process can be applied,[377] whereas Section 3 states that in high risk circumstances, enhanced CDD is required.[378] There are similarities between the 4th Directive and the Recommendations of the FATF in relation to CDD; the wording of some of respective sections detailing when CDD is to be applied is nearly identical,[379] and the threshold of €15,000 is the same.[380] The information required to be gathered is very similar, the identity of the customer is a priority, as well as focussing establishing the beneficial owner of the property and the purpose of the business relationship.[381]

Chapter 4 of the Directive outlines the reporting obligation Member States should establish in their jurisdictions. The first stipulation, in Article 32, is that "[e]*ach Member State shall establish an FIU in order to prevent, detect and effectively combat money laundering*".[382] A Financial Intelligence Unit (FIU) is also prescribed by the FATF Recommendations,[383] and both the EU and the FATF expect FIUs to be to the organisation where reports produced to comply AML legislation are sent and analysed. The reports which are to be sent to the FIU are produced by regulated institutions, the

[377] ibid at Articles 15-17.
[378] ibid at Articles 18-24.
[379] See Article 11(a) and (f) compared to Recommendation 10 (i) and (iv).
[380] Financial Action Task Force, 'The FATF Recommendations' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> accessed 05 July 2019 at p12.
[381] ibid.
[382] Directive 2015/849/EU 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 [2015] OJ L.141/73 Article 32.
[383] Financial Action Task Force, 'The FATF Recommendations' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> accessed 05 September 2019 at p9.

Directive requires a regulated entity to report if it "*knows, suspects or has reasonable grounds to suspect that funds, regardless of the amount involved, are the proceeds of criminal activity*",[384] this form or reporting is known as a suspicious activity report (SAR). Article 39 prohibits the disclosure of the SAR to the customer concerned or third persons,[385] this is to prevent the potential money launderer being tipped off that their transaction has been flagged, and taking steps to protect themselves from a potential investigation. Article 39 is comparable to FATF Recommendation 21 which states that regulated entities should be "*prohibited by law from disclosing ("tipping-off") the fact that a suspicious transaction report (STR) or related information is being filed with the FIU*."[386]

"*Member States shall require the competent authorities to monitor effectively, and to take the measures necessary to ensure, compliance with*"[387] the Directive. As part of this each Member State should ensure the relevant authorities have "*adequate powers*"[388] to monitor compliance, and to have the required "financial, human and technical resources to perform their functions."[389] This is an area of the Directive which is quite broad, giving no floors or ceilings as to the resources Member States should

[384] Directive 2015/849/EU 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 [2015] OJ L.141/73 Article 33(1)(a).
[385] ibid at Article 39.
[386] Financial Action Task Force, 'The FATF Recommendations' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> accessed 05 September 2019 at p17.
[387] Directive 2015/849/EU 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 [2015] OJ L.141/73 Article 48.
[388] ibid at Article 48(2).
[389] ibid.

make available to the regulators, which could lead to disparities between the standards on regulation in Member States. The FATF Recommendations are also not completely clear as to what constitutes adequate regulation, but the mutual evaluation programme of the FATF can address attainment of the Recommendations in FATF members. Another board Article of the Directive is Article 49 which concerns cooperation between national authorities, as with providing adequate resources, it is difficult to quantify or set standards in cooperation and as such Member States will vary in their levels of national cooperation. Article 49 mirrors part of Recommendation 2 of the FATF.[390]

It can be seen that in places the 4th Money Laundering Directive is quite prescriptive in what is required of Member States, particularly in relation to customer due diligence and suspicious activity reporting, but in other areas there is still the potential for the standards in Member States to be very different. It can be seen that the EU's approach to money laundering is very similar to that of the FATF, it follows a risk-based approach and places an emphasis on intelligence gathering through CDD and SARs. Both the EU and FATF require an FIU to be at the centre of a country's information gathering process, and that compliance with preventative measures is overseen by an 'adequately' resourced authority. The 4th Directive is silent on the issue of cryptocurrencies, this is addressed in the 5th Anti-Money Laundering Directive.

[390] Financial Action Task Force, 'The FATF Recommendations' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> accessed 05 September 2019 at p9.

4.9.3. Policy towards cryptocurrencies

As identified in chapter three, the European Central Bank (ECB) has defined virtual currencies in 2012 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*."[391] The ECB subsequently released further analysis in 2015,[392] and while it stated that its position on virtual currencies remained consistent with the 2012 report, it has modified its definition of virtual currencies. Virtual currencies are now defined as "*a digital representation of value, not issued by a central bank, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money.*" The notable differences between the definitions show that attitudes towards cryptocurrencies are changing, the word 'unregulated' has been removed; cryptocurrencies are no longer referred to as 'digital money' instead they are referred to as a 'representation of value' and an 'alternative to money'; and an emphasis is now placed on cryptocurrencies not being issued by a central bank, rather than defining who issues and controls the cryptocurrency. The new definition shows that institutions within the traditional financial system are attempting to understand cryptocurrencies, rather than simply dismiss them.

[391] ECB, 'Virtual Currency Schemes' <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> accessed 02 June 2019 at p13.
[392] ECB, 'Virtual currency schemes – a further analysis' <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> accessed 11 September 2019.

5th Anti-Money Laundering Directive

Further evidence that the EU is recognising cryptocurrencies, particularly the money laundering risks, is through the 5th Anti-Money Laundering Directive.[393] In July 2016, only a year after the 4th Directive was enacted, a revision was proposed by the Commission, which included "*tackling terrorist financing risks linked to virtual currencies*".[394] By virtue of the EU's approach to money laundering being entangled with terrorist financing, the revision to the Directive in relation to terrorist financing would also apply to money laundering. The 5th Anti-Money Laundering Directive adds "*virtual currency exchange platforms as well as custodian wallet providers to the list of obliged entities within the scope of the Directive*;"[395] which mirrors the guidance of the FATF with regards to bringing points of intersection between cryptocurrencies and the traditional financial system under the scope of EU AML regulations. While this is a positive step, it presents the same short comings as identified in the FATF guidance, the measures only apply to businesses exchanging cryptocurrency for fiat currency and will leave a large proportion of the cryptocurrency network outside of AML regulation.

[393] Council Directive 2018/843/EU 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 L 156/43.
[394] EUROPA, 'Revision of the Anti-Money Laundering Directive (AML). Countering Terrorist Financing' <http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-revision-of-the-anti-money-laundering-directive-(aml)> accessed 01 September 2019.
[395] EUROPA, 'Revision of the Fourth Anti-Money-Laundering Directive' <http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/607260/EPRS_BRI%282017%29607260_EN.pdf> accessed 10 September 2019.

4.9.4. Summary EU's Approach to risks of Money Laundering using Cryptocurrencies

The EU is in a unique position to legislate in its Member States, this gives it the opportunity to be a world leader in regulating new phenomenon; if it were to be bold and regulate cryptocurrencies it would be likely to set the global trend due to the size of the economies within it. Despite this power, the EU is a complex organisation, and it has ignored its own advice in the past when given the opportunity to create world leading legislation, specifically in the 1980s and 1990s where the EU approved the CDPC Select Committee recommendations but ultimately did not adopt the recommendations.[396] The EU has expanded its AML regime to the same level as the guidance of the FATF, which demonstrates an international consistency, but one which falls short of addressing the issues posed by cryptocurrencies.

4.10. Summary

The origins of money laundering can be seen to be as difficult to trace as it is to prevent or pursue; the nature of money laundering would suggest it is as old as crime itself, but the modern concept can be seen to have its origins in the 1920s.[397] The history of AML legislation is also not straightforward, it can be seen that governments and international organisations have struggled with defining, measuring, isolating, and preventing money laundering. The international approach has its origins in the UN's predecessor, the League of Nations, but the UN took until 2000 to decouple money laundering from the drugs trade, before which the two criminal activities had been

[396] See 4.7.3-4 above and: N. Ryder, *Financial Crime in the 21st Century: Law and Policy* (Edward Elgar, Cheltenham, 2011) at p.18.
[397] M. Levi, R Naylor and P Williams, *Financial Havens, Banking Secrecy and Money Laundering* (New York, 1998).at p.12.

approached together rather than recognised as individual. Conversely, individual jurisdictions such as the US, the UK and Australia recognised that money laundering was not confined to the drugs trade much earlier than the UN, yet these jurisdictions have since confused the area by entwining money laundering and counter terrorist financing. Assessing the origins of the modern crime of money laundering and the development of the fight against it, it is a quirk that the term originates from the affairs of the President of a country that now takes a global lead in its prevention. It is clear that money laundering remains impossible to accurately measure, and that the globalised nature of the modern world means it has become, more than ever, a global problem. Cryptocurrencies fit within a globalised world, without recognising physical borders, which suits money launderers and it is this suitability which forms the main reasoning for the contention; cryptocurrencies are appealing to money launders and their characteristics make them vulnerable to money laundering.

The role of the UN in AML best practice grew over the latter half of the 20th century but has subsided since the creation of the FATF and the development of the EU, who set the modern agenda in international AML developments; this is clearly observed in relation to cryptocurrencies. The UN has been absent in addressing the threats posed by cryptocurrencies, whereas the FATF and the EU are instigating a widening of the AML regulatory perimeter to include cryptocurrencies. The regulation recommended by the FATF is a first step to addressing the money laundering concerns posed by cryptocurrencies, as the regulation of cryptocurrency service providers will only regulate the edges of cryptocurrency networks. The EU's 5th Anti-Money Laundering Directive mirrors the guidance of the FATF, and therefore mirrors its flaws. Both the EU and the FATF should encourage the development of applications which can utilise

wealth of data available through publicly available blockchains. In 2015, the FATF has suggested "*actors in the VC space should seek to develop technology-based solutions that will improve compliance*";[398] such as application programming interfaces (APIs) to provide identification information,[399] but this has not led to published results.

The next chapter analyses the money laundering laws of the UK, assessing their applicability to cryptocurrencies. The chapter also analyses the existing AML measures of the UK and highlights the need for reform to widen the regulatory perimeter to cover cryptocurrencies.

[398] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2019 para 51 at p14.
[399] Financial Action Task Force, 'Guidance for A Risk-Based Approach to Virtual Currencies' <https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf> accessed 01 August 2019, para 52 at p14.

Chapter 5. United Kingdom

5.1. Chapter Overview

This chapter will outline the United Kingdom's (UK) approach to money laundering. It will analyse both the criminal offences and the preventative measures, and subsequently, the applicability of the law to cryptocurrencies will be assessed. As well as the law, the response to cryptocurrencies in the UK will be considered through the reactions of the relevant authorities. The anti-money laundering (AML) approach of the UK has similarities to that of the US and Australia, in that the combatting of money laundering has two clear elements; criminalisation and preventative measures. The preventative measures can further be divided into know your customer, or customer due diligence (CDD), and suspicious activity reports (SARs); both of these types of measures are intended to increase financial intelligence.

This chapter will first assess the UK money laundering offences, determining whether they may be committed using virtual currencies. Sections 327-329 of the Proceeds of Crime Act 2002 (POCA 2002) are found to be applicable to cryptocurrencies, and cryptocurrencies are identified as capable of being criminal property under s.340. Confiscation of cryptocurrencies is not the focus of these thesis, but it presents a further complication in money laundering cases and an avenue for future research.[1] It is clear that cryptocurrencies are capable of being criminal property, and be confiscated, but clarity is needed in what the accepted procedure is for dealing with

[1] For a detailed analysis of international trends in asset recovery see: C. King, C. Walker and J. Gurulé, *The Palgrave Handbook of Criminal and Terrorism Financing Law, Volume 1* (Palgrave Macmillan, 2018) Part III.

seized cryptocurrency. Following analysis of the criminal offences, it will be considered whether cryptocurrency service providers should be subject to CDD and reporting requirements under the AML legislation of the UK. It is argued that the AML regulation could, and should, already be applied. Once the legislation has been analysed the regulatory agencies will be considered, first the primary authorities and then the secondary authorities; their role will be considered in relation to the UK AML approach, with particular focus on the Financial Conduct Authority (FCA) and the Government. Having established the roles of the authorities, then special attention will be given to the relevant authorities' approach to cryptocurrencies, which, to date, has been limited to consultations rather than regulation. Lastly, reforms will be considered with regard to the applicability of the law to cryptocurrencies, it is recommended that the guidance of the Financial Action Task Force (FATF) is adopted, but that the UK goes further than the guidance and seeks to develop novel approaches to the money laundering threat posed by cryptocurrencies. Development of technology to automate analysis of the blockchain is proposed, to utilise the wealth of transaction data available.

5.2. AML Approach

The approach to money laundering in the UK has two broad elements, criminalisation and preventive measures. Money laundering is criminalised through POCA 2002,[2] and the Money Laundering Regulations 2017[3] provide the preventative measures which are administered by the supervisory authorities set out in Regulation 7.[4] While not the only supervisory authority, the analysis of the UK AML approach will focus on the

[2] Proceeds of Crime Act 2002.
[3] Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (Money Laundering Regulations 2017).
[4] Money Laundering Regulations 2017, reg.7.

Financial Conduct Authority (FCA) as it is the authority with the widest responsibility, which includes "*credit and financial institutions (including money service businesses)*",[5] and "*electronic money institutions*",[6] which are the most relevant institutions to cryptocurrencies. The UK has relatively long history of creating AML legislation, and first criminalised money laundering by virtue of the Drug Trafficking Offences Act 1986.[7] As demonstrated in chapter four, the UK has traditionally kept place with international standards, first legislating in the same year as the US, and is a founding member of the FATF.[8] In 2018 mutual evaluation report, the FATF found the UK had *"implemented an AML/CFT system that is effective in many respects*",[9] but that "*improvements are needed to strengthen supervision and implementation of preventive measures, and ensure that financial intelligence is fully exploited*."[10] The UK AML approach must be analysed and applied to cryptocurrencies, and the concerns of the FATF explored.

5.3. Criminalising Money Laundering

The UK money laundering offences are found in Part 7 of POCA 2002,[11] specifically ss.327-333. The three main offences are concealing,[12] arrangements,[13] and

[5] ibid reg.7(a)(i).
[6] ibid reg.7(a)(iv).
[7] Drug Trafficking Offences Act 1986.
[8] FATF, 'United Kingdom' <https://www.fatf-gafi.org/countries/#United%20Kingdom> accessed 11 September 2019.
[9] FATF, 'Anti-money laundering and counter-terrorist financing measures – United Kingdom, Fourth Round Mutual Evaluation Report' (Paris, December 2018) <fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-Kingdom-2018.pdf> accessed 11 September 2019 at para 4.
[10] ibid.
[11] Proceeds of Crime Act 2002, Part 7.
[12] ibid s.327.
[13] ibid s.328.

acquisition, use and possession.[14] In addition to the money laundering offences there are the offences of failing to disclose knowledge of money laundering[15] and tipping off the suspect.[16]

5.3.1. Money Laundering Offences – s.327, s.328, and s.329

Section 327 sets out the concealing offence, which is satisfied if a person conceals,[17] disguises,[18] converts,[19] transfers,[20] or removes[21] "*criminal property from England and Wales or from Scotland or from Northern Ireland.*"[22] The focus of the offence is upon the movement of property, there is no requirement that the movement be of a financial nature, which allows a wide gamut of activity to satisfy the offence. The arrangements offence is set out in s.328; "*a person commits an offence if he enters into or becomes concerned in an arrangement which he knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person.*"[23] The use of the phrase "*by whatever means*"[24] indicates a very wide interpretation, which may be applied to any number of varying arrangements. Finally, Section 329 sets out the acquisition offence; a person commits an offence if they acquire,[25] use,[26] or possess[27] criminal property. Each of the POCA offences is drafted widely, allowing a range of activities to satisfy the offence, while the offences are

[14] ibid s.329.
[15] ibid s.332.
[16] ibid s.333.
[17] ibid s.327(1)(a).
[18] ibid s.327(1)(b).
[19] ibid s.327(1)(c).
[20] ibid s.327(1)(d).
[21] ibid s.327(1)(e).
[22] ibid s.327(1).
[23] ibid s.328(1).
[24] ibid.
[25] ibid s.329(1)(a).
[26] ibid s.329(1(b).
[27] ibid s.329(1)(c).

commonly referred to as ‘money laundering offences’ they need not involve any recognisable money changing hands, the focus is on property or value being transferred.

Money laundering convictions have been obtained where Bitcoin has been used. In 2018 Bitcoin worth over £1.2million was seized and Sergejs Teresko was sentenced to 9 years imprisonment,[28] and in April 2019 Thomas White was convicted of a number of offences, including money laundering related to £192,000 worth of Bitcoins.[29] These examples demonstrate that the UK offences are interpreted as being wide enough to include cryptocurrency activity.

5.3.2. Criminal Property

UK money laundering offences exist entirely separately from the offences which the criminal property heralds from; an individual will be found guilty of money laundering even if they did not commit the crime which produced the criminal property, or benefit from the criminal property. Section 340(4) makes it clear that it does not matter “*who carried out the conduct;*”[30] “*who benefited from it;*”[31] or “*whether the conduct occurred before or after the passing of*”[32] POCA 2002. The stipulation in s.340(4)(c) further demonstrates the separation of the offence from the laundering process; it should be

[28] *R* v *Teresko* [2018] Crim LR 81, Crown Prosecution Service, ‘More than £1.2million of Bitcoin seized from drug dealer’ (19 July 2018) <https://www.cps.gov.uk/south-east/news/more-ps12-million-bitcoin-seized-drug-dealer> accessed 11 September 2019.
[29] BBC News, ‘Liverpool 'dropout' jailed for Silk Road dark web site’ (12 April 2019) <https://www.bbc.co.uk/news/uk-england-merseyside-47913780> accessed 11 September 2019 and National Crime Agency, ‘Student behind $100m dark web site jailed for 5 years 4 months’ (12 April 2019) <https://www.nationalcrimeagency.gov.uk/news/student-behind-100m-dark-web-site-jailed-for-5-years-4-months?highlight=WyJiaXRjb2luIiwiYml0Y29pbnMiXQ==> accessed 11 September 2019.
[30] Proceeds of Crime Act 2002, Part 7, s.340(4)(a).
[31] ibid s.340(4)(b).
[32] ibid s.340(4)(c).

made clear that this does not give the Act retrospective effect, but it does mean that the money laundering offences are stand-alone offences and do not require a conviction for the offence from which the criminal property emanates.

Section 340(3) of POCA focusses on the benefits of the property rather than defining what can and cannot constitute property. Criminal property is anything that "*constitutes a person's benefit from criminal conduct or it represents such a benefit*",[33] which "*the alleged offender knows or suspects*"[34] is such a benefit. The definition recognises that the proceeds of crime are often broken up to avoid detection, as such the criminal property may represent a benefit "*in whole or part*"[35] and can be direct or indirect.[36] This wide definition of criminal property can therefore encompass the broad array of assets which may be used to disguise illegal gains. While no definition of cryptocurrency exists in law, the courts have clearly viewed it as property, as demonstrated by the convictions of *Teresko*[37] and *White*.[38] The confiscation and restraint of Bitcoins is a further demonstration of the courts viewing cryptocurrency as property. Hall observes that in the Teresko case Bitcoin was accepted as "*realisable property*",[39] which includes intangible property,[40] satisfying s.84(1) of POCA[41] and

[33] ibid s.340(3)(a).
[34] ibid s.340(3)(b).
[35] ibid s.340(3)(a).
[36] ibid.
[37] Crown Prosecution Service, 'More than £1.2million of Bitcoin seized from drug dealer' (19 July 2018) <https://www.cps.gov.uk/south-east/news/more-ps12-million-bitcoin-seized-drug-dealer> accessed 11 September 2019.
[38] National Crime Agency, 'Student behind $100m dark web site jailed for 5 years 4 months' (12 April 2019) <https://www.nationalcrimeagency.gov.uk/news/student-behind-100m-dark-web-site-jailed-for-5-years-4-months?highlight=WyJiaXRjb2luIiwiYml0Y29pbnMiXQ==> accessed 11 September 2019.
[39] J Hall, 'Restraint orders: R. v Teresko (Sergejs) Kingston Crown Court: HH Judge Lodder QC: unreported 11 October 2017' (2018) 1 CLR 81 at 82.
[40] ibid.
[41] Proceeds of Crime Act 2002, s.84(1).

allowing a s.41[42] restraint order to be obtained. Confiscation and restraint can be complicated in relation to cryptocurrency as the lack of a centralised authority means law enforcement agencies are dependent upon obtaining the login details of the offender in order to access their cryptocurrency wallet. When using fiat currency with traditional financial institutions, an institution can assist the law enforcement agencies. Tracking and obtaining cryptocurrency holdings can be a time-consuming process for the police, the recent seizure of Bitcoins from Grant West followed a "*lengthy police investigation*"[43] and involved undercover police officers following West onto a train to view him logging into his accounts and catching him with "*fingers on the keyboard*".[44] The volatility of cryptocurrency values presents a further complication when seizing laundered money, as demonstrated by the cases of Teresko and West. Teresko's 295 Bitcoins[45] were seized in April 2017,[46] at the end of April 2017 that quantity of Bitcoins was worth £298,649,[47] by the time of the court order on 11 October 2017,[48] the value of the 295 Bitcoins was £1,057,911.[49] Reports of the value of Bitcoins seized from Teresko vary depending on the date each source took their exchange rate from, a further demonstration of the volatility in cryptocurrency values. Likewise, in the case of West the value of the Bitcoins at the time of seizure in September 2017[50] was

[42] ibid s.41.
[43] Brett Wilson LLP, 'Bitcoin seized as 'realisable assets' in confiscation proceedings' (London, 03 September 2019) <https://www.brettwilson.co.uk/blog/bitcoin-seized-as-realisable-assets-in-confiscation-proceedings/> accessed 12 September 2019.
[44] M. Busby, 'Bitcoin worth £900,000 seized from hacker to compensate victims' The Guardian (London, 23 August 2019).
[45] cf Hall (n39) at 81.
[46] BBC News, 'Criminal's Bitcoin seized in Surrey Police first' (Surry, 21 July 2018) <https://www.bbc.co.uk/news/uk-england-surrey-44896665> accessed 12 September 2019.
[47] Based on a value of 1 Bitcoin = £1012.37: XE, 'XE Currency Charts: XBT to GBP' <https://www.xe.com/currencycharts/?from=XBT&to=GBP&view=5Y> accessed 12 September 2019.
[48] *R* v *Teresko* [2018] Crim LR 81 (Unreported).
[49] Based on a value of 1 Bitcoin = £3586.14: XE, 'XE Currency Charts: XBT to GBP' <https://www.xe.com/currencycharts/?from=XBT&to=GBP&view=5Y> accessed 12 September 2019.
[50] Brett Wilson LLP, 'Bitcoin seized as 'realisable assets' in confiscation proceedings' (London, 03 September 2019) <https://www.brettwilson.co.uk/blog/bitcoin-seized-as-realisable-assets-in-confiscation-proceedings/> accessed 12 September 2019.

£3,104.12 per Bitcoin[51] and by the time the court order for confiscation was given the value has increased to £8,324.81 per Bitcoin,[52] which led to £922,978.14 being confiscated.[53] While the value fluctuations have been beneficial in recent confiscations, this will not always be the case and the time between the initial seizure and the court order for converting the property into Pounds may lead to substantially lower value asset recoveries.

Once the cryptocurrency is confiscated there are currently two options for authorities wishing to convert the currency, they can either use a cryptocurrency exchange or sell the cryptocurrency at public auction, Hall observes that the US approach is use public actions, whereas Dutch authorities use exchanges.[54] The UK approach is unclear, in the Teresko case an exchange was used,[55] but in 2019 a UK police force used the public auction method for the first time.[56] Confiscation of cryptocurrencies is not the focus of these thesis, but it presents a further complication which cryptocurrencies present, and an avenue for future research.[57] King notes the importance of confiscation in the fight against organised crime, using the language used by Tony Blair in 1999 while UK Prime Minister, who said that "*we want to ensure crime doesn't*

[51] Based on a value of 1 Bitcoin = £3104.12: XE, 'XE Currency Charts: XBT to GBP' <https://www.xe.com/currencycharts/?from=XBT&to=GBP&view=5Y> accessed 12 September 2019.
[52] Based on a value of 1 Bitcoin = £8324.81: XE, 'XE Currency Charts: XBT to GBP' <https://www.xe.com/currencycharts/?from=XBT&to=GBP&view=5Y> accessed 12 September 2019.
[53] BBC News, 'Prolific Sheerness hacker ordered to pay back £922k' (Kent, 23 August 2019) <https://www.bbc.co.uk/news/uk-england-kent-49450676> accessed 12 September 2019.
[54] cf Hall (n39) at 82.
[55] ibid.
[56] Wilsons Auctions, '£500k of bitcoin seized from UK criminal to be auctioned, with no reserve!' (19 September 2019) <https://www.wilsonsauctions.com/news/500k-of-bitcoin-seized-from-uk-criminal-to-be-auctioned-with-no-reserve/> accessed 30 September 2019
[57] For a detailed analysis of international trends in asset recovery see : C. King, C. Walker and J. Gurulé, *The Palgrave Handbook of Criminal and Terrorism Financing Law, Volume 1* (Palgrave Macmillan, 2018) Part III.

pay."[58] It is clear that cryptocurrencies are considered criminal property, and can be confiscated, but clarity is needed in what the accepted procedure is for dealing with seized cryptocurrency.

5.3.3. Sentences

A conviction for an offence under section 327, 328, or 329 is punishable by prison sentence of up to 14 years, a fine not exceeding the statutory minimum, or both. The Sentencing Council issue guidance for courts in England and Wales, releasing updated guidance for money laundering offences in 2016.[59] While the maximum sentence is 14 years, the guidelines state that this length of sentence should be reserved for offenders laundering £10 million or more and with the highest level of culpability. Indicators of high culpability may include; taking a leading role in a group of offenders or pressuring others to take part, the length of time the offender was involved, and whether the money laundering was complex or required significant planning. As established earlier in this chapter, laundering money using cryptocurrencies can satisfy the relevant criminal offences, it is also clear from the sentencing guidelines that the use of cryptocurrencies, and the complexity they add, will mean offenders will likely to be held to a high culpability. The average prison sentence for money laundering reached an all-time high of 27 months in 2018,[60] up

[58] C. King, 'Asset Recovery: An Overview' in C. King, C. Walker and J. Gurulé, *The Palgrave Handbook of Criminal and Terrorism Financing Law, Volume 1* (Palgrave Macmillan, 2018) at p.377.
[59] Sentencing Council, 'Fraud, bribery and money laundering offences: Definitive guideline' <https://www.sentencingcouncil.org.uk/wp-content/uploads/Fraud-bribery-and-money-laundering-offences-Definitive-guideline2.pdf> accessed 15 September 2019.
[60] Financial Times, 'Length of UK prison terms for money launderers hits record high' (1 September 2019) <https://www.ft.com/content/846c0e5c-c9a4-11e9-af46-b09e8bfe60c0> accessed 12 September 2019.

from 20.5 months in 2008.[61] Fines for money laundering are increasingly uncommon, in 2013 fines were issued in 15% of money laundering cases, compared to just 7% in 2018.[62] Cases involving cryptocurrencies remain rare, and each of the three cases above concern multiple offences in addition to money laundering, so it is difficult to generalise in relation to sentence length. White was sentenced to 5 years and 4 months, for approximately £192,000 laundered in Bitcoins in addition to drug offences and trading in child sex images.[63] Teresko was jailed for 9 years and 4 months for money laundering and drug offences, the assets involved were valued at over £1million.[64] Finally, West was jailed for 10 years and 8 months, his convictions were for fraud, computer misuse, and drug offences, and his cryptocurrency was seized as the proceeds of his crime.[65] The sentences demonstrate that cryptocurrencies will add to the complexity of the money laundering scheme, and raise the level of culpability, but factors such as the value of money involved and the severity of the predicate offences the offender has been convicted of will also influence the length of the sentence.

It is clear from this assessment of the UK money laundering offences that these may be committed using cryptocurrencies, and convictions have been obtained. Having

[61] F Cameron, 'Sentences for money laundering getting longer: research' (Pinsent Masons LLP, OUT-LAW, 2 September 2019) <https://www.pinsentmasons.com/out-law/news/sentences-for-money-laundering-getting-longer-research> accessed 12 September 2019.
[62] ibid.
[63] BBC News, 'Liverpool 'dropout' jailed for Silk Road dark web site' (12 April 2019) <https://www.bbc.co.uk/news/uk-england-merseyside-47913780> accessed 11 September 2019 and National Crime Agency, 'Student behind $100m dark web site jailed for 5 years 4 months' (12 April 2019) <https://www.nationalcrimeagency.gov.uk/news/student-behind-100m-dark-web-site-jailed-for-5-years-4-months?highlight=WyJiaXRjb2luIiwiYml0Y29pbnMiXQ==> accessed 11 September 2019.
[64] BBC News, 'Criminal's Bitcoin seized in Surrey Police first' (Surry, 21 July 2018) <https://www.bbc.co.uk/news/uk-england-surrey-44896665> accessed 12 September 2019.
[65] BBC News, 'Prolific Sheerness hacker ordered to pay back £922k' (23 August 2019) <https://www.bbc.co.uk/news/uk-england-kent-49450676> accessed 24 September 2019.

established that the criminal law is applicable, it must also be considered whether transactions involving cryptocurrencies are subject to UK reporting requirements.

5.4. Preventative Measures

The UK's money laundering prevention strategy can be split into two main elements; these are SARs and CDD requirements. The relevant law is found within the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017[66] (Money Laundering Regulations 2017), which were enacted to comply with the Fourth Money Laundering Directive;[67] the 2017 regulations replace the Money Laundering Regulations 2007,[68] which were enacted to implement the Third Money Laundering Directive.[69] The Proceeds of Crime Act also contains an offence of failing to reporting suspicious activity when required to.[70] As noted by Ryder,[71] the UK has incorporated preventative measures since the Drug Trafficking Offences Act 1986,[72] and "*was one of the first EU members to incorporate preventive money laundering measures.*"[73] The FATF mutual evaluation in 2018 found that with regard to "*technical compliance, the legal framework is particularly strong*"[74] but that

[66] Money Laundering Regulations 2017.
[67] Directive 2015/849/EU 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 [2015] OJ L.141/73.
[68] The Money Laundering Regulations 2007.
[69] Council Directive 2005/60/EC of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, [2005] OJ L309/15.
[70] Proceeds of Crime Act 2002, Part 2, s.330-332.
[71] N. Ryder *Money Laundering - An Endless Cycle?: A Comparative Analysis of the Anti-Money Laundering Policies in the United States of America, the United Kingdom, Australia and Canada* (Routledge, London, 2012).
[72] Drug Trafficking Offences Act 1986.
[73] cf Ryder (n71) at p91.
[74] FATF, 'Anti-money laundering and counter-terrorist financing measures – United Kingdom, Fourth Round Mutual Evaluation Report' (Paris, December 2018) <fatf-

"*major improvements are needed to strengthen supervision and implementation of preventive measures, and ensure that financial intelligence is fully exploited.*"[75] CDD requirements and the SARs regime will be outlined and applied to cryptocurrencies. Compliance with AML regulation is enforced by the FCA,[76] but SARs are submitted to the National Crime Agency (NCA), as that is the UK financial intelligence unit (FIU).

5.4.1. Customer Due Diligence

The Money Laundering Regulations 2017 set out CDD requirements for regulated firms, to determine whether cryptocurrency transactions may be subject to reporting requirements it will first be necessary to establish what constitutes a regulated institution. Regulation 8 sets out the application of the regulations, Reg.8(2) lists the regulated institutions of which Reg.8(2)(b) "*financial institutions*"[77] may apply cryptocurrency exchanges. The Money Laundering Regulations 2017 definition of a financial institution includes "*an undertaking, including a money service business, when it carries out one or more of the activities listed in points 2 to 12, 14 and 15 of Annex 1 to the capital requirements directive.*"[78] Annex 1 of the Capital Requirements Directive outlines the common functions any financial institution may perform, but in relation to cryptocurrency exchanges points 4, 5, and 15 may be satisfied. Point 4 being "*payment services,*"[79] point 5 being "i*ssuing and administering other means of*

gafi.org/media/fatf/documents/reports/mer4/MER-United-Kingdom-2018.pdf> accessed 11 September 2019 at para 5.

[75] ibid at para 4.

[76] Financial Conduct Authority, 'Money laundering and terrorist financing' (03 August 2015) <https://www.fca.org.uk/firms/financial-crime/money-laundering-terrorist-financing> accessed 17 September 2019.

[77] Money Laundering Regulations 2017, Regulation 8(2)(b).

[78] ibid Regulation 10(2)(a).

[79] Council Directive 2013/36/EU of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC [2013] OJ L176/338, Annex I (4).

payment … insofar as such activity is not covered by point 4,"[80] and point 15 being "*issuing electronic money*."[81] Based on these provisions it is likely that a cryptocurrency exchange may be deemed a financial institution. Additionally, money services businesses are included as a financial institutions in the Regulations, this further strengthens the argument that cryptocurrency exchanges should be subject to AML requirements. The definition of a 'money services business' under Reg.3 of the Money Laundering Regulations[82] is an "*an undertaking which by way of business operates a currency exchange office, transmits money (or any representations of monetary value) by any means or cashes cheques which are made payable to customers.*"[83] The phrase "*or any representations of monetary value*"[84] is a very wide drafting and while Bitcoin has a particularly high value in fiat currency, but most other convertible virtual currencies also have a monetary value in fiat currencies, so may satisfy this definition. Based on this analysis; cryptocurrency service providers could be subject to CDD requirements, though no evidence of enforcement exists. Regulation 4 sets out the limitations, the most relevant of which would be Reg.4(2) which states that the regulations do not apply to those engaging in financial activity "*on an occasional or very limited basis,*"[85] so it would be unlikely to apply to the users of cryptocurrencies, only the operators of exchanges.

The CDD requirements are set out in Part 3 of the Money Laundering Regulations 2017, Regulation 27 identifies when CDD should take place, and Regulation 28

[80] ibid at Annex I (5).
[81] ibid at Annex I (15).
[82] Money Laundering Regulations 2017, Regulation 3.
[83] ibid Regulation 3(1)(d).
[84] ibid Regulation 3(1)(d).
[85] ibid Regulation 4(2).

outlines what information is required. CDD measures must be applied when a business relationship is first established,[86] when an occasional transaction exceeding €1,000 takes place,[87] where money laundering is suspected,[88] or where the "*veracity or adequacy*"[89] of the previously obtained information is doubted.[90] While the 2007 Regulations were less prescriptive, requiring the same information from all types of customers; the 2017 regulations require differing CDD information from different types of customers. The focus of CDD is on identifying the customer, verifying their identity and obtaining information on the "*purpose and intended nature of the business relationship or occasional transaction*."[91] The requirements are altered if the customer is a company; where the identification of the customer requires the name of the company, the company number or relevant registration number, and the address of the company's registered office.[92] Additionally the regulated entity should "*take reasonable measures to determine and verify*"[93] the customer company's constitution and the names of the board of directors.[94] As has been identified, the purpose of the Money Laundering Regulations 2017 is to meet the requirements of the 4th Money Laundering Directive, this can be seen in the focus on the beneficial owner of the money or property being transferred. Regulation 28(4) states that where a customer company is owned is "*beneficially owned by another person*"[95] then the regulated

[86] ibid Regulation 27(1)(a).
[87] ibid Regulation 27(1)(b).
[88] ibid Regulation 27(1)(c).
[89] ibid Regulation 27(1)(d).
[90] ibid.
[91] ibid Regulation 28(2)(c).
[92] ibid Regulation 28(3)(a).
[93] ibid Regulation 28(3)(b).
[94] ibid Regulation 28(3)(b).
[95] ibid Regulation 28(4).

entity must identify that beneficial owner,[96] and further efforts must be made to identify subsequent beneficial owners if the first beneficial owner is a corporation.[97]

CDD has inherent weaknesses, money laundering is concerned with making money appear legitimate, so it follows that launders will provide information which adheres to accepted norms. Chaikin highlights the assumption that customers will be honest and that there are no legal requirements for customers to provide full disclosure of the names they use or the accounts they have opened,[98] there is no reason why a money launderer will give truthful information. It has been identified already in this thesis that cryptocurrencies provide users with mechanisms to conceal their identity,[99] applying CDD requirements to cryptocurrency service providers will be more difficult than for the traditional financial institutions. Irwin and Dawson note that "*cybercriminals are likely to be comfortable obtaining fraudulent documents*"[100] which can defeat CDD, and that the high cost of implementing extensive identification processes is not proportionate to those making small cryptocurrency payments.[101] CDD requirements are also vulnerable to professionals who assist in money laundering. Long prior to the existence of CDD, individuals have offered services to 'clean' money. Rider observes that "[s]*ince the days of Meyer Lansky there have been individuals who are prepared,*

[96] ibid Regulation 28(4)(a).
[97] ibid Regulation 28(4)(c).
[98] D. Chaikin, 'Risk-Based Approaches to Combatting Financial Crime' (2009) 8(2) Journal of Law and Financial Crime 20 at 23.
[99] The anonymity attached to cryptocurrencies is addressed by the US Government Accountability Office in their 2014 report, which described such currencies as pseudonymous, as the although the users name is not known, other details are published on the blockchain; such as their Bitcoin address, the time of the transaction, and the amount: United States Government Accountability Office, 'Virtual Currencies: Emerging Regulatory, Enforcement, and Consumer Protection Challenges' <http://gao.gov/assets/670/663678.pdf> accessed 16 December 2015 at p.6.
[100] A. S. M. Irwin, and C. Dawson, 'Following the cyber money trail: Global challenges when investigating ransomware attacks and how regulation can help' (2019) 22(1) JMLC 110 at 125.
[101] ibid.

for a fee or part of the action, to provide their services to whoever may wish to have their money hidden or laundered."[102] Rider goes on to note that the "*modern money launderer is unlikely to be involved as a member of a criminal organisation*"[103] instead they are likely to be within the financial services industry and "*prepared to make his services available to whoever is willing to pay.*"[104] Such individuals will be likely to pass CDD checks without drawing attention to themselves, undermining the AML measures.

In addition to initial CDD, the Money Laundering Regulations 2017 require a regulated firm to "*conduct ongoing monitoring of a business relationship*."[105] This means scrutinising transactions to ensure consistency with the customer's usual behaviour,[106] and ensuring CDD records are kept up-to-date.[107]

CDD is to be conducted within the risk-based approach. Regulation 28(12) makes clear that the "*ways in which a relevant person complies with the requirement to take CDD measures, and the extent of the measures taken*"[108] must reflect the "*risk assessment carried out by the relevant person*"[109] and an "*assessment of the level of risk arising in any particular case*."[110] It is recognised that the measures "*may differ*

[102] B. Rider, 'The practical and legal aspects of interdicting the flow of dirty money' (1996) 3(3) JFC 234 at 241.
[103] ibid.
[104] ibid.
[105] Money Laundering Regulations 2017, Regulation 28(11).
[106] ibid Regulation 28(11)(a).
[107] ibid Regulation 28(11)(b).
[108] ibid Regulation 28(12)
[109] ibid Regulation 28(12)(a)(i).
[110] ibid Regulation 28(12)(a)(ii).

from case to case."[111] The higher the money laundering risk attached to the type of business being undertaken, the greater the due diligence should be. This policy is clear from Regulation 33 of the Money Laundering Regulations,[112] which requires "*enhanced customer due diligence measures and enhanced ongoing monitoring*"[113] to reduce the risk is particular situations. This includes any transaction involving a high-risk jurisdiction,[114] involving politically exposed people,[115] and transactions which are complex and unusually large.[116] In the 2007 regulations, transactions requiring enhanced CDD included situations "[w]*here the customer has not been physically present for identification purposes, a relevant person must take specific and adequate measures to compensate for the higher risk.*"[117] The nature of cryptocurrency means that the user may rarely physically meet the regulated entity, therefore a regulated cryptocurrency exchange would be required to apply enhance CDD under the 2007 regulations. Unfortunately, the 2017 regulations are less clear, the "*physically present*"[118] has been removed and instead the enhanced measures should be applied in "*correspondent relationships with a credit institution or a financial institution;*"[119] but the definition of a correspondent relationship is poorly defined in Regulation 34;

> "correspondent relationship" means—
>
> (i) the provision of banking services by a correspondent to a respondent including providing a current or other liability account and related services, such as cash management, international funds transfers,

[111] ibid Regulation 28(12)(b).
[112] ibid Regulation 33.
[113] ibid Regulation 33(1).
[114] ibid Regulation 33(1)(b).
[115] ibid Regulation 33(1)(d).
[116] ibid Regulation 33(1)(f).
[117] Money Laundering Regulations 2007. Regulation 14(2).
[118] ibid.
[119] Money Laundering Regulations 2017. Regulation 33(1)(c).

cheque clearing, providing customers of the respondent with direct access to accounts with the correspondent (and vice versa) and providing foreign exchange services; or

(ii) the relationship between and among credit institutions and financial institutions including where similar services are provided by a correspondent to a respondent, and including relationships established for securities transactions or funds transfers."[120]

The term correspondent is not defined which is confusing, but a basic understanding of the definition could mean that the term 'correspondent relationship' replaces the 2007 provision in relation to the customer not being physically present and thus cryptocurrency transactions would be likely to require enhanced due diligence. Regulation 33(5) outlines the enhanced due diligence measures, which include seeking independent verification of the customers identity,[121] taking further steps to understand the "*background, ownership and financial situation of the customer*",[122] and placing greater scrutiny on transactions.[123]

The Money Laundering Regulation 2017 also provides a "*simplified due diligence*"[124] process under Regulation 37; the effect of this is to remove requirements where there is no suspicion of money laundering or terrorist financing, taking into account the risk factors identified in Regulation 37(3) and with regard for the risk assessment which all

[120] ibid Regulation 34(4)(a).
[121] ibid Regulation 33(5)(a).
[122] ibid Regulation 33(5)(b).
[123] ibid Regulation 33(5)(d).
[124] ibid Regulation 37.

regulated entities must carry out. The circumstances where Regulation 37 may apply are limited and none are likely to apply to cryptocurrencies. CDD information should identify the customer and build up intelligence pertaining to their behaviour, this information should be used by regulated institutions to help decide when a specific transaction is suspicious, and whether a SAR needs to be submitted to the NCA.

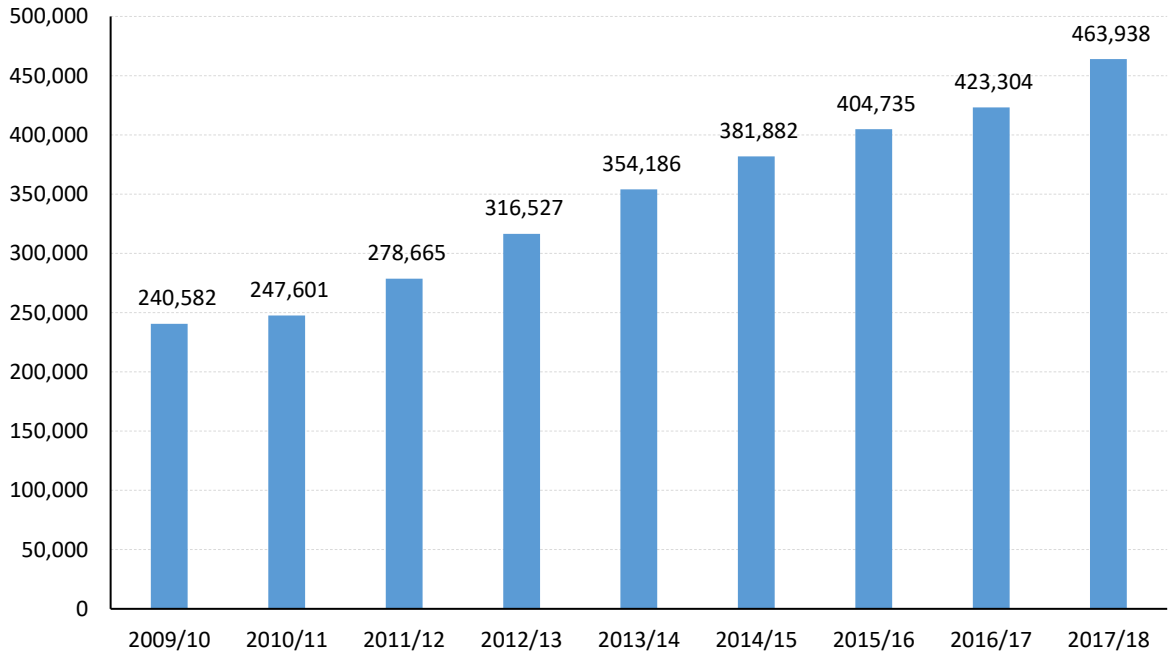
5.4.2. Money Laundering Reporting Requirements

The second element of the UK's preventative approach is reporting requirements, specifically through SARs. As with the US and Australian systems, a SAR is sent to the FIU when a transaction, or series of transactions, raises suspicions of money laundering or terrorist financing. It is a legal obligation in the UK for those in the regulated sector to report suspicious transactions. The legal obligation can be found in ss.330-332 of POCA 2002,[125] s.330 sets out the criteria of the offence for a person in the regulated sector. A person commits an offence if they know or suspect,[126] or have reasonable grounds to know or suspect,[127] that a person is engaged in money laundering based on information that came from their course of business,[128] and they fail to "*make the required disclosure as soon as is practicable after the information or other matter comes to*"[129] them.

[125] Proceeds of Crime Act 2002, ss.330-332.
[126] ibid s.330(1)(a).
[127] ibid s.330(1)(b).
[128] ibid s.330(2).
[129] ibid s.330(3).

Section 331 concerns a nominated officer, they will commit an offence if the same conditions as s.330 are met, the only difference being that "*such knowledge or suspicion, came to him in consequence of a disclosure made under section 330.*"[130] As a nominated officer, they will receive disclosures via s.330 and be required to submit a report to the NCA.[131]

Figure 6. Suspicious Activity Report Volume[132]



SARs are submitted to the UK FIU, which is the NCA, Figure 6 shows the steady rise in the number of SARs submitted annually since 2010, the trend suggests that by 2020

[130] ibid s.331(3)(b).
[131] Money Laundering Regulations 2017, Article 3(1).
[132] Compiled using annual totals published in: Serious Organised Crime Agency, 'Suspicious Activity Reports Regime: Annual Report 2010' (London, 26 November 2010) <https://www.octf.gov.uk/OCTF/media/OCTF/images/publications/SARS%20Annual%20Report/SARs-Annual-Report-2010.pdf?ext=.pdf> accessed 15 September 2019, White & Chase, 'New UK AML Action Plan – The Increased Role of the Private Sector' (London, April 2016) <https://www.whitecase.com/sites/whitecase/files/files/download/publications/new-uk-aml-action-plan-the-increased-role-of-the-private-sector.pdf> accessed 15 September 2019, National Crime Agency,

the annual volume will be double that of 2010. The rising number of SARs being submitted to the NCA could cause difficulties as the FATF identified the "*UKFIU suffers from a lack of available resources*",[133] in terms of both personnel, technology, and "*analytical capability*".[134] The FATF was especially concerned as "*similar issues were raised over a decade ago in the UK's previous FATF mutual evaluation.*"[135] In its 2018 report on the SARs regime, the Law Commission linked the high numbers of SARs to three connected causes, a low threshold for reporting based on suspicion,[136] defensive reporting due to criminal liability for failing to report,[137] and the concept of suspicion remaining poorly defined.[138] The efficacy of the SARs regime could be impacted if the FIU is unable to process reports, this would be exacerbated if AML regulation is applied to cryptocurrencies, as it would increase the volume of reports further.

'Suspicious Activity Reports (SARs) Annual Report 2014' (London, 24 March 2015) <http://www.octf.gov.uk/OCTF/media/OCTF/images/publications/SARS-Annual-Report-2014.pdf?ext=.pdf> accessed 15 September 2019, National Crime Agency, 'Suspicious Activity Reports (SARs) Annual Report 2015' (London, 18 May 2017) <https://nationalcrimeagency.gov.uk/who-we-are/publications/2-sars-annual-report-2015/file> accessed 15 September 2019, National Crime Agency, 'National Crime Agency Annual Report and Accounts 2015–16' (London, 21 July 2016) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/583545/NCA_Annual_Report_and_Accounts_2015-16__web_.pdf> accessed 15 September 2019, National Crime Agency, 'National Crime Agency Annual Report and Accounts 2016–17' (London, 20 July 2017) <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/25-nca-annual-report-2016-17/file> accessed 15 September 2019, National Crime Agency, 'National Crime Agency Annual Report and Accounts 2017–18' (London, 19 July 2018) <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/177-nca-annual-report-accounts-2017-18/file> accessed 15 September 2019, and National Crime Agency, 'Suspicious Activity Reports (SARs) Annual Report 2018' (London, 15 March 2019) <https://nationalcrimeagency.gov.uk/who-we-are/publications/256-2018-sars-annual-report/file> accessed 15 September 2019.

[133] FATF, 'Anti-money laundering and counter-terrorist financing measures – United Kingdom, Fourth Round Mutual Evaluation Report' (Paris, December 2018) <fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-Kingdom-2018.pdf> accessed 11 September 2019 at para 6.

[134] ibid.

[135] ibid.

[136] Law Commission, *Anti-money laundering: the SARs regime* (Law Com No 384, 2018) para 5.11.

[137] ibid at para 5.12.

[138] ibid at para 5.13.

The SARs regime in the UK has been criticised by the Court of Appeal, as well as by Ryder who points out the increases in defensive reporting,[139] which is also identified by Leong.[140] The Law Commission noted that as the "*criminal liability rests with the reporter*"[141] a "*culture of defensive reporting*"[142] has developed. Defensive reporting is used to explain the sharp rise in SARs since it became an offence not to submit.[143] This goes against the purpose of the reporting, if the aim is to highlight genuinely suspicious transactions then these suspicious transactions will be much harder to identify in the sea of reports filled to prevent prosecution. Additional criticism could be levied at the use of the word suspicious which is subjective and guidance from the courts has not been helpful. The Law Commission found the term suspicious was "*ill-defined, unclear and inconsistently applied*"[144] by those submitting reports. The term has been long been problematic in English law, Lord Devlin stated in *Hussien* v *Chong Fook Kam*[145] that the ordinary meaning of suspicion "*is a state of conjecture or surmise where proof is lacking*"[146] which is not definitive enough to be helpful in determining whether a SAR should be submitted. Lord Devlin's definition was provided before it was a criminal offence not to report, introduced by a 1993 amendment to the Drug Trafficking Offences Act 1986.[147] Criminal liability for failing to report creates further needs for a clear threshold for suspicion, which has not been provided. In *R v Da*

[139] cf Ryder (n71) at p93.
[140] A. Leong, 'Chasing dirty money: domestic and international measures against money laundering' (2007) 10(2) Journal of Money Laundering Control 140.
[141] Law Commission, *Anti-money laundering: the SARs regime* (Law Com No 384, 2018) para 5.12.
[142] ibid.
[143] A. Leong, 'Chasing dirty money: domestic and international measures against money laundering' (2007) 10(2) Journal of Money Laundering Control 140.
[144] Law Commission, *Anti-money laundering: the SARs regime* (Law Com No 384, 2018) para 5.13.
[145] *Shaaban bin Hussien* v *Chong Fook Kam* [1970] 2 WLR 441.
[146] ibid per Lord Devlin at 445.
[147] Drug Trafficking Offences Act 1986, s.26B. The offence is now found at s.330 of the Proceeds of Crime Act 2002.

Silva,[148] Longmore LJ held that "*it seems to us that the essential element of the word suspect and its affiliates, in this context, is that the defendant must think that there is a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice*".[149] *Da Silva* has been upheld, most notably by *K Ltd* v *National Westminster Bank plc*[150] and *Shah* v *HSBC Private Bank (UK) Ltd*[151] leaving the term 'suspicious' inadequately defined. The Joint Money Laundering Steering Group note that in addition to the subjective test from *Da Silva*, an objective text is clear from the wording of the offences.[152] Criminal liability arises for "*failing to disclose information when reasonable grounds exist for knowing or suspecting that a person is engaged in money laundering/terrorist financing*."[153] Examples of reasonable grounds include factors pertaining to the origin of the transaction, how the relevant funds were discovered, the monetary values involved, the destination of the money, and whether any apparent links to crime exist.[154] The objective text provides limited assistance, as the word reasonable also has differing meanings based on the context it is being considered. The Law Commission found that the low threshold for suspicion was contributing to the large volume of reports being submitted.[155] With regards to cryptocurrency service providers, if they are deemed to be money services businesses, and subject to reporting requirements, then it could be of increased difficulty for them to establish what is, and is not, suspicious. This is because they may have limited information with which to determine what is normal for their customer if

[148] *R v Da Silva* [2007] 1 WLR 303.
[149] ibid at 308.
[150] K Ltd v National Westminster Bank plc (Revenue and Customs Commissioners and another intervening) [2006] EWCA Civ 1039
[151] *Shah* v *HSBC Private Bank (UK) Ltd [2012] EWHC 1283*
[152] Joint Money Laundering Steering Group, 'Prevention of money laundering/combating terrorist financing: Part I, 2017 REVISED VERSION' (13 December 2017) <http://www.jmlsg.org.uk/download/10005> accessed 21 October 2019 at 6.15.
[153] ibid.
[154] ibid.
[155] Law Commission, *Anti-money laundering: the SARs regime* (Law Com No 384, 2018) para 5.11.

their customer regularly transacts privately within cryptocurrency networks. Cryptocurrency service providers would be required to submit SARs based on less detailed information that traditional financial institutions and so may report to protect themselves from liability, thus adding to the issue of defensive reporting.

5.5. Applicability of Preventative Measures to Cryptocurrencies

At present the FCA does not regulate cryptocurrencies in any capacity, the FCA's approach to cryptocurrencies will be analysed below at 5.7. Despite the lack of regulation, it is relatively straightforward to apply AML measures to cryptocurrency service providers, but there are potential practical issues in doing this. While regulation should be widened to cryptocurrency service providers, as recommended by the FATF,[156] this will still leave gaps in the regulation of cryptocurrencies, as peer-to-peer transactions will continue to go unregulated. It is not possible to apply the SARs regime to peer-to-peer transactions in the same way it can be for traditional financial transactions, as there is no human interaction at a point where the transaction can be held prior to a review, by an FIU. The SARs regime will need to be modified in order to apply to cryptocurrency transactions, while transactions cannot be frozen, the wealth of information the blockchain provides means that FIUs can monitor the blockchain themselves, and could identify money laundering behaviour. The pseudonymity provided by cryptocurrencies means that all the FIU would be able to obtain is public keys rather than names, but, as demonstrated by Reynolds and Irwin,

[156] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2019 para 86 at p23.

this can be negated by "*analysis of transaction history tracing back to an interaction with a Bitcoin exchange in which* [the money launderer was] *required to submit forms of identifying information.*"[157] Despite this potential, it is unlikely that the NCA is going to be capable of this, as it requires resources the FATF has identified as lacking in availability to the NCA, namely; human resources, IT resources, and analytical capability.[158]

5.6. Authorities

In this section, the primary and secondary authorities of the UK AML approach will be identified, and their responsibilities will be detailed, after this their roles can be assessed in relation to cryptocurrencies. As identified by Ryder, primary authorities are responsible for creating AML policy and legislation, while secondary authorities are tasked with enforcement.[159] The primary authorities of the UK are government departments, and the principal secondary authorities in the UK are the NCA, as the FIU this is the authority that reports are submitted to, and the principle regulator of financial institutions, the FCA. The secondary authorities are not part of the government, the NCA is an "*independent non-ministerial government department*",[160] and the FCA is an "*independent public body funded entirely by the firms*"[161] it

[157] P. Reynolds and A.S.M. Irwin, 'Tracking digital footprints: anonymity within the bitcoin system' (2017) 20(2) JMLC 172 at 187.
[158] FATF, 'Anti-money laundering and counter-terrorist financing measures – United Kingdom, Fourth Round Mutual Evaluation Report' (Paris, December 2018) <fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-Kingdom-2018.pdf> accessed 11 September 2019 at para 10.
[159] cf Ryder (n71) at p.25.
[160] National Crime Agency, 'Governance and transparency' <https://www.nationalcrimeagency.gov.uk/who-we-are/governance-and-transparency> accessed 17 September 2019.
[161] Financial Conduct Authority, 'About the FCA' (24 April 2016) <https://www.fca.org.uk/about/the-fca> accessed 17 September 2019.

regulates. A third category is also recognised by Ryder;[162] tertiary agencies, which may include "*trade associations and professions which are threatened by illegal transactions*."[163] The UK has one identifiable cryptocurrency trade association in the form of CryptoUK.[164]

5.6.1. Primary

HM Treasury

HM Treasury is the principle policy-making authority for UK AML legislation and regulation.[165] It represents the UK at the FATF[166] and is "*responsible for the implementation of the Money Laundering Directives and the execution of the UN's financial sanctions regime.*"[167] In this capacity HM Treasury has an instrumental role in ensuring the UK financial sector complies with its international obligations, and in formulating and enacting AML policy. [168] HM Treasury will regularly assess the money laundering threats to the UK, it undertook its first national risk assessment in 2015.[169] The risk assessment found that the UK AML regulators were most knowledgeable "*about cash-based money laundering, particularly cash collection networks, international controllers, and money service businesses, although some gaps in*

[162] cf Ryder (n71) at p.25.
[163] ibid.
[164] CryptoUK, 'About Us' <https://cryptouk.io/about/> accessed 23 October 2019.
[165] cf Ryder (n71) at p79.
[166] Financial Action Task Force, 'Mutual evaluation of United Kingdom of Great Britain and Northern Ireland' <http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20UK%20FULL.pdf> accessed 02 March 2016 at p.24
[167] cf Ryder (n71) at p79.
[168] Financial Action Task Force, 'Mutual evaluation of United Kingdom of Great Britain and Northern Ireland' <http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20UK%20FULL.pdf> accessed 02 March 2016 at p.24.
[169] HM Treasury, 'UK national risk assessment of money laundering and terrorist financing' (October 2015) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf> accessed 28 October 2019.

knowledge remain."[170] This was attributed to "*the resources that law enforcement agencies have invested over a number of years in tackling cash-based money laundering and the drugs trade (which largely generates proceeds in the form of cash)*."[171] The risk assessment is an indicator that the UK AML approach needs to develop its approach to non-cash based money laundering, which would include cryptocurrencies.

Home Office

While HM Treasury is responsible for the financial sector, the Home Office has responsibility for "*all UK primary legislation concerning money laundering and terrorist financing; overall police strategy and targets for money laundering and terrorist financing investigations and prosecutions*"[172] As outlined in this chapter, the UK AML legislation can be found within Part 7 of POCA 2002,[173] the Terrorism Act 2000,[174] and the Money Laundering Regulation 2017.[175]

Foreign and Commonwealth Office

The Foreign and Commonwealth Office has a very limited role in UK AML policy, it is only concerned with "*implementation international Treaties and Conventions*",[176] and

[170] ibid at p.4.
[171] ibid.
[172] Financial Action Task Force, 'Mutual evaluation of United Kingdom of Great Britain and Northern Ireland' <http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20UK%20FULL.pdf> accessed 02 March 2016 at p.24
[173] Proceeds of Crime Act 2002, Part 7.
[174] Terrorism Act 2000.
[175] Money Laundering Regulations 2017.
[176] cf Ryder (n71) at p79.

therefore it will not be considered in detail in relation to cryptocurrencies, as to date there are no applicable international treaties.

5.6.2. Secondary

Financial Conduct Authority (FCA)

The FCA was established in 2012, it replaced the beleaguered Financial Services Authority, which was heavily criticised in the wake of the 2007-08 financial crisis.[177] The FCA's 'Integrity Objective' is found at s.1D of the Financial Services and Markets Act 2000 and requires the FCA to protect and enhance the integrity of the UK financial system.[178] This includes reducing the extent to which the financial services industry can be used for purposes connected with financial crime.[179] Money laundering is pursued using a 'risk-based' approach; greater AML requirements are placed on those firms and individuals who are most susceptible to money laundering. The FCA's AML rules are contained in the Senior Management Arrangements, Systems and Controls (known as SYSC), specifically SYSC 6.3. Srivastava notes that the risk-based approach in SYSC "*is intended to provide more flexibility to firms,*"[180] and Ryder observes that this flexibility "*allows them to identify the risks and determine how they can best allocate their resources in areas which are most vulnerable.*"[181]

[177] The FSA was notably criticised in the 'Run on the Rock' report see: Treasury Select Committee, The Run on the Rock, HC56-II 2007-08.
[178] Financial Services and Markets Act 2000, s.1D(1)
[179] Financial Services and Markets Act 2000, s.1D(2)(b) and A. Srivastava, 'UK Part II: UK Law and Practice' in A. Srivastava, M. Simpson and N. Moffatt (eds) *International Guide to Money Laundering and Practice* (Haywards Heath, Bloomsbury, 2013) at 2.188.
[180] A. Srivastava, 'UK Part II: UK Law and Practice' in A. Srivastava, M. Simpson and N. Moffatt (eds) *International Guide to Money Laundering and Practice* (Haywards Heath, Bloomsbury, 2013) at 2.189.
[181] cf Ryder (n71) at p.81.

The FCA has enforcement powers, these are intended to support its objectives "*by making it clear there are real and meaningful consequences for firms and individuals who don't follow the rules.*"[182] Since its creation in 2013, the FCA has imposed 193 fines,[183] amounting to £3,513,743,864, therefore the average fine imposed is £18,205,927. These figures are distorted by the extraordinary fines imposed on large banks for highly publicised failings in recent years, such as the LIBOR and FOREX market manipulation scandals, and the record braking fines of £102million for Standard Chartered[184] and £163million for Deutsche Bank[185] for their AML failings. The FCA does not publish statistics for AML compliance enforcement actions, but in 2019 the 2018/19 Anti-Money Laundering Annual Report it was stated that since 2012, 18 AML enforcement cases had been concluded by the FCA and its predecessor the Financial Services Authority.[186] It is clear that while the FCA will take enforcement action against non-compliant institutions, its supervision is spread across other conduct related areas of financial regulation.

[182] Financial Conduct Authority, 'Enforcement' (22 April 2016) <https://www.fca.org.uk/about/enforcement> accessed 18 September 2019.
[183] Based on published enforcement notices: Financial Conduct Authority, 'Enforcement' (22 April 2016) <https://www.fca.org.uk/about/enforcement> accessed 18 September 2019.
[184] Financial Conduct Authority, 'FCA fines Standard Chartered Bank £102.2 million for poor AML controls' 09 April 2019) <https://www.fca.org.uk/news/press-releases/fca-fines-standard-chartered-bank-102-2-million-poor-aml-controls> accessed 18 September 2019.
[185] Financial Conduct Authority, 'FCA fines Deutsche Bank £163 million for serious anti-money laundering controls failings' (31 January 2017) <https://www.fca.org.uk/news/press-releases/fca-fines-deutsche-bank-163-million-anti-money-laundering-controls-failure> accessed 18 September 2019.
[186] Financial Conduct Authority, 'Anti-money laundering Annual report 2018/19' (09 July 2019) <https://www.fca.org.uk/publication/corporate/annual-report-2018-19-anti-money-laundering.pdf> accessed 18 September 2018 at p12.

National Crime Agency

Created in 2011, the NCA is a national authority tasked with combatting crime across the spectrum, as a result is has a "*wide remit*"[187] to "*tackle serious and organised crime, strengthen* […] *borders, fight fraud and cyber crime, and protect children and young people from sexual abuse and exploitation.*"[188] The NCA is the FIU of the UK. The NCA is a "*Law Enforcement Model*"[189] FIU when considered against the Egmont Group typology. This is because the NCA "*implements anti-money laundering measures alongside already existing law enforcement systems, supporting the efforts of multiple law enforcement or judicial authorities with concurrent or sometimes competing jurisdictional authority to investigate money laundering*."[190] As the UKFIU, all SARs are sent to the NCA; it *receives more than 380,000 SARs a year*.[191] Upon receiving SARs, the NCA "*identifies the most sensitive SARs and sends them to the appropriate organisations for investigation*.[192]

The NCA aims to "*provide leadership in these areas through* [it's] *organised crime, border policing, economic crime and CEOP commands, the National Cyber Crime Unit and specialist capability teams.*"[193] Money laundering is the responsibility of the 'Economic Crime Command', and the Home Office is expected to "*ensure a coherent*

[187] National Crime Agency, 'What We Do' <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do> accessed 02 March 2016.
[188] ibid.
[189] Egmont Group, 'Financial Intelligence Units (FIUs)' <http://www.egmontgroup.org/about/financial-intelligence-units-fius> accessed 11 March 2016.
[190] ibid.
[191] National Crime Agency, 'UK Financial Intelligence Unit' <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/ukfiu> accessed 04 March 2016.
[192] ibid.
[193] National Crime Agency, 'What We Do' <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do> accessed 02 March 2016.

approach to the use of resources focussed on economic crime across the full range of agencies deploying them."[194] The Economic Crime Command strategy is based on 4 principles knows as the "*'4P' components of the Serious & Organised Crime Strategy.*"[195] The '4Ps' are 'Prevent', 'Pursue', 'Protect', and 'Prepare'. The Economic Crime Command claims to tackle money laundering in three main ways, by "[l]*eading multi-agency action*" against national and international money laundering,[196] targeting criminals within professions vulnerable to money laundering, such as lawyers, accountants and bankers,[197] and increasing operational capabilities.[198]

In December 2014, the NCA placed emphasis on 'High End Money Laundering', which the NCA defines as *the laundering of funds, wittingly or unwittingly, through the UK financial sector and related professional services.*"[199] This definition could be criticised as the financial sector is a wide definition, and relatively small amounts of money may be laundered through it. The NCA does provide a more helpful distinction as well, describing 'high end money laundering as including;

> "[m]ajor *frauds and overseas corruption work, where the raw material of the crime is electronic and cash is only used further down the laundering*

[194] GOV.UK, 'The National Crime Agency A plan for the creation of a national crime-fighting capability' https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97826/nca-creation-plan.pdf> accessed 02 March 2016 at p.20.
[195] National Crime Agency, 'Economic Crime Command' <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime> accessed 02 March 2019.
[196] National Crime Agency, 'Economic Crime Command' <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime> accessed 02 March 2016.
[197] ibid.
[198] ibid.
[199] National Crime Agency, 'High End Money Laundering: Strategy and Action Plan' <http://www.nationalcrimeagency.gov.uk/publications/625-high-end-money-laundering-strategy/file> accessed 02 March 2016 at para 3.

process to disguise audit trails or extract profits. In this respect, it can be distinguished from the laundering of street cash generated by the activities of organised criminal groups (OCGs)."[200]

This distinction is notable as the key difference between 'High End Money Laundering' and more traditional money laundering is that the placement stage may be easier for the money launderer to achieve as the funds are already in an electronic format.

It can be seen from the approach of the NCA, via the Economic Crime Command, that there is a strong emphasis on inter-agency co-operation. "*The NCA works closely with partners to deliver operational results,*"[201] an example of this could be the Joint Money Laundering Intelligence Taskforce which has supported over 500 investigations, assisting in approximately 130 arrests and confiscating £13m.[202] While the NCA is a national body it is clearly also an international one, it states that it has "*an international role to cut serious and organised crime impacting on the UK through our network of international liaison officers.*"[203]

[200] ibid at para 4.
[201] National Crime Agency, 'What We Do' <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do> accessed 02 March 2016.
[202] National Crime Agency, 'National Economic Crime Centre' <https://www.nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-centre> accessed 19 September 2019.
[203] National Crime Agency, 'What We Do' <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do> accessed 02 March 2016.

Similarly to the FCA, the NCA is not solely focused on money laundering, it is responsible for tackling all serious and organised crime in the UK.[204] Examples of recent convictions obtained by the NCA include a 4 years and 6 months jail term and an order to repay £7.3m of laundered money,[205] eight members of a crime group who laundered £1.8m in connection with drug offences received sentences ranging from 7 years to 18 months,[206] and a total of 11 years in prison sentences imposed on 3 men for their role in a £1million drug business and money laundering scheme.[207] It is difficult to analyse the sentences for money laundering in isolation as convictions are for multiple offences rather than money laundering alone.

Crown Prosecution Service

The CPS was established in 1985 through the Prosecution of Offences Act[208] and is the "*principal prosecuting authority for England and Wales, acting independently in criminal cases investigated by the police and others.*"[209] The CPS decides whether to prosecute an individual, and the appropriate charges to bring, it prepares cases and instructs counsel to present the case at court, and also provides support to victims and

[204] National Crime Agency, 'Our Mission' <https://www.nationalcrimeagency.gov.uk/who-we-are/our-mission> accessed 19 September 2019.
[205] National Crime Agency, 'Ex-Goldman Sachs investment banker ordered to pay back £7.3 million' (06 September 2019) <https://www.nationalcrimeagency.gov.uk/news/ex-goldman-sachs-investment-banker-ordered-to-pay-back-7-3-million> accessed 19 September 2019.
[206] National Crime Agency, 'Seventy years for multi-million pound drugs and money laundering group' (26 July 2019) <https://www.nationalcrimeagency.gov.uk/news/seventy-years-for-multi-million-pound-drugs-and-money-laundering-group> accessed 19 September 2019.
[207] National Crime Agency , 'RAF sergeant and pensioner jailed for involvement in £1m drug dealing ring' <https://www.nationalcrimeagency.gov.uk/news/raf-sergeant-and-pensioner-jailed-for-involvement-in-1m-drug-dealing-ring?highlight=WyJtb25leSIsImxhdW5kZXJpbmciLCJsYXVuZGVyIiwibGF1bmRlcmVkIiwibGF1bmRlcmVycyIsImxhdW5kZXJlciIsImxhdW5kZXJlcidzIiwibGF1bmRlcnMiLCJtb25leSBsYXVuZGVyaW5nIl0= > accessed 19 September 2019.
[208] Prosecution of Offences Act 1985, Part 1.
[209] Crown Prosecution Service, 'What We Do' <http://www.cps.gov.uk/about/> accessed 02 March 2016.

witnesses.[210] In this capacity, the CPS may prosecute money laundering offences under Part 7 of the Proceeds of Crime Act 2002.[211] The CPS will bring the majority of individual money laundering cases, where the resources of the larger agencies are not required.

Her Majesty's Revenue and Customs

HMRC is a 'supervisory authority' under the Money Laundering Regulations 2017. Simpson and Moffatt state that this means HMRC have "*an obligation to 'monitor firms that they supervise and if necessary, to make measures for the purpose of securing compliance*"[212] HMRC is responsible for a wide range of supervision, largely where the supervision of the FCA does not extend; it is responsible for high value dealers,[213] and money services businesses or payment services not supervised by the FCA.[214] HMRC have not been allocated any responsibilities regarding the supervision of cryptocurrencies.

5.6.3. Tertiary

CryptoUK

CryptoUK describe themselves as the "*UK's self-regulatory trade association*"[215] of the cryptocurrency sector. CryptoUK have created a code of conduct which is members

[210] ibid.
[211] Proceeds of Crime Act 2002, Part 7.
[212] Financial Services and Markets Act 2000, s.1D(2)(b) and A. Srivastava, 'UK Part II: UK Law and Practice' in A. Srivastava, M. Simpson and N. Moffatt (eds) *International Guide to Money Laundering and Practice* (Haywards Heath, Bloomsbury, 2013) at 2.182.
[213] Money Laundering Regulations 2017, Reg 7(1)(c)(i).
[214] ibid Reg 7(1)(c)(ii)-(v).
[215] CryptoUK, 'About Us' <https://cryptouk.io/about/> accessed 23 October 2019.

should follow,[216] but the code is not legally binding. One of the principles of CryptoUK's code is self-regulation, which has been superseded by the FCA taking on the AML regulation of cryptocurrency service providers.[217] The importance of CryptoUK is difficult to measure as it is still in its infancy, it boasts over 30 members[218] including some prominent market participants such as eToro[219] and Coinbase.[220] A weakness of CryptoUK is that is appears to have limited influence, it has been invited to discussions with the FCA which is positive,[221] but it does not appear to be in discussions with government, as demonstrated by its open letter to the Chancellor in July 2019.[222] A tertiary authority such as CryptoUK could be well-placed to advise regulators on a tailored approach to cryptocurrencies, as their members include participants in the cryptocurrencies industry. The NCA and the FCA should implement the regulation as national authorities, but as part of the joint up approach recommend by Irwin and Turner,[223] "*information sharing between multiple stakeholders from the law enforcement, financial intelligence units, cyber security organisations and fintech industry*"[224] is required. CryptoUK could be a valuable link to the cryptocurrency industry.

[216] CryptoUK, 'Code of Conduct' <https://cryptouk.io/codeofconduct/> accessed 23 October 2019.
[217] HM Government 'Economic Crime Plan' (12 July 2019) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/816215/2019-22_Economic_Crime_Plan.pdf> accessed 23 October 2019 at 4.9.
[218] CryptoUK, 'CryptoUK Members' <https://cryptouk.io/members/> accessed 23 October 2019.
[219] eToro, 'eToro' <https://www.etoro.com/> accessed 23 October 2019.
[220] Coinbase, 'Coinbase' <https://www.coinbase.com/> accessed 23 October 2019.
[221] CryptoUK, 'CryptoUK hosts 5MLD roundtable at the FCA' (24 July 2019) https://cryptouk.io/2019/07/24/cryptouk-hosts-5mld-roundtable-at-the-fca/> accessed 23 October 2019.
[222] CryptoUK, 'Open Letter to Chancellor Sajid Javid from CryptoUK' (25 July 2019) <https://cryptouk.io/2019/07/25/open-letter-to-chancellor-sajid-javid-from-cryptouk/> accessed 23 October 2019.
[223] A. S. M. Irwin and A. B. Tuner, 'Illicit Bitcoin transactions: challenges in getting to the who, what, when and where' (2018) 21(3) JMLC 297 at 310.
[224] ibid.

Having outlined the relevant authorities with AML responsibilities, the next section assesses the reaction of the UK authorities to the money laundering threat posed by cryptocurrencies.

5.7. AML Regulation of Cryptocurrencies

5.7.1. HM Treasury

The UK Treasury began addressing cryptocurrencies with a call for information[225] to gather views on digital currencies and subsequent published responses in March 2015.[226] HM Treasury found that while "[a]*lmost all respondents to the call for information commented that digital currencies can offer a degree of anonymity to users,*"[227] which might be appealing for money laundering, there were differences of opinion in relation to the extent of the anonymity afforded to users. On the issue of the level of anonymity, some traditional financial institutions characterised cryptocurrencies as "*anonymous and untraceable,*"[228] but the submission from user and cryptocurrency service providers argued for the term "'*pseudonymous' rather than anonymous*."[229] Using the term 'pseudonymous' is consistent with FATF guidance when assessing the anonymity offered by cryptocurrencies;[230] this term is favoured due to the publicly available ledger of transactions created by cryptocurrencies, such

[225] GOV.UK, 'Digital currencies: call for information' <https://www.gov.uk/government/consultations/digital-currencies-call-for-information/digital-currencies-call-for-information> accessed 11 March 2019.
[226] GOV.UK, 'Digital currencies: response to the call for information' <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf> accessed 11 March 2019.
[227] ibid at p.11.
[228] ibid.
[229] ibid.
[230] Financial Action Task Force, 'Guidance for a Risk-Based Approach – Virtual Currencies' <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf> accessed 19 September 2019 at p23 para 98.

as Bitcoin, which documents every transaction. The ledger, known as the blockchain;[231] will include information such as the users' public Bitcoin addresses, the time of the transaction, and the amount. The view that cryptocurrency transactions are traceable is supported by the research of Meiklejohn *et al*,[232] who "*were able to identify 1.9 million public keys with some real-world service or identity, although in many cases the identity was not a real name, but rather (for example) a username on a forum*"[233] and Juhász *et al* who were able to identify users' IP addresses from Bitcoin transactions.[234]

HM Treasury reported respondents concerns that "*a number of potential criminal activities that could take place involving digital currencies*."[235] The Silk Road case[236] was given as an example "*where digital currencies have been in evidence as a payment vehicle, such as the buying and selling of illicit goods and services via online marketplaces*"[237] While there have been high profile cases such as that of Silk Road and Liberty Reserve,[238] and "*there were a number of other illicit activities mentioned where respondents considered there to be potential for digital currencies to be*

[231] The public ledger of Bitcoin. See chapter three for explanation of what the blockchain at 3.3.
[232] Sarah Meiklejohn, et al, "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names," (2013) 38(6) ;Login: 10.
[233] ibid at p.14.
[234] P. L. Juhász, J. Stéger, D. Kondor and G. Vattay, 'A Bayesian approach to identify Bitcoin users' (2018) 13(12) PLoS ONE 1.
[235] GOV.UK, 'Digital currencies: response to the call for information' <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf> accessed 11 March 2016 at p.11.
[236] FBI, 'Ross Ulbricht, aka Dread Pirate Roberts, Sentenced in Manhattan Federal Court to Life in Prison' <https://www.fbi.gov/newyork/press-releases/2015/ross-ulbricht-aka-dread-pirate-roberts-sentenced-in-manhattan-federal-court-to-life-in-prison> accessed 11 March 2016.
[237] GOV.UK, 'Digital currencies: response to the call for information' <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf> accessed 11 March 2016 at p.11.
[238] Thompson Reuters, 'Liberty Reserve founder must face $6 bln laundering case in U.S.' <http://www.reuters.com/article/usa-cybersecurity-liberty-reserve-idUSL1N11T2G420150923> accessed 11 March 2016.

used,"[239] the respondents to the consultation paper could not provide any evidence of such use, or the extent to which such use could be taking place.[240] Furthermore, "[s]*ubmissions mentioned money laundering, terrorist financing, tax evasion and sanctions evasion as possible or likely activities facilitated by the distinctive features of digital currencies.*"[241]

Despite the reported appeal for money launderers, the consultation paper also identifies a number of disadvantages; such as price volatility and "*the need for some technical familiarity or expertise.*"[242] Other factors which were highlighted were low numbers of total transactions, when compared to traditional currency, and the "*relatively small number of individuals and businesses accepting digital currencies as payment for goods and services.*"[243] These factors may reduce the level of flexibility for money launderers as their transactions may appear more suspicious in a smaller group of transactions and with a reduced pool of businesses to funnel their proceeds through. Due to these issues the consultation paper concluded that "*serious organised money launderers may favour conventional payment methods instead.*"[244]

On the question of regulation, the consultation found the large majority of respondents favoured some form of regulation. The call for information received over 80

[239] GOV.UK, 'Digital currencies: response to the call for information' <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf> accessed 11 March 2016 at p.11.
[240] ibid.
[241] ibid.
[242] ibid at p.12.
[243] ibid.
[244] ibid.

respondents that "*on the whole favoured acting using existing frameworks in the short-term*[245]" due to the potential costs of a bespoke regime and that it may be premature to attempt to create a bespoke regime. The argument against a bespoke regime was that cryptocurrencies *"are still in a very early stage of development and it is difficult to predict what direction the technology might go in."*[246]

As a result of the consultation, and in respect of the appeal of cryptocurrencies to both legitimate and illicit purposes, the "*government intends to apply anti-money laundering regulation to digital currency exchanges.*"[247] This approach was decided upon due to the nascent state of digital currencies in the UK, and while the risk of digital currencies was perceived to be low, consumer protection and potential criminal uses must be considered.[248] The UK Government failed to follow through on its plan to regulate cryptocurrency exchanges, the ongoing fallout from the 2016 EU referendum has dominated the political agenda. The average number of Acts of Parliament passed per year between 2010 to date is 31, compared to 38 from 2000-2009, and 54 per year in the 80s and 90s.[249] Although legislation was not passed, in 2018 HM Treasury created the 'Cryptoassets Taskforce'[250] which has been tasked with setting out the "*UK's policy and regulatory approach to cryptoassets and distributed ledger technology in financial*

[245] ibid.
[246] ibid.
[247] ibid.
[248] ibid.
[249] All figures based on data gathered from: Legisaltion.Gov, 'Your search for UK Public General Acts has returned more than 200 results' < https://www.legislation.gov.uk/ukpga> accessed 20 September 2019.
[250] HM Treasury, 'Fintech Sector Strategy: Securing the Future of UK Fintech' (22 March 2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/692874/Fintech_Sector_Strategy_print.pdf> accessed 20 September 2019 at p18.

services."[251] The UK has adopted the term 'cryptoassets' to describe "*cryptographically secured digital representations of value or contractual rights that use some type of distributed ledger technology.*"[252] The term cryptoassets is interchangeable with the term cryptocurrencies, which is used in this research and more commonly worldwide.[253] The Cryptoassets Taskforce published their final report in October 2018.[254]

The recommendations of the Cryptoassets Taskforce are similar to that of HM Treasury in 2015 in response to their call for information,[255] but the plans for regulation are more detailed. The Cryptoassets Taskforce outline a 'regulatory perimeter' to determine which cryptocurrencies and related activities are to be covered by the regulation of the FCA.[256] It was noted that cryptocurrencies can be used to complete cross border transactions, and that the cryptocurrency elements of such transactions are not regulated,[257] which is a concern. With regards to AML measures and cryptocurrencies, the most important conclusion from the Cryptoassets Taskforce is that the "*government will bring fiat-to-cryptoasset exchange firms and custodian wallet*

[251] GOV.UK, 'Cryptoassets Taskforce: final report' (30 July 2018) <https://www.gov.uk/government/publications/cryptoassets-taskforce> accessed 20 September 2019.
[252] Financial Conduct Authority, 'Cryptoassets: Our Work' (23 January 2019) https://www.fca.org.uk/firms/cryptoassets> accessed 20 September 2019.
[253] The Bank of England explains what cryptoassets are by explaining cryptocurrencies: Bank of England, 'What are cryptoassets (cryptocurrencies)?' <https://www.bankofengland.co.uk/knowledgebank/what-are-cryptocurrencies> accessed 20 September 2019.
[254] HM Treasury, 'Cryptoassets Taskforce: final report' (29 October 2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf> accessed 20 September 2019.
[255] GOV. UK, 'Digital currencies: response to the call for information' <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf> accessed 20 September 2019.
[256] HM Treasury, 'Cryptoassets Taskforce: final report' (29 October 2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf> accessed 20 September 2019 at p.17.
[257] ibid.

providers within the scope of AML/CTF regulation, as required by [the 5th Money Anti-Laundering Directive]."[258] By implementing the 5th Anti-Money Laundering Directive[259] the UK will also be compliant with the guidance issued by the FATF.[260]

5.7.2. Financial Conduct Authority

The FCA does not currently supervise cryptocurrency service providers, their website is explicitly clear on this point:

> *Exchange tokens (such as Bitcoin and 'cryptocurrency' equivalents) are not currently regulated in the UK. This means that the transfer, purchase and sale of exchange tokens, including the operation of exchange token exchanges, all currently fall outside our regulatory remit.*[261]

This position is repeated in the FCA's response to the 2019 Cryptoassets Taskforce consultation on the regulation of cryptocurrencies.[262] The consultation found that almost all respondents agreed that cryptocurrencies were outside of the regulatory perimeter,[263] but only a third of respondents said that regulation should be imposed.[264]

---

[258] ibid at 5.7 on p.41.
[259] Council Directive 2018/843/EU 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 L 156/43.
[260] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2019.
[261] Financial Conduct Authority, 'Cryptoassets' (07 March 2019) <https://www.fca.org.uk/consumers/cryptoassets> accessed 23 September 2019.
[262] Financial Conduct Authority, 'Guidance on Cryptoassets: Feedback and Final Guidance to CP 19/3' (London, July 2019) <https://www.fca.org.uk/publication/policy/ps19-22.pdf> accessed 23 September 2019 at 2.3.
[263] ibid at 2.4.
[264] ibid at 2.5.

In March 2019 the FCA published research into UK consumers' use of cryptocurrencies.[265] It was not focussed on financial crime, but the findings were concerning when viewed from an AML perspective. The headline findings were that users were buying cryptocurrencies based on limited information, often influenced by a rejection of mainstream media, a fear of missing out on trends, and seeking to 'get rich quick'. [266] The report stated that a "*typical journey to purchasing cryptoassets for these respondents was based on a suggestion by a single acquaintance, or a persuasive online source relaying the large sums of money to be made.*"[267] This creates favourable conditions for fraudsters and those seeking unsuspecting money mules. If consumers are poorly informed then they are more likely to make poor financial choices, and the numbers of individuals being used as money mules is increasing both in young people[268] and older people.[269] The FCA report found that users would be more influenced by online sources rather than mainstream media, which means these users will be in areas of the internet completely free from regulatory scrutiny, which puts them at risk of being persuaded or duped into assisting with money laundering.

The FCA is now the principal regulator of cryptocurrency service providers since the implementation of the 5th Anti-Money Laundering Directive,[270] it is therefore required

[265] Financial Conduct Authority, 'How and why consumers buy cryptoassets: A report for the FCA' (07 March 2019) <https://www.fca.org.uk/publication/research/how-and-why-consumers-buy-cryptoassets.pdf> accessed 23 September 2019.
[266] ibid at p.47
[267] ibid.
[268] BBC News, 'Rise in teenage money mules prompts warnings' (16 September 2019) <https://www.bbc.co.uk/news/business-49717288> accessed 23 September 2019.
[269] BBC News, ''Money mules': Rising numbers are in middle age' (18 June 2019) <https://www.bbc.co.uk/news/uk-48671542> accessed 23 September 2019.
[270] HM Treasury, 'Cryptoassets Taskforce: final report' (29 October 2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/7

to enforce compliance with AML regulation. The guidance provided by the FCA shows the UK is going beyond the minimum requirements of the EU directive. The 5th Anti-Money Laundering Directive requires businesses which exchange between cryptocurrency and fiat currency to be regulated, whereas the FCA also includes businesses which exchange cryptocurrency for other cryptocurrencies. It is currently unclear how the FCA plans implement regulation of cryptocurrency service providers, it is yet to determine how regulation will be tailored to apply to such businesses. The issue of the UK's withdrawal from the EU has been addressed by the FCA and the Cryptoassets Taskforce, the current position is that the UK will continue to implement EU Law.[271] "*Obligations derived from EU law will continue to apply and firms must continue with implementation plans for EU legislation*"[272] while the UK remains a member of the EU, and during any transitional period.[273] The initial consultation was conducted while Theresa May was Prime Minister, but no clear or predictable changes have occurred since Boris Johnson became Prime Minister. The response to the consultation on the transposition of the Directive was published in January 2020, and made clear that while the UK is leaving the EU, it would still apply EU law during the implementation period of the UK withdrawal.[274] The consultation also states that the UK remains committed to implementing the standards of the FATF, which are of an equal standard to the EU measures.

52070/cryptoassets_taskforce_final_report_final_web.pdf> accessed 20 September 2019 at 5.7 on p.41.

[271] Financial Conduct Authority, 'Guidance on Cryptoassets: Feedback and Final Guidance to CP 19/3' (London, July 2019) <https://www.fca.org.uk/publication/policy/ps19-22.pdf> accessed 23 September 2019 at 1.33.

[272] ibid.

[273] ibid.

[274] HM Treasury, 'Transposition of the Fifth Money Laundering Directive: response to the consultation' (London, January 2020) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/860491/5MLD_Consultation_Response.pdf> accessed 27 July 2020 at 1.3.

5.7.3. National Crime Agency

Based on the NCA's website it is not clear how it views the money laundering threat of cryptocurrencies. However, in the response to the government's 'Digital currencies: call for information' the NCA suggested that the *"predominant criminal use of such currencies was on online marketplaces for the sale and purchase of illicit goods and services."*[275] The NCA's initial assessment was that "*digital currencies had not been widely adopted as a means of payment for goods and services in the broader criminal community."*[276] Additionally the NCA observed that the *"scale of the threat was difficult to assess, but said that there was little evidence to indicate use by established money laundering specialists or that digital currencies played a role in terrorist financing."*[277] In making this judgement, the NCA considered that the *"majority of illicit digital currency spends were for low-value transactions."*[278] This assessment by the NCA could be viewed as a fair at the time it was made, but the value of cryptocurrencies has increased since, Bitcoin reached a record high of $19,447 in December 2017.[279]

The NCA does consider cryptocurrencies as a crime threat, but is does so among its cybercrime activities, rather than money laundering.[280] The focus of the NCA's

[275] GOV. UK, 'Digital currencies: response to the call for information' <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf> accessed 11 March 2016 at p.14.
[276] ibid.
[277] ibid.
[278] ibid.
[279] XE, 'USD per 1 XBT' <https://www.xe.com/currencycharts/?from=XBT&to=USD&view=2Y> accessed 19 March 2019.
[280] National Crime Agency, 'Cyber Crime' <https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime?highlight=WyJiaXRjb2luIiwiYml0Y29pbnMiXQ==> accessed 20 September 2019.

cryptocurrency concerns appear to be focussed on 'cryptojacking',[281] which refers to the practice of using malware to use a victim's computer to mine cryptocurrency for the malware creator.[282]

Although money laundering through cryptocurrencies is not a publicised priority of the NCA, it has recently assisted in the conviction of Thomas White, for running a $100m dark web business selling drugs and indecent images of children.[283] White was convicted of multiple offences, including money laundering, and was sentenced to 5 year and 4 months. It not possible to infer how the use of cryptocurrency affected White's sentence, but it is in-line with the typical length of sentence the NCA investigations have led to. Despite the NCA's opinion of a minimal threat existing, it is worth noting the principles of its approach, which are to pursue, prevent, and prepare against serious organised crime in the UK,[284] and the conviction of White demonstrates that the NCA will not ignore cryptocurrency money laundering. Therefore, in relation to protecting and preparing, the NCA should remain watchful of cryptocurrencies, especially if they become more widely used, as they may require more attention.[285]

[281] National Crime Agency, 'The cyber threat to UK business 2017/18' (10 April 2018) <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/178-the-cyber-threat-to-uk-business-2017-18/file> accessed 20 September 2019 at p25.
[282] ibid.
[283] National Crime Agency, 'Student behind $100m dark web site jailed for 5 years 4 months' (12 April 2019) <https://www.nationalcrimeagency.gov.uk/news/student-behind-100m-dark-web-site-jailed-for-5-years-4-months?highlight=WyJiaXRjb2luIiwiYml0Y29pbnMiXQ==> accessed 20 September 2019.
[284] National Crime Agency 'Economic Crime Command' <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime> accessed September 2019.
[285] See chapter three at 3.4 for a discussion of money, whether cryptocurrencies are used widely enough to be considered money.

5.8. Compliance with Financial Action Task Force Guidance

In light of the 2019 *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*[286] issued by the FATF, the level to which the UK is compliant must be assessed. The UK is currently not compliant with the latest guidance from the FATF, as it currently does not regulate cryptocurrency service providers, but it is partially compliant as it is assessing the risks posed by cryptocurrencies.

The FATF guidance addresses how its members can apply the Recommendations to what it describes as 'virtual assets' and 'virtual asset service providers'. Virtual assets (VAs) are defined as a "*digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes*."[287] This definition is wide and includes cryptocurrencies, the FATF guidance "*focuses on VAs that are convertible for other funds or value, including both VAs that are convertible to another VA and VAs that are convertible to fiat or that intersect with the fiat financial system,*"[288] which demonstrates a clear targeting of cryptocurrencies. Virtual asset service providers (VASPs) are defined as any natural or legal person providing financial services relating to VAs, which includes exchanging between VAs and fiat currencies or other forms of VAs, transferring virtual assets or providing mechanisms for the storage of VAs, or providing a market for buying and selling VAs.[289]

[286] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2019
[287] ibid at para 33(b).
[288] ibid at para 14.
[289] ibid at para 33(c).

In relation to Recommendation 1, members should conduct risk assessments of VAs and VASPs in their jurisdiction. The UK has been assessing the risks posed by cryptocurrencies since 2015 through public consultation,[290] and the most recent publications from the Cryptoassets Taskforce provide definitions and understanding of how the types of "*VA products and services function, fit into, and affect all relevant regulatory jurisdictions for AML/CFT purposes*".[291] This satisfies part of the FATF guidance on the implementation of Recommendation 1 in relation to cryptocurrencies but there is a lack of clarity to the treatment of VAs, so the UK does not "*promote similar AML/CFT treatment for similar products and services with similar risk profiles*."[292] The UK needs to provide clear guidance on the regulation of cryptocurrencies in order to fully comply with the FATF guidance.

FATF guidance on Recommendations 3-7 require legislation relating to money laundering offences, confiscation and asset freezing to consider "*all funds or value-based terms in the Recommendations, such as "property," "proceeds," "funds," "funds or other assets," and other "corresponding value," as including VAs.*"[293] The UK is compliant with this guidance, as has been demonstrated through successful convictions for money laundering offences,[294] and successful conversion of cryptocurrency assets[295] where confiscation has been possible. From the successful

[290] GOV. UK, 'Digital currencies: response to the call for information' <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf> accessed 24 September 2019.
[291] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 September 2019 para 58
[292] ibid.
[293] ibid at para 65.
[294] See the convictions of White, Teresko, and West discussed at 7.3.3 above.
[295] cf Hall (n39) and see discussion at 7.3.2 above.

convictions it appears that the UK will not need to legislate in order to comply with FATF guidance.

The UK is technically compliant with FATF guidance on the regulation of cryptocurrency service providers. "*Countries should designate one or more authorities that have responsibility for licensing and/or registering VASPs*."[296] The UK has designated the FCA as this authority, but the FCA are yet to implement any regulation. Cryptocurrency exchanges and service providers are required to register with the FCA, which is compliant with FATF guidance in relation to applying Recommendation 14 to VASPs,[297] and in applying Recommendation 15 with regard to new technologies.[298]

When the FCA does apply AML regulation to cryptocurrency service providers it will need to ensure CDD processes are completed by newly regulated entities[299] to the same standards as the entities that are currently regulated. [300] As well as complying with CDD requirements, cryptocurrency service providers should become part of the UK's SARs regime,[301] share information with the NCA as the FIU,[302] and have

[296] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2019 para 77.
[297] ibid at para 107.
[298] Financial Action Task Force, 'The FATF Recommendations' <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> accessed 24 September 2019 at p.15.
[299] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2019 para 91.
[300] As outlined above at 7.4.1.
[301] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2019 para 124.
[302] ibid at para 129.

adequate risk management systems.[303] The FATF recommend that particular attention must be paid to the pseudonymous nature of cryptocurrencies, the lack of a physical meeting with the customer, and payments from unidentified third parties.[304] The FATF guidance in unclear as to how these issues should be addressed, but it is clear that they raise the level of risk associated with such transactions.[305] The FATF is clear that people who manage cryptocurrency service providers should not be criminals, thus should be required to be qualified people.[306]

The FATF provides guidance as to how the FCA can adapt its supervision for cryptocurrency service providers, and such guidance is applicable to all regulated institutions. One example of adjustments suggested is employing "*both offsite and onsite access to all relevant risk and compliance information*",[307] but that offsite alone is not "*appropriate in higher risk situations.*"[308] Additionally a varied frequency and nature of the supervision is suggested, using "*periodic reviews and ad hoc AML/CFT supervision as issues emerge.*"[309] Finally, the FATF recommend adjusting the intensity of AML supervision to correlate with the level of risk identified with the regulated entity.[310] The suggestions from the FATF are applicable to all regulated entities, and the guidance demonstrates the FATF recommend a proportionate response, in line with the risk based approach, and not a one size fits all approach to cryptocurrencies. As part of a risk based approach the FATF recommends that supervisors increase

[303] ibid at para 104.
[304] ibid at para 100.
[305] ibid at para 100.
[306] ibid at para 82.
[307] ibid at para 153(a).
[308] ibid at para 153(a).
[309] ibid at para 153(b).
[310] ibid at para 153(c).

their understanding of cryptocurrencies and the related businesses to better inform their risk assessments.[311] Through the Cryptoassets Taskforce and the research published by the FCA,[312] the UK is clearly developing its understanding of cryptocurrencies, but further development will require investment in training and IT capabilities, which have been identified as deficiencies in the UKFIU by the FATF.[313]

The FATF is also clear that Recommendation 33 is implemented through the regulation of cryptocurrencies, requiring record keeping and that statistics are maintained.[314] This is in keeping with the collection of financial intelligence, meaning the FIU will have the appropriate data to be able to better determine what transactions are suspicious and require investigation.

In assessing the UK's compliance with the FATF guidance, it is clear that the UK's criminal offences are compliant with the FATF guidance, as the money laundering offences are not avoided by using cryptocurrencies; this is demonstrated by successful prosecutions. The UK is becoming compliant in Recommendations relating to supervision of VASPs, this will be addressed fully by 2021, as this is the deadline for VASPs to register with the FCA under the amended 2017 Money Laundering Regulations. Widening the regulatory perimeter is required, and has been promised

[311] ibid at para 144.
[312] Financial Conduct Authority, 'How and why consumers buy cryptoassets: A report for the FCA' (07 March 2019) <https://www.fca.org.uk/publication/research/how-and-why-consumers-buy-cryptoassets.pdf> accessed 23 September 2019
[313] FATF, 'Anti-money laundering and counter-terrorist financing measures – United Kingdom, Fourth Round Mutual Evaluation Report' (Paris, December 2018) <fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-Kingdom-2018.pdf> accessed 11 September 2019 at para 6
[314] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2019 para 74.

by both the Cryptoassets Taskforce and the FCA, but as the implementation is not yet in effect it cannot be judged. While a welcome step, the widening of the regulatory perimeter is limited as it applies existing AML measures to cryptocurrencies, rather than developing a tailored approach.

5.9. Summary

This chapter has identified that UK money laundering offences are future proofed with regard to cryptocurrencies, because the drafting of the criminal law is clearly wide enough for the offences to be satisfied if criminals use cryptocurrencies. The money laundering convictions obtained demonstrate a sentencing policy which is consistent with cases not involving cryptocurrencies, but the limited number of cases and multi-offence nature of the convictions means it is not possible to draw clear conclusions or identify any trends. The convictions prove that money laundering using cryptocurrencies is taking place, but the extent is unclear. Seizing cryptocurrencies presents a further complication to more traditional money laundering techniques, and where cryptocurrencies have been successfully seized, the length of time from seizure to converting the assets into fiat currencies could lead to law enforcement agencies facing a lottery as to what they eventually recover due to fluctuating values.

With regards to the preventative measures, cryptocurrencies are not yet subject to AML regulations in the UK. The UK has a developed AML approach, keeping pace with international standards since first creating money laundering offences in the 1980s. The UK has a recognised FIU in the form of the NCA, which receives all SARs,

but this authority has been identified as having "*a lack of available resources*"[315] by the FATF, in terms of personnel, technology, and "*analytical capability*".[316] These weaknesses are of particular concern given the threat posed by cryptocurrencies, and will require investment as identified by the FATF in its 2019 guidance.[317] The Cryptoassets Taskforce has been charged with addressing the threats posed by cryptocurrencies, of which money laundering has been identified as a concern and the FCA has been determined as the appropriate authority to regulate cryptocurrency service providers. The FCA is the principal regulator of the UK financial services sector and is responsible for enforcing compliance with AML legislation, but has repeatedly stated that is does not currently regulate cryptocurrencies. The FCA will be required to regulate cryptocurrency service providers for AML purposes, in accordance with the EU's 5th Anti-Money Laundering Directive, but it remains to be seen how the FCA will implement such regulation. The future regulation of cryptocurrencies in the UK remains unclear as the FCA has only published guidance on which businesses need to register with it, it is reasonable to predict that cryptocurrency service providers will be required to adhere to CDD and reporting requirements, as this is the level of regulation required by the 5th Anti-Money Laundering Directive.

The next chapters will consider the approach of the United States of America and Australia, as cryptocurrency service providers are already subject to AML regulation

[315] FATF, 'Anti-money laundering and counter-terrorist financing measures – United Kingdom, Fourth Round Mutual Evaluation Report' (Paris, December 2018) <fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-Kingdom-2018.pdf> accessed 11 September 2019 at para 6.
[316] ibid.
[317] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2019 para 144.

in these jurisdictions. This is overseen by the Financial Crimes Enforcement Network (FinCEN) in the US and the Australian Transaction Reports and Analysis Centre (AUSTRAC) in Australia. The responses of the US and Australia will be used to provide potential lessons for the UK in regulating cryptocurrencies.

Chapter 6. United States of America

6.1. Chapter Overview

In this chapter, the applicability of the Unites States of America's (US) money laundering offences and preventative measures to cryptocurrencies will be assessed. Firstly, the money laundering offences will be outlined, and it will be considered whether or not it is possible to commit these offences using cryptocurrencies. It will be seen that the criteria of US money laundering offences will still be met where cryptocurrencies are used to process the proceeds of crime. Secondly, the preventive measures will be assessed; the US anti-money laundering (AML) regime will be analysed, and it will be seen whether or not these preventive measures apply to cryptocurrency transactions, and cryptocurrency businesses. In light of regulator guidance, cryptocurrency users are not required to adhere AML requirements, but those operating as a business, especially operating exchanges, are required to meet the same standard as 'money services businesses'.[1] After analysing the legislation, the various authorities will also be considered, first in terms of their role in the AML regime, and then considering how the relevant authorities are addressing cryptocurrencies. Having analysed the legislation and authorities, the response of the US will be assessed against the guidance of the Financial Action Task Force (FATF) issued in 2019.

[1] FinCEN, 'Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies' <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf> accessed 04 September 2019.

6.2. AML Approach

Tomas and Roppolo[2] split US AML legislation into two categories; criminal law and the implementing of regulations under the Bank Secrecy Act 1970 (BSA). This is a split, which is consistent with both the UK and Australia; money laundering is pursued through criminalising money laundering and implementing preventative measures which regulated entities must comply with.

6.3. Criminalising Money Laundering

US money laundering offences are codified under Title 18 of the United State Code §§1956-1957, which were introduced by the Money Laundering Control Act 1986.[3] Section 1956 contains three offences; money laundering, international money laundering, and laundering money activity using money purported to be criminal proceeds. The third offence will only apply in government sting operations; such operations are also able to secure convictions for international money laundering. §1957 contains a further money laundering offence, which criminalises "*spending or depositing tainted money.*"[4]

[2] J. P. Thomas and W. V. Roppolo, 'United States of America' in A. Srivastava, M. Simpson and N. Moffat, *International Guide to Money Laundering Law and Practice* (Bloomsbury, 2013) at 41.20.
[3] Pub. L. No. 99-570, 100 Stat. 3207-18.
[4] Federation of American Scientists, 'Congress Research Service: Money Laundering: An Overview of 18 USC 1956 and Related Federal Criminal Law' <https://www.fas.org/sgp/crs/misc/RL33315.pdf> accessed 11 December 2015.

6.3.1. §1956 - Laundering of monetary instruments

The actus reus of the money laundering offence is conducting, or attempting to conduct, *"a financial transaction which in fact involves the proceeds of specified unlawful activity."*[5] The mens rea of the offence is the knowledge and intent of the individual; "*knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity,*"[6] and intending to promote the "*carrying on of specified unlawful activity;*"[7] evade tax;[8] avoid reporting requirements;[9] or hide the ownership of the property.[10] In hiding the ownership, the intent must be to "*conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity*."[11] This is a broad drafting of the law, which is required so as to encompass the broad nature of money laundering.

A separate offence exists in §1956(a)(2), which is committed if a person moves "*a monetary instrument or funds*"[12] either from inside the US to outside the US, or from outside the US to inside the US. The mens rea of the international money laundering offence has a lower threshold than the §1956(a)(1) offence, as there is no requirement to know that the monetary instrument or funds are the proceeds of crime. The intent of the transaction is the same as in §1956(a)(1), but with the omission of the tax evasion criterion. With regard to the intent of the defendant, emphasis is placed on their understanding of the money involved; the money may be legitimate money, which

[5] 18 USC §1956(a)(1).
[6] ibid.
[7] 18 USC §1956(a)(1)(A)(i).
[8] 18 USC §1956(a)(1)(A)(ii).
[9] 18 USC §1956(a)(1)(B)(ii).
[10] 18 USC §1956(a)(1)(B)(i).
[11] ibid.
[12] 18 USC §1956(a)(2).

is used in a sting operation. The knowledge of the defendant "*may be established by proof that a law enforcement officer represented*"[13] the proceeds of a specified unlawful activity, and "*the defendant believed such representations to be true.*"[14] As with the §1956(a)(1) offence, the defendant must intend to "*conceal or disguise the nature, the location, the source, the ownership, or the control of*" the criminal proceeds.

The third money laundering offence in §1956 is designed to allow for government sting operations; it removes the requirement for a 'specified unlawful activity' as this would not have taken place if the money came from a law enforcement agency. The knowledge requirement for this offence is slightly different to that of the first two offences; the prosecutor must show that the offender believed the "*representation made by a law enforcement officer*."[15] The financial transaction element of the actus reus is the same as §1956(a)(1), therefore, for the offence to be committed using cryptocurrencies, the definition of a financial transaction needs to be satisfied. The mens rea of the offence, as with §1956(a)(1)-(2), requires the individual to intend to "*conceal or disguise the nature, location, source, ownership, or control of*"[16] the proceeds in question.

The first two offences are very similar, but there are two key distinctions; firstly, §1956(a)(1) does not define where the activity must take place, whereas §1956(a)(2) states that the offence must involve a transaction passing in or out of the United States.

[13] ibid.
[14] ibid.
[15] 18 USC §1956(a)(3)(C).
[16] 18 USC §1956(a)(3)(B).

Secondly §1956(a)(2) uses the terms "*monetary instrument or funds,*"[17] which differs from the term "*financial transaction*"[18] used in §1956(a)(1). The third offence has the same requirements and §1956(a)(1), but the proceeds do not need to be from a specified unlawful activity. For cryptocurrencies to be used to satisfy §1956(a)(1) and (3), the term "*financial transaction*"[19] needs to be defined, and for §1956(a)(2) to apply, "*monetary instrument or funds*"[20] must be defined; cryptocurrencies must satisfy these definitions in order for the offences to be committed using cryptocurrencies. If cryptocurrencies satisfy the definition, then they must be the proceeds of an 'unlawful activity'. There must be knowledge that the proceeds involved represented such proceeds, and intent to "*conceal or disguise the nature, location, source, ownership, or control*"[21] of the proceeds.

The conviction of Ross Ulbricht confirms that the use of cryptocurrency can satisfy §1956. Ulbricht created and operated Silk Road, a website which facilitated the trading of illegal items such as drugs,[22] and was only accessible using a Tor browser which provided anonymity to users.[23] Among the offences Ulbricht was found guilty of, §1956 received special attention from the court, specifically whether transactions in Bitcoin satisfied the term financial transaction. The court concluded that the "*money laundering statute is broad enough to encompass use of Bitcoins in financial*

[17] 18 USC §1956(a)(2).
[18] 18 USC §1956(a)(1).
[19] ibid.
[20] 18 USC §1956(a)(2).
[21] 18 USC §1956(a)(1)-(3).
[22] Department of Justice, U.S. Attorney's Office Southern District of New York, 'Ross Ulbricht, A/K/A "Dread Pirate Roberts," Sentenced In Manhattan Federal Court To Life In Prison' (Manhattan, New York, 29 May 2015) <https://www.justice.gov/usao-sdny/pr/ross-ulbricht-aka-dread-pirate-roberts-sentenced-manhattan-federal-court-life-prison> accessed 05 September 2019.
[23] BBC News, 'Silk Road drug website founder Ross Ulbricht jailed' (30 May 2015) <https://www.bbc.co.uk/news/world-us-canada-32941060> accessed 05 September 2019.

transactions."[24] Ulbricht is not the only individual to be convicted for money laundering using cryptocurrencies, numerous convictions have been announced through press releases from the Department of Justice. Cases vary in complexity and value, just as all criminal cases will, from an international gang being investigated for 18 months,[25] to a one-man operation of a much smaller scale.[26] The prosecutions for money laundering using cryptocurrencies demonstrate that §1956 does not need reform, as cryptocurrency transactions clearly satisfy the widely drafted criminal offences.

6.3.2. §1957: Engaging in monetary transactions in property derived from specified unlawful activity

A further money laundering offence is contained in 18 USC §1957; this offence criminalises "*spending or depositing tainted money.*"[27] The offence requires an individual to "*engage in a monetary transaction in criminally derived property of a value greater than $10,000 and is derived from specified unlawful activity.*"[28] The wording of §1957(a) is similar to §1956(a)(2) in that it requires a "*monetary transaction,*"[29] rather than a financial transaction. However, the definition provided in §1957(a)(1) makes it clear that this can be satisfied by anything constituting a financial transaction, in

[24] *United States v. Ulbricht*, 858 F.3d 71, 82–83 (2d Cir. 2017) at 570.
[25] Department of Justice, U.S. Attorney's Office Western District of Washington, 'Multi-State International Drug Trafficking Organization Targeted in 18-Month Investigation' (Washington, United States, 6 December 2018) <https://www.justice.gov/usao-wdwa/pr/multi-state-international-drug-trafficking-organization-targeted-18-month-investigation> accessed 04 September 2019.
[26] Department of Justice, U.S. Attorney's Office Central District of California, '"Bitcoin Maven" Sentenced to One Year in Federal Prison in Bitcoin Money Laundering Case' <https://www.justice.gov/usao-cdca/pr/bitcoin-maven-sentenced-one-year-federal-prison-bitcoin-money-laundering-case> accessed 04 September 2019.
[27] Federation of American Scientists, 'Congress Research Service: Money Laundering: An Overview of 18 USC 1956 and Related Federal Criminal Law' <https://www.fas.org/sgp/crs/misc/RL33315.pdf> accessed 11 December 2015.
[28] 18 USC §1957(a).
[29] ibid.

§1956(a)(1). As with the §1956 offences the offender does not need to know the specific origin of the money, but the §1957 offence is easier for the prosecution to obtain a conviction, as the prosecution do not need to "*prove the defendant knew that the offense from which the criminally derived property was derived was specified unlawful activity.*"[30] Case law[31] has shown that the prosecution only have to demonstrate that the offender knew they were "*receiving 'dirty' money, regardless of whether* [they] *knew the specific source*."[32] The §1957 offence is equally applicable to cryptocurrencies as §1956.

6.3.3. Financial Transaction

A financial transaction has a wide definition in §1956(c)(4), it includes "*the movement of funds by wire or other means*",[33] and can include the transfer of "*any real property, vehicle, vessel, or aircraft*".[34] 'Transaction' also has a broad definition in §1956(c)(3), including "*a purchase, sale, loan, pledge, gift, transfer, delivery, or other disposition*".[35] These definitions are wide, so as to allow for the vast array of mechanisms by which the proceeds of crime may be moved; as such this is not difficult to satisfy. The difficulties that may arise in relation to cryptocurrencies will be whether sending cryptocurrencies constitutes a financial transaction, or even a transaction at all. Given the already very broad definitions, it is likely that for the purposes of a money laundering offence, a cryptocurrency transfer will be considered to satisfy "*a*

[30] 18 USC §1957(c).
[31] See *USA vs Hawkey*, 148 F.3d 920 8th Cir.1998.
[32] L. Low et al, 'Country Report: The US Anti-Money Laundering System' in M. Pieth and G. Aiolfi, *A Comparative Guide to Anti-Money Laundering* (Edward Elgar, 2004) at p360.
[33] 18 USC §1956(c)(4).
[34] ibid.
[35] 18 USC §1956(c)(3).

transaction which in any way or degree affects interstate or foreign commerce […] *involving the movement of funds by wire or other means.*"[36] The Internal Revenue Service (IRS) has declared that for taxation purposes, virtual currencies are property, not currency;[37] but US money laundering law makes it clear that the buying, selling or otherwise transferring of property other than currency, can still constitute money laundering.[38] Therefore, converting illicit funds into cryptocurrency and transferring that cryptocurrency will satisfy the transaction requirement of the money laundering offence. In *USA v Ulbricht*[39] it was reasoned that there "*is no doubt that if a narcotics transaction was paid for in cash, which was later exchanged for gold, and then converted back to cash, that would constitute a money laundering transaction*",[40] and by the same virtue, an individual "*can money launder using Bitcoin*".[41]

6.3.4. Specified Unlawful Activity

Money laundering can only take place with illicit funds, if the funds are legitimate then no money laundering can take place. US law states that in order for an offence of money laundering to be committed, the funds must be the proceeds of a "*specified unlawful activity*;"[42] a list of such activities is found in §1956(c)(7). While the list of domestic offences under §1956(c)(7) is very wide as the US will have full jurisdiction to declare which of its own criminal offences satisfy US money laundering offences, the list of foreign offences is shorter. The foreign, or international, offences are found

[36] 18 USC §1956(c)(4).
[37] Inland Revenue Service, 'Notice 2014-21' <https://www.irs.gov/pub/irs-drop/n-14-21.pdf> accessed 17 December 2015.
[38] The §1956 offences refer to 'property' rather than currency.
[39] *United States v. Ulbricht*, 858 F.3d 71, 82–83 (2d Cir. 2017).
[40] ibid at 570.
[41] ibid at 570.
[42] 18 USC §1956(a)(1) and 18 USC §1956(a)(2)(A).

at §1956(c)(7)(D); as stated, the list is shorter than that of the domestic offences, but it is still a broad list. When first enacted the list only contained offences "*involving a controlled substance abuse, kidnapping, robbery, extortion, destruction of property by means of explosive or fire, a crime of violence or bank fraud*"[43]

The Uniting and Strengthening America by Providing Appropriate Tools to Restrict, Intercept and Obstruct Terrorism Act of 2001[44] (PATRIOT Act 2001) extends the list of foreign offences. The list currently includes destruction of aircraft, bribery, smuggling, embezzlement, child pornography, and even copyright.[45] Low, *et al*, have observed that where the offences committed are not included on the list, a prosecution can still be obtained "*by 'boot-strapping' them onto domestic*"[46] specified unlawful activities, this is demonstrated by *USA v Trapilo*.[47] Wire fraud is an offence that may be used for this, as the money will be part of a domestic offence via the transaction.[48] The requirement for a specified unlawful activity is unaffected by the use of cryptocurrencies.

6.3.5. Knowledge that the property involved represented the proceeds of crime

Knowledge must be present in order for money laundering offences to apply; the offender must act know that the property "*represents the proceeds of some form of unlawful activity.*"[49] With regard to this, the offender does not need to have knowledge

[43] cf Low et al (n32) at p353.
[44] 2001, Pub. L. No. 107-56
[45] 18 USC §1956(c)(7)(D).
[46] cf Low et al (n32) at p353.
[47] 130 F.3d 547. 2nd Cir. 1997
[48] cf Low et al (n32) at p353.
[49] 18 USC §1956(a)(1) and 18 USC §1956(a)(2)(B).

of the 'specified unlawful activity' the property resulted from. All that is required is that the offender knows the relevant property came from an "*activity that constitutes a felony under State, Federal, or foreign law, regardless of whether or not such activity is specified in paragraph (7)*."[50] As with the previous elements of the money laundering offences, this is drafted relatively widely, the offender does need to know that the money came from a 'specified unlawful activity', it only matters that it came from some form of criminal activity. Low *et al*, note how this element of the offence has been interpreted in the courts, stating that although knowledge is required by legislation, examples of 'wilful blindness'[51] have been accepted as satisfying the knowledge requirement.[52] The move from actual knowledge to wilful blindness is observed by Von Kaenel, as being judge led;[53] the legislation still requires knowledge, but the threshold for this has been lowered through case law, stemming from *United States* v *Jewell*[54] in 1976.

The knowledge element of the offence would be no different if the offender was to use cryptocurrency; the knowledge requirements are independent of the mechanism by which the money is laundered. One potential difference would be that it might be more plausible to deny knowledge of origins of the funds if they are being transferred using a crypto-currency, as the identity of the parties to a transaction may not be revealed to each other. This may be a test of the 'wilful blindness' standard; whether a defendant be able to successfully argue that they did not know the identity of the person they

[50] 18 USC §1956(c)(1).
[51] See *USA vs Campbell*, 997 F.2d 854, 857. 4th Cir 1992.
[52] cf Low et al (n32) at p355.
[53] F. J. Von Kaenel 'Wilful Blindness: A Permissible Substitute for Actual Knowledge under the Money Laundering Control Act?' (1993) 71 Wash ULQ 1189 at 1202.
[54] *United States* v *Jewell* 532 F.2d 697 (9th Cir.1976).

were dealing with, without attracting questions as to why they would deal with someone they do not know. Such considerations are currently speculative, the principle may be tested in the courts in the future.

6.3.6. Sentences

The three money laundering offences in §1956 each carry maximum sentences of twenty years; the domestic and international offences may also be punished by a fine, this may be up to "*$500,000 or twice the value*"[55] of the funds involved. The §1957 offence has a lower level fine; $250,000 for an individual,[56] or $500,000 for an organisation.[57] Examples of convictions include a 20 year sentence for drug trafficking and money laundering,[58] a forfeiture of $1,000,000 and a 5 year probationary sentence for structuring transactions to the value of $2.9million,[59] and a 30 year sentence for leading an international money laundering operation valued at over $250million.[60] It can be seen that structuring payments alone will be treated less severely than instances where drug trafficking is involved, or the complexity of the money laundering operation is high, particularly international schemes. Money laundering using cryptocurrencies will add complexity to the scheme, but will not immediately lead to a long sentence, a small-scale cryptocurrency money laundering operation has been

[55] 18 USC §1956(a)(1) and (2).
[56] 18 USC § 3571(b)(3).
[57] 18 USC § 3571(c)(3).
[58] S Parks, 'Houston Man Sentenced for Federal Drug Trafficking and Money Laundering Violations' (DEA, 17 May 2019)<https://www.dea.gov/press-releases/2019/05/17/houston-man-sentenced-federal-drug-trafficking-and-money-laundering> accessed 06 August 2019,
[59] K Korte, 'Postal Annex Owner Sentenced for Structuring Currency Transactions' (DEA, 11 September 2018) <https://www.dea.gov/press-releases/2018/09/11/postal-annex-owner-sentenced-structuring-currency-transactions> accessed 06 August 2019.
[60] S A K Mori 'Leader of International Drug Money Laundering Organization Sentenced to 30 Years in Prison' (DEA, 14 August 2018) <https://www.dea.gov/press-releases/2018/08/14/leader-international-drug-money-laundering-organization-sentenced-30> accessed 06 August 2019.

punished with a one-year sentence.[61] However, as shown by the *Ulbricht* case, much longer sentences will be imposed where the money laundering is complex and connected to multiple offences.[62] The criminal offences in the UK are equally applicable to those in the US, as demonstrated by the convictions in recent years,[63] but the prison sentences in UK cases have been shorter than in the US. Given that the US criminal offences clearly apply, attention must turn to preventative measures to analyse how the money laundering threat posed by cryptocurrencies is being combatted.

6.4. Preventative measures

Preventative measures can be divided into two categories, reporting requirements and customer due diligence. The US implements currency transaction reports (CTRs) and suspicious activity reports (SARs) as part of its reporting requirements, and customer due diligence is covered through know your customer (KYC) protocols. The two broad categories of AML measures interrelate, for example, a reporting entity is much better informed in deciding whether to submit a SAR if it has effective KYC provisions in

[61] Department of Justice, U.S. Attorney's Office Central District of California, '"Bitcoin Maven" Sentenced to One Year in Federal Prison in Bitcoin Money Laundering Case' <https://www.justice.gov/usao-cdca/pr/bitcoin-maven-sentenced-one-year-federal-prison-bitcoin-money-laundering-case> accessed 04 September 2019.
[62] BBC News, 'Silk Road drug website founder Ross Ulbricht jailed' (30 May 2015) <https://www.bbc.co.uk/news/world-us-canada-32941060> accessed 05 September 2019.
[63] Example discussed in chapter five at 5.3.1. including: *R* v *Teresko* [2018] Crim LR 81, Crown Prosecution Service, 'More than £1.2million of Bitcoin seized from drug dealer' (19 July 2018) <https://www.cps.gov.uk/south-east/news/more-ps12-million-bitcoin-seized-drug-dealer> accessed 11 September 2019 and BBC News, 'Liverpool 'dropout' jailed for Silk Road dark web site' (12 April 2019) <https://www.bbc.co.uk/news/uk-england-merseyside-47913780> accessed 11 September 2019 and National Crime Agency, 'Student behind $100m dark web site jailed for 5 years 4 months' (12 April 2019) <https://www.nationalcrimeagency.gov.uk/news/student-behind-100m-dark-web-site-jailed-for-5-years-4-months?highlight=WyJiaXRjb2luIiwiYml0Y29pbnMiXQ==> accessed 11 September 2019.

place. With regards to cryptocurrencies, the types of service providers that the preventative measures apply to will be of particular importance, as anti-money laundering regulations are applicable to cryptocurrency exchanges. The Financial Crimes Enforcement Network (FinCEN) issued guidance in 2013 on the application of its rules, making clear that while a regular user will not be subject to FinCEN regulation,[64] exchanges and administrators would be money services businesses, and would need to comply with FinCEN regulation.[65]

6.4.1. Currency Transaction Reports

Financial institutions are required to report each transaction of more than $10,000.[66] This requirement applies to single transactions, or to a number of transactions which aggregate total is over the value of $10,000.[67] Transactions are defined broadly, including purchases of "*chips, tokens, and other gaming instruments",*[68] payments on "*any form of credit*",[69] and currency exchanges.[70] A financial institution may be defined under the BSA 1970,[71] but the reporting requirement is determined based on the transaction rather than the institution as determined by FinCEN and the IRS.[72] The advice of FinCEN and the IRS is that "[e]*ach person engaged in a trade or business who, in the course of that trade or business, receives more than $10,000 in cash in*

[64] FinCEN, 'Guidance - FIN-2013-G001 - Issued: March 18, 2013 - Subject: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies' <https://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf> accessed 06 August 2019 at p2.
[65] ibid.
[66] 31 CFR §103.22(b)(1).
[67] 31 CFR §103.22(c).
[68] 31 CFR §103.22(b)(1)(i)(A).
[69] 31 CFR §103.22(b)(1)(i)(D).
[70] 31 CFR §103.22(b)(1)(i)(H).
[71] Codified at 31 U.S. Code § 5312.
[72] IRS, 'IRS/FinCEN Form 8300' <https://www.irs.gov/pub/irs-pdf/f8300.pdf> accessed 15 October 2019.

one transaction or in two or more related transactions"[73] must report. Related transactions are transaction *"conducted in a 24-hour period,"*[74] but transactions more than 24 hours apart may still be deemed related if "*the recipient knows, or has reason to know, that each transaction is one of a series of connected transactions*."[75]

A cryptocurrency transaction, like any transaction, will vary in size; freedom to contract and the wide range of reasons to transact mean that the values being transferred will differ. However, a factor that is particular to cryptocurrencies, is that the value of transaction may also vary from day to day due to the fluctuations in the cryptocurrency's value against the US Dollar.[76]

[73] ibid at p.3.
[74] ibid.
[75] ibid.
[76] Cryptocurrency value changes are discussed in chapter three at 3.3.

Figure 7. Bitcoin Value in US Dollars in 2018[77]

Figure 7 shows the generally downward trend in Bitcoin's value over 2018 but at a much greater rate than in established fiat currencies. The graph shows values from the beginning of each month in 2018, but values also fluctuated wildly in short periods, which could present some practical difficulties for submitting CTRs. On 7th January the value of bitcoin was $17,102.88,[78] so any transaction over 0.59 Bitcoin would need to be reported, but by 18th January the value of Bitcoin is $11,169.64[79] so transactions over 0.90 Bitcoin would need to be reported. The value of Bitcoin dropped over the course of 2018 and by 1st January 2019, a CTR would be required for a transaction of more 27.12 Bitcoin. While it is simple enough for a business to keep track of the value of Bitcoin, it becomes more complicated once other cryptocurrencies are considered,

[77] Complied using date from: XE, 'XE Currency Table: XBT - Bitcoin' <https://www.xe.com/currencytables/?from=XBT&date=2019-01-01> accessed 07 August 2019.
[78] XE, 'USD per 1 XBT' <https://www.xe.com/currencycharts/?from=XBT&to=USD&view=2Y> accessed 07 August 2019.
[79] ibid.

of which over 2000 exist.[80] The requirement of cryptocurrency businesses to submit CTRs to FinCEN presents a practical challenge for the regulated entities in keeping track of mandatory reports, but also upon FinCEN in monitoring compliance.

Annual CTR submission statistics are not available, but in 2016 the FATF mutual evaluation report stated that the average number of CTRs per year was 15,283,950. Requiring cryptocurrency businesses to submit CTRs will obviously lead to an increase in CTRs. It is difficult to claim that FinCEN are able to devote adequate attention to each and every CTR, and with numbers set to increase it will lead to the gathering of ever more data, but not necessarily intelligence. The UK does not implement mandatory threshold transaction reporting, and this research does not advocate the UK adopting such reporting standards. The FATF has identified that the NCA (the UKFIU) is already under resourced with the existing volume of SARs,[81] introducing further reports would not assist the NCA.

6.4.2. Suspicious Activity Reports

The BSA 1970 introduced SARs in the US, and initially only required banks and money services businesses to report.[82] §103.18-20 set out the criteria for when a bank or relevant business should report a transaction. This has since been widened by the PATRIOT Act 2001 to include all Securities Exchange Commission (SEC) registered

[80] CoinMarketCap list 2310 currencies on its 'All Cryptocurrencies' page: CoinMarketCap, 'All Cryptocurrencies' < https://coinmarketcap.com/all/views/all/> accessed 08 August 2019.
[81] FATF, 'Anti-money laundering and counter-terrorist financing measures – United Kingdom, Fourth Round Mutual Evaluation Report' (Paris, December 2018) <fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-Kingdom-2018.pdf> accessed 11 September 2019 at para 6.
[82] 31 CFR §§103.18-20 (2002).

brokers and dealers.[83] It as has also been extended to casinos by FinCEN,[84] and the Commodity Futures Trading Commission (CFTC) has applied it to futures commission merchants, commodity trading advisors and commodity pool operators.[85] The wording of the criteria differs slightly in each of the sections of the BSA 1970, but the meanings are the same as those found at §103.18(a)(2).[86] A regulated entity must report any transaction over $5,000 which is suspected to be from "*illegal activities*"[87] or "*assets derived from illegal activities*",[88] to evade the BSA 1970,[89] or has no "*apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage*"[90] in.

The only material difference in the law regarding the relevant types of entities is that money services businesses are required to report a suspicious transaction if it "*involves or aggregates funds or other assets of at least $2,000.*"[91] As with the CTRs the value of the transaction in cryptocurrency would need to be calculated against the $2,000 threshold before the entity reports.

The term 'suspicious' is also used by the UK when determining when a report is required, where it has caused confusion in determining when a report is necessary, as discussed in chapter five, at 5.4.2. Suspicion remains undefined in the US, as

[83] Pub. L. No. 107-56, §356(a).
[84] 67 Fed. Reg. 60722 (2002).
[85] Pub. L. No. 107-56, §356(b).
[86] 31 CFR §103.18(a)(2) codified at 12 CFR §21.11(c)(4).
[87] 31 CFR §103.18(a)(2)(i).
[88] ibid.
[89] 31 CFR §103.18(a)(2)(ii).
[90] 31 CFR §103.18(a)(2)(iii).
[91] 31 CFR §103.20(a)(2) codified at 31 CFR § 1022.320(a)(2).

observed by the Government Accountability Office; "*specific criteria for determining whether a transaction is suspicious have never been developed*."[92] FinCEN does provide some guidance as to when to report, and also some 'Red Flags' to be aware of which may trigger suspicion, and as such a report, but this guidance is not definitive. The first part of the FinCEN guidance simply restates the law, the transaction is reportable is it suspected to involve money from criminal activity, evade the BSA 1970, or have no apparent legal purpose.[93] The guidance provided on 'Red Flags' is more practical as FinCEN gives examples of 'Red Flag' incidents. These include the use of fake identification, customers reacting negatively to requests for identification, transactions very close to mandatory reporting value, and groups of transactions from multiple customers in a short period of time.[94] FinCEN's guidance suggests certain factors should be considered upon a 'Red Flag', such as whether the transaction is "*unusually large*",[95] whether the transaction is different to the customer's normal pattern of business, or whether the frequency of transactions is unusual.[96] These considerations demonstrate the inter-related nature of preventative measures as the questions may be best answered if the relevant KYC measures have been observed, and the reporting entity knows what is 'usual' for the customer. Transactions through cryptocurrency businesses are more likely to be viewed as suspicious as they take place remotely. It is more difficult to verify an individual's identity over the internet so the 'Red Flag' incidents relating to identity could be triggered frequently in cryptocurrency businesses, adding to the volume of SARs submitted to FinCEN.

---

[92] General Accounting Office, Money Laundering: Needed Improvements for Reporting Suspicious *Transactions Are Planned* (Washington, DC: General Accounting Office, 1995) at p11.
[93] FinCEN, 'Reporting Suspicious Activity – A Quick Reference Guide for Money Services Businesses' <https://www.fincen.gov/statutes_regs/guidance/pdf/msbsar_quickrefguide.pdf> accessed 14 October 2019.
[94] ibid.
[95] ibid.
[96] ibid.

Figure 8. Suspicious Activity Report Volume[97]

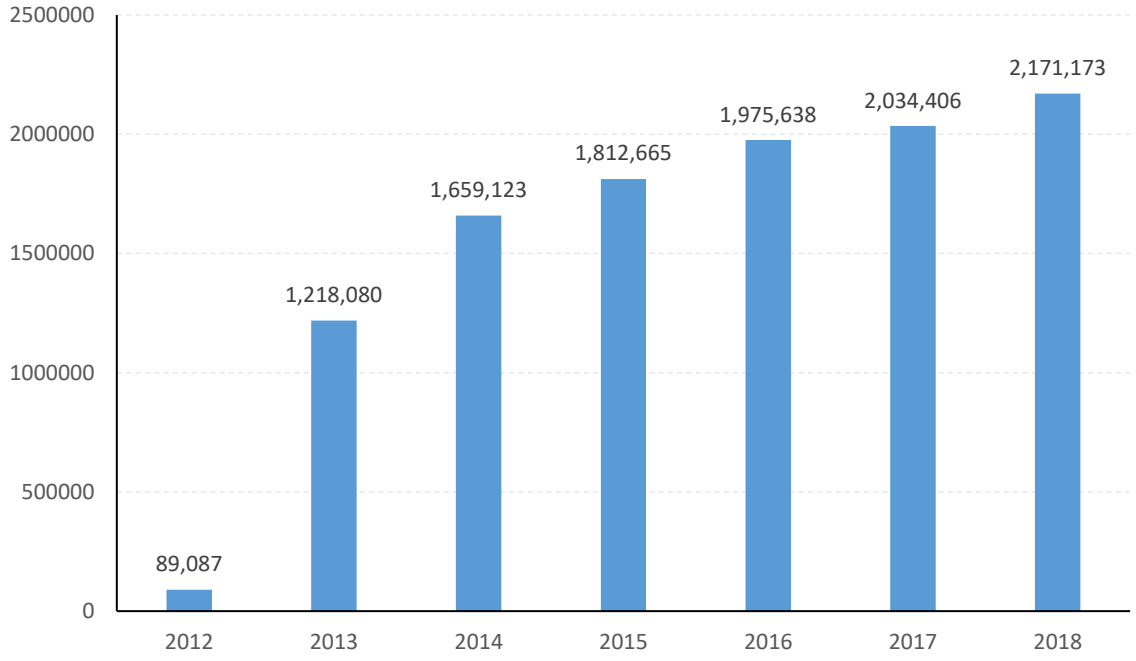


Figure 8 shows the annual volume of SARs submitted to FinCEN, which has increased year on year since 2012. One reason for the consistent rise in SARs is defensive reporting, as identified by Levi in the 1990s,[98] by McNeil in the early 2000s,[99] and Ryder in 2012.[100] The increasing size of sanctions imposed on banks, such as the $1.256bn settlement with HSBC in 2011,[101] and the $1bn sanction imposed on

[97] Compiled from the FinCEN Suspicious Activity Report Statistics tool, using the following search options; 'Industry Type': All, 'Year & Month': 2012-2018 respectively, all other selectors were left blank, the search tool is available at: FinCEN, 'Suspicious Activity Report Statistics (SAR Stats)' <https://www.fincen.gov/reports/sar-stats> accessed 21 August 2019.
[98] M. Levi, 'Evaluating the "New Policing": Attacking the Money Trail of Organized Crime' (1997) 30(1) Australian and New Zealand Journal of Criminology 1 at 9.
[99] C. McNeil, 'The Australian Anti-Money Laundering Reform in the International Context' (2007) 22(6) Journal of International Banking Law and Regulation 340 at 341.
[100] N. Ryder, *Money laundering – an endless cycle? A comparative analysis of the anti-money laundering policies in the United States of America, the United Kingdom, Australia and Canada* (Routledge, London, 2012) at 5.8.
[101] Department of Justice, 'HSBC Holdings Plc. and HSBC Bank USA N.A. Admit to Anti-Money Laundering and Sanctions Violations, Forfeit $1.256 Billion in Deferred Prosecution Agreement' (11 December 2012) <https://www.justice.gov/opa/pr/hsbc-holdings-plc-and-hsbc-bank-usa-na-admit-anti-money-laundering-and-sanctions-violations> accessed 23 August 2019.

Standard Chartered in 2019[102] for money laundering compliance failings, leads regulated institutions to comply so as to avoid receiving such punishments. Defensive reporting is where regulated institutions report whenever there is risk of suspicion, rather when there is genuine suspicion. This inflates the volume of reports to FinCEN, and makes it more difficult to determine which SARs need to be investigated. Given the severity of the potential sanctions for non-compliance, it is likely that cryptocurrency businesses, will adopt a similar approach to the institutions in the traditional financial system. A further risk for cryptocurrency businesses is that their ability to absorb a large fine may be dependent on the value of their holdings, which, as seen in Figure7, can be volatile. If failings take place while cryptocurrency value are high, then the potential money laundering will be of a higher value and the fine imposed on the institution will be higher. The expansion of the SARs regime to cryptocurrencies is likely to increase the volume of SARs, both due to defensive reporting, and simply because the number of regulated institutions has increased.

6.4.3. Know Your Customer

The second key element of the preventative measures is record keeping and KYC protocols. Specific records must be kept in certain circumstances, for example a customer verification process must be undertaken in the event of a sale or issuance of "*bank check or draft, cashier's check, money order or traveller's check for $3,000 or more,*"[103] and any other transaction over $10,000.[104] Information required from a new

[102] Department of Justice, 'Standard Chartered Bank Admits to Illegally Processing Transactions in Violation of Iranian Sanctions and Agrees to Pay More Than $1 Billion' (9 April 2019) <https://www.justice.gov/opa/pr/standard-chartered-bank-admits-illegally-processing-transactions-violation-iranian-sanctions> accessed 23 August 2019.
[103] 31 CFR §1010.415(a).
[104] 31 CFR §1010.410.

customer includes, but is not limited to; the name and address of the customer; their social security number of the purchaser, or identification number; their date of birth; the date of purchase; the type(s) of instrument(s) purchased; and the identification number of the purchased instrument(s).[105] In addition to these details in the event of a large transaction, financial institutions should also have customer identification programs (CIP) for all of their customers. A bank's CIP must be "*appropriate for its size and type of business,*"[106] but specific information is to be collected by all regulated businesses. A customer's name, date of birth, relevant addresses, and identification number are examples of mandatory data to be obtained.[107]

These requirements are part of a risk-based approach to money laundering which allows for differing requirements for different sized institutions. 31 CFR §103.121 sets the minimum requirements, but bigger institutions will be expected to do more to monitor their customers than smaller institutions. While 31 CFR §103.121 applies to banks, money services businesses are covered by 31 CFR §1022.210; which also states that the anti-money laundering program should correlate with "*the risks posed by the location and size of, and the nature and volume of the financial services provided by, the money services business*."[108] A money services business is any business that chases, exchanges, transfers, or transmits money, or similar instruments, domestically or internationally,[109] whilst not being a depository institution.[110] The minimum standards for a money services business is to verify their

[105] Criteria found in 31 CFR §1010.410 and 31 CFR §1010.415(a).
[106] 31 CFR §103.121.
[107] 31 CFR §103.121(b)(i)(1)-(5).
[108] 31 CFR §1022.210(b).
[109] 31 USC §5330(d)(1)(A).
[110] 31 CFR §1022.210(d)(1)(C).

customers' identity,[111] complete filing reports,[112] create and retain records,[113] and respond to requests for law enforcement.[114] A money services business is also required to provide education and training,[115] and undertake regular reviews of its anti-money laundering program.[116] The money services business should designate an individual to ensure compliance with the program.[117]

By complying with the KYC protocols and having an appropriate CIP it is easier to answer the questions which should be triggered by 'Red Flag' incidents and make it easier for an institution to decide what is, and is not, suspicious. KYC may also provide a greater bank of intelligence, and maybe even evidence if an investigation does need to take place. The issue with regards to cryptocurrencies is that KYC protocols and CIPs may not be possible to implement, or it may be harder to do so compared to other institutions. The nature of cryptocurrency businesses means they are unlikely to ever meet their customers physically, which in turn means it is not possible to confidently identify their customers. Chaikin finds fault with relying on customer data, criticising the assumption that customers will be honest and that there are no legal requirements for customers to provide full disclosure of the names they use or the accounts they have opened.[118] Chaikin also criticised the notably Western approach to what customer data needs to be collected, as this is ineffective for ethic groups who

[111] 31 CFR §1022.210(d)(1)(A).
[112] 31 CFR §1022.210(d)(1)(B).
[113] 31 CFR §1022.210(d)(1)(C).
[114] 31 CFR §1022.210(d)(1)(D).
[115] 31 CFR §1022.210(d)(3).
[116] 31 CFR §1022.210(d)(4)
[117] 31 CFR §1022.210(d)(2).
[118] D. Chaikin, 'Risk-Based Approaches to Combatting Financial Crime' (2009) 8(2) Journal of Law and Financial Crime 20 at 23.

use different naming systems.[119] It has been identified already in this thesis that cryptocurrencies provide users with mechanisms to conceal their identity,[120] applying KYC requirements to cryptocurrency businesses will be more difficult than for the traditional financial institutions.

6.5. Applicability of Preventative Measures to Cryptocurrencies

It has been established at 6.3.3 that cryptocurrencies will satisfy the term 'financial transaction' and as such money laundering offences are applicable, without a need to amend the law. The applicability of AML provisions to cryptocurrency businesses was not initially clear, but the FinCEN guidance of 2013 makes it clear that exchanges and administrators are viewed as money services businesses, and therefore need to comply with AML regulation.[121] By applying AML regulation to cryptocurrency businesses, the US is compliant with the FATF guidance issued in 2019,[122] before the guidance was released. The US has been proactive in applying its existing law, but simply widening AML regulation to cover cryptocurrency businesses does not show a detailed understanding of the issue. KYC protocols are applied to cryptocurrency

[119] ibid.
[120] The anonymity attached to cryptocurrencies is addressed by the US Government Accountability Office in their 2014 report, which described such currencies as pseudonymous, as the although the users name is not known, other details are published on the blockchain; such as their Bitcoin address, the time of the transaction, and the amount: United States Government Accountability Office, 'Virtual Currencies: Emerging Regulatory, Enforcement, and Consumer Protection Challenges' <http://gao.gov/assets/670/663678.pdf> accessed 04 September 2019 at p.6.
[121] FinCEN, 'Guidance - FIN-2013-G001 - Issued: March 18, 2013 - Subject: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies' <https://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf> accessed 06 August 2019 at p2.
[122] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2019.

businesses as money service businesses, but this approach fails to address the peculiarities of cryptocurrencies, and that collecting different data may be required. The application of AML to exchanges shows a level of proactivity, but no measures appear to be applied to the Bitcoin blockchain itself, or any other distributed ledgers. The next section of this chapter will identify the relevant authorities addressing money laundering in the US and enforcing the law.

6.6. Authorities

The US adopts a multi-regulator approach to combatting financial crime and money laundering is no different. As identified by Ryder, the various regulatory bodies can be categorised into primary and secondary authorities.[123] Primary authorities are responsible for creating AML policy and legislation, while secondary authorities are tasked with enforcement.[124] The principal secondary authority is the financial intelligence unit (FIU) as this is the authority that reports are submitted to, the FIU of the US is FinCEN.

6.6.1. Primary Authorities

Department of the Treasury (DoT)

The DoT is the finance department of the US, tasked with maintaining the economy, protecting the integrity of the US financial system, and managing the US Government's

[123] cf Ryder (n100) at p.25.
[124] ibid.

resources.[125] The DoT's pursuit of financial crime involves safeguarding the US financial system and targeting national security threats.[126] This is achieved by issuing guidance on combatting money laundering; such as the '*2007 National Money Laundering Strategy*'[127] and '*National Money Laundering Risk Assessment 2015*'.[128] The 2007 Strategy document sets out the AML goals of the DoT, which include, safeguarding the banking system, enhancing transparency, blocking the flow of bulk cash out of the US, and pursuing money laundering both domestically and internationally.[129]

A number of secondary authorities take direction from the DoT, in particular FinCEN, which is the FIU, and the Office of Terrorism and Financial Intelligence, which has a wide range of legal powers through its position within the DoT.[130]

[125] US Department of the Treasury, 'Duties & Functions of the U.S. Department of the Treasury' <https://home.treasury.gov/about/general-information/role-of-the-treasury> accessed 20 October 2019.
[126] ibid.
[127] US Department of Justice, '2007 National Money Laundering Strategy' <http://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/nmls.pdf> accessed 20 October 2019.
[128] US Department of the Treasury, 'National Money Laundering Risk Assessment 2015' <http://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf> accessed 20 October 2019.
[129] US Department of Justice, '2007 National Money Laundering Strategy' <http://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/nmls.pdf> accessed 20 October 2019 at page i.
[130] US Department of the Treasury, 'Resource Centre – Money Laundering' <https://home.treasury.gov/policy-issues/terrorism-and-illicit-finance/money-laundering> accessed 16 October 2019.

Department of Justice

The Department of Justice (DoJ) undertakes investigations into instances of money laundering,[131] it is the principal government entity responsible for prosecutions at the federal level,[132] and it fulfils its duties through its 40 departments.[133] The most relevant departments of the DoJ are secondary authorities, which pursue money laundering; namely the Federal Bureau of Investigation (FBI) and the Drug Enforcement Agency (DEA). While the DoJ is a primary authority it may also take enforcement actions itself, in this role the DoJ can bring prosecution cases and impose sanctions.[134]

Department of State

The Department of State (DoS) is primarily concerned with international cooperation in combatting money laundering;[135] in this role it will liaise with the DoT and DoJ, as well as the governments and authorities of other jurisdictions to improve international money laundering standards. The DoS operates in a similar way to the DoT and DoJ in that is has many departments, offices and bureaus, which may be tasked with the various roles that the department fulfils. The Bureau of International Narcotics and Law

---

[131] cf Ryder (n100).
[132] Financial Action Task Force, 'Third Mutual Evaluation Report on Anti-Money Laundering and Combatting the Financing of Terrorism: United States of America' <http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20US%20full.pdf> accessed 03 September 2019.
[133] US Department of Justice, 'Agencies' <http://www.justice.gov/agencies/chart#OAG> accessed 03 December 2018.
[134] Examples of enforcement actions can be seen in DoJ press releases: Department of Justice, 'Justice News' <https://www.justice.gov/news> accessed 29 August 2019. One example involved breaches of sanctions against Iran: Department of Justice, 'Iranian Businessman Pleads Guilty to Conspiracy to Violate U.S. Sanctions by Exporting Carbon Fiber From the United States to Iran' (New York, 29 August 2019) <https://www.justice.gov/opa/pr/iranian-businessman-pleads-guilty-conspiracy-violate-us-sanctions-exporting-carbon-fiber> accessed 29 August 2019.
[135] The Department of State is the department of the Secretary of State whom "Under the Constitution, the President of the United States determines U.S. foreign policy. The Secretary of State, appointed by the President with the advice and consent of the Senate, is the President's chief foreign affairs adviser. The Secretary carries out the President's foreign policies through the State Department and the Foreign Service of the United States": US Department of State, 'Duties of the Secretary of State' <http://www.state.gov/secretary/115194.htm> accessed 18 October 2019.

Enforcement Affairs is once such office and every year *"U.S. officials from agencies with AML responsibilities assess the money laundering situations in approximately 200 jurisdictions*."[136]

6.6.2. Secondary Authorities

As stated above, the US adopts a multi-regulator approach, this is most prevalent in its secondary authorities, within the Office of Terrorism and Financial Intelligence alone there are 9 other organisations listed within its organisational chart. The sheer volume of authorities makes it impractical to list them all in this chapter, therefore only the most relevant authorities will be outlined here. The focus of this section is on the principal secondary authorities addressing money laundering, namely the Office of Terrorism and Financial Intelligence, FinCEN and the Securities Exchange Commission.

Office of Terrorism and Financial Intelligence

The Office of Terrorism and Financial Intelligence (TFI) is an office within the DoT; as the name suggest the TFI combats both terrorist financing and financial crime. The focus of this thesis is money laundering, which, as argued in chapter four, is distinct from terrorist financing and should be treated as such.[137] In the TFI's AML role it "*develops and implements the National Money Laundering Strategy as well as other*

[136] US Department of State, '2015 INCSR: Money Laundering/Financial Crimes Countries' <https://2009-2017.state.gov/j/inl/rls/nrcrpt/2014/vol2/222471.htm> accessed 23 October 2019.
[137] See chapter four at 4.10.

policies and programs to fight financial crimes."[138] The TFI has a very wide capacity, covering intelligence across the financial system relating "*combating rogue nations, terrorist facilitators, weapons of mass destruction (WMD) proliferators, money launderers, drug kingpins, and other national security threats*."[139]

Figure 9. Organisation of the TFI[140]

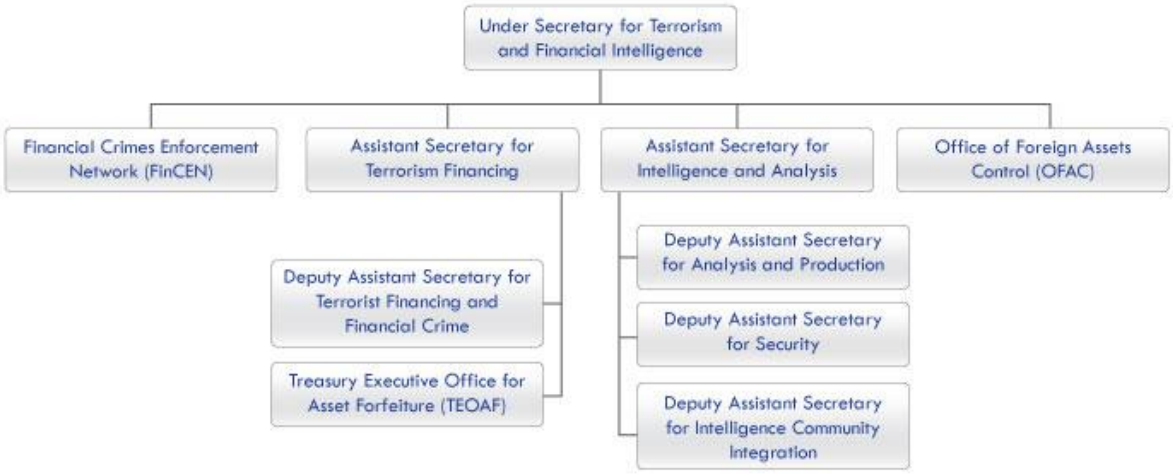


Figure 9 shows the hierarchy of the authorities under the TFI. Each of the 4 offices is accountable to the TFI and a clear division of priorities can be seen. The most relevant division of the TFI for the purposes of AML is FinCEN as it is the FIU of the US and responsible for implementing the BSA 1970.[141]

[138] US Department of the Treasury, 'About>Terrorism and Financial Intelligence' <http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Terrorism-and-Financial-Intelligence.aspx> accessed 16 October 2019.
[139] ibid.
[140] Image taken from: Department of the Treasury, 'Organizational Structure » Offices » Terrorism and Financial Intelligence' <https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Terrorism-and-Financial-Intelligence.aspx> accessed 30 August 2019.
[141] FinCEN, 'What We Do' <http://fin-cenus.com/what-we-do.html> accessed 03 October 2019.

Financial Crime Enforcement Network (FinCEN)

FinCEN aims to "*safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities.*"[142] It is the FIU of the US, as identified by the FATF.[143] FinCEN is responsible for enforcing the BSA 1970.[144] FinCEN is accountable to the DoT, and FinCEN's director reports to the Under Secretary of the Office of Terrorism and Financial Intelligence. FinCEN works in cooperation with the IRS,[145] which is indicative of the interconnectedness of US regulatory authorities. As the FIU, FinCEN is the recipient of both SARs and CTRs, and is responsible for deciding whether to take such reports further. As a secondary authority FinCEN is also responsible for enforcing compliance of AML regulations.[146] FinCEN's money laundering enforcement actions should be distinguished from broader money laundering prosecutions, as FinCEN will sanction regulated institutions for non-compliance rather than that the institution itself has committed money laundering.

[142] ibid.
[143] Financial Action Task Force, 'Third Mutual Evalulation Report on Anti-Money Laundering and Combatting the Financing of Terrorism: United States of America' <http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20US%20full.pdf> accessed 28 October 2019.
[144] FinCEN, 'What We Do' <http://fin-cenus.com/what-we-do.html> accessed 03 October 2019.
[145] Financial Action Task Force, 'Third Mutual Evalulation Report on Anti-Money Laundering and Combatting the Financing of Terrorism: United States of America' <http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20US%20full.pdf> accessed 28 October 2019 at p.16.
[146] FinCEN, 'Law Enforcement Overview' <https://www.fincen.gov/resources/law-enforcement-overview> accessed 30 August 2019.

Securities Exchange Commission (SEC)

The SEC is an independent industry regulator, created by the Securities Exchange Act 1934,[147] in the wake of the Great Crash of 1929. Due to the nature of its capacity as a regulator, the SEC, like FinCEN, is primarily concerned with ensuring regulated firms comply with AML measures, rather than convictions for money laundering offences. The SEC sets out its mission as being "*to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation*."[148] The SEC issues guidance on AML regulations[149] and contributes to debates on money laundering issues.[150]

Each of the authorities identified has a role in implementing the US AML regime. The DoJ and the many state and district Attorney Generals' offices are concerned with obtaining money laundering convictions, and they have utilised the existing law to obtain convictions for money laundering involving cryptocurrencies. The preventative measures are implemented by a number of authorities, but the focus of this chapter will be on FinCEN as the FIU of the USA, and the agency which is responsible for supervising money services business.[151] The next section analyses the AML regulation of cryptocurrencies, it is noted that there has been a widening of the regulatory perimeter to include cryptocurrencies, and that FinCEN has instigated this

[147] Securities Exchange Act 1934, Sec.4.
[148] US Securities Exchange Commission, 'About the SEC' <http://www.sec.gov/about/whatwedo.shtml> accessed 28 October 2019.
[149] US Securities Exchange Commission, 'Spotlight on Anti-Money laundering Rulemaking' <https://www.sec.gov/spotlight/moneylaundering.htm> accessed 27 October 2019.
[150] US Securities Exchange Commission, 'SPEECH - Anti-Money Laundering: An Often-Overlooked Cornerstone of Effective Compliance' <http://www.sec.gov/news/speech/anti-money-laundering-an-often-overlooked-cornerstone.html> accessed 27 October 2019.
[151] FinCEN, 'Reporting Suspicious Activity – A Quick Reference Guide for Money Services Businesses' <https://www.fincen.gov/statutes_regs/guidance/pdf/msbsar_quickrefguide.pdf> accessed 27 October 2019.

expansion, therefore the US has adopted a regulator led widening of the regulatory perimeter.

6.7. AML Regulation of Cryptocurrencies

In May 2014 the Government Accountability Office (GAO) published a report,[152] which assessed the risks posed by virtual currencies. This report identified the federal agencies that may be affected by the continued development of cryptocurrencies. The GAO only considered the implications of convertible virtual currencies as these currencies "*interact with the real economy because depository institutions (for example, banks and credit unions) may have business relationships with companies that exchange virtual currencies for government-issued currencies.*"[153] To this end the GAO identified FinCEN, prudential banking regulators, the Consumer Financial Protection Bureau, the SEC, the CFTC, and the Department of Homeland Security and Justice as having potential responsibilities for regulating virtual currencies. The GAO report was not solely concerned with money laundering risks, this section will focus on the relevant identified authorities which have responsibilities for tackling money laundering.

[152] United States Government Accountability Office, 'Virtual Currencies: Emerging Regulatory, Enforcement, and Consumer Protection Challenges' <http://gao.gov/assets/670/663678.pdf> accessed 04 September 2019.
[153] ibid at p.5.

6.7.1. FinCEN

The GAO identified FinCEN as the agency with the biggest relationship with cryptocurrencies, due to its role as the chief implementing agency of the BSA 1970.[154] In this capacity, where entities engage in "*virtual currency transactions with U.S. customers or become customers of a U.S. financial institution*"[155] FinCEN is responsible for ensuring that such entities comply with AML regulations.[156] FinCEN has identified cryptocurrency exchanges as money services businesses[157] and takes responsibility for regulating such exchanges, ensuring they have adequate AML procedures.[158] FinCEN only regulates convertible virtual currencies, which have value in real currency or may act as a substitute for real currency,[159] as a result FinCEN's regulatory remit includes cryptocurrencies, as defined in chapter three.[160] FinCEN has issued enforcement actions against cryptocurrency businesses which it considered to be money services business, these actions were against Ripple Labs,[161] BTC-e and

[154] 31 CFR §1010.810(a).
[155] United States Government Accountability Office, 'Virtual Currencies: Emerging Regulatory, Enforcement, and Consumer Protection Challenges' <http://gao.gov/assets/670/663678.pdf> accessed 04 September 2019 at p.12.
[156] 31 CFR §1010.810(a) and United States Government Accountability Office, 'Virtual Currencies: Emerging Regulatory, Enforcement, and Consumer Protection Challenges' <http://gao.gov/assets/670/663678.pdf> accessed 04 September 2019 at p.12.
[157] FinCEN, 'Guidance - FIN-2013-G001 - Issued: March 18, 2013 - Subject: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies' <https://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf> accessed 06 August 2019 at p2.
[158] ibid at p1.
[159] United States Government Accountability Office, 'Virtual Currencies: Emerging Regulatory, Enforcement, and Consumer Protection Challenges' <http://gao.gov/assets/670/663678.pdf> accessed 04 September 2019 at p.13.
[160] See chapter three at 3.7.
[161] FinCEN, 'FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger' (Washington, 5 May 2015) <https://www.fincen.gov/sites/default/files/enforcement_action/2016-08-02/20150505.pdf> accessed 02 September 2019.

Alexander Vinnik,[162] and Eric Powers.[163] The first FinCEN enforcement action against a cryptocurrency exchange business was in 2015, when Ripple Labs Inc were required to pay $700,000 for breaching BSA 1970 requirements.[164] Ripple Labs were found to have acted as a money services business and traded a virtual currency without registering with FinCEN.[165] The case came two years after FinCEN had stated it would regulate cryptocurrency exchanges, and in addition to receiving a financial penalty, Ripple Labs agreed to "*conduct a three-year "look-back" to* [review] *suspicious activity reporting for prior suspicious transactions.*"[166] The 'look-back' demonstrates the commitment of FinCEN to ensuring AML regulations are adhered to, and that as the FIU, any potentially intelligence is still gathered. A contrasting enforcement action can be seen in July 2017, when a penalty of $110,003,314 was imposed on BTC-e, and a penalty of $12,000,000 was imposed on Alexander Vinnik, the operator of the exchange.[167] In this case the fines imposed were much larger, as the value of cryptocurrency being transferred was larger than in the Ripple Labs case; BTC-e transferred over $296,000,000 in Bitcoin transactions,[168] as well as a considerable

[162] FinCEN, 'In the Matter of BTC-E a/k/a Canton Business Corporation and Alexander Vinnik' (Vienna, United States, 07 June) <2017https://www.fincen.gov/sites/default/files/enforcement_action/2017-07-27/Assessment%20for%20BTCeVinnik%20FINAL2.pdf> accessed 02 September 2019.
[163] FinCEN, 'In the Matter of Eric Powers' (Vienna, United States, 18 April 2019) https://www.fincen.gov/sites/default/files/enforcement_action/2019-04-18/Assessment%20Eric%20Powers%20Final%20for%20Posting%2004.18.19_1.pdf> accessed 02 September 2019.
[164] FinCEN, 'FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger' (Washington, 5 May 2015) <https://www.fincen.gov/sites/default/files/enforcement_action/2016-08-02/20150505.pdf> accessed 02 September 2019 at p1.
[165] ibid at p1.
[166] ibid at p2.
[167] FinCEN, 'In the Matter of BTC-E a/k/a Canton Business Corporation and Alexander Vinnik' (Vienna, United States, 07 June) <2017https://www.fincen.gov/sites/default/files/enforcement_action/2017-07-27/Assessment%20for%20BTCeVinnik%20FINAL2.pdf> accessed 02 September 2019 at p.9.
[168] ibid at p.2.

value in transactions in other cryptocurrencies.[169] The value of the transactions was not the only aggravating factor, BTC-e handled over 300,000 Bitcoins which were stolen in the from the hacking of Mt. Gox exchange[170] in which 744,408 Bitcoins were stolen,[171] and while Ripple Labs agreed to a 'look-back', no such agreement appears in the BTC-e enforcement notice. The BTC-e and Vinnik case demonstrates that the punishments for not complying with FinCEN regulation can be severe, and financial penalties will increase if criminal activity is also discovered. The most recent FinCEN enforcement action against a cryptocurrency exchange is the $35,350 fine imposed on Eric Powers.[172] The sanction imposed on Powers was for breaches of the BSA 1970, as was the case for Ripple Labs and the BTC-e and Vinnik cases, but the value of the transactions completed by Powers were much lower. Powers failed to "*(a) register as an MSB with FinCEN; (b) establish and implement an effective written anti-money laundering (AML) program; (c) detect and adequately report suspicious transactions; and (d) report currency transactions*."[173] While the list of charges are similar to previous enforcement action by FinCEN, Powers conducted over 1,700 transactions,[174] and his most prevalent suspicious customer's transactions equated to $86,000.[175] Powers was not directly implicated in any known crimes, which contrasts with BTC-e and Vinnik where the Mt. Gox connection existed.

[169] ibid.
[170] ibid at p.6.
[171] BBC News, 'Top Bitcoin exchange MtGox goes offline' <https://www.bbc.co.uk/news/technology-26333661> accessed 02 September 2019.
[172] FinCEN, 'In the Matter of Eric Powers' (Vienna, United States, 18 April 2019) https://www.fincen.gov/sites/default/files/enforcement_action/2019-04-18/Assessment%20Eric%20Powers%20Final%20for%20Posting%2004.18.19_1.pdf> accessed 02 September 2019 at p.7.
[173] FinCEN, 'In the Matter of Eric Powers' (Vienna, United States, 18 April 2019) https://www.fincen.gov/sites/default/files/enforcement_action/2019-04-18/Assessment%20Eric%20Powers%20Final%20for%20Posting%2004.18.19_1.pdf> accessed 02 September 2019 at p.2.
[174] ibid.
[175] ibid at p.5.

From the enforcement actions FinCEN has taken so far, it is appears that a reasonable approach has been taken. Fines are being imposed, and the size of the fines imposed are clearly influenced by mitigating or aggravating factors. Where the values of transferred currency is lower, a lower fine will be imposed, compared to high value cases which received larger sanctions. Additional criminal behaviour will be an aggravating factor, but attempts to retrospectively comply with FinCEN regulation will be considered, as shown by the Ripple Labs case. Deterrence is not mentioned in any of the enforcement notices, but as noted by Ryder,[176] one of FinCEN's objectives is the deterrence of financial crime,[177] therefore a consideration in determining a fine will be deterring others from the same activity. In the UK, the comparable agencies are the NCA as the FIU and the FCA as the principal regulator. The FCA has failed to take the bold approach that FinCEN has taken. The FCA could have interpreted the definition of a 'money services business' in the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017[178] to include cryptocurrency service providers, and thus apply its regulation, but it has not. The UK will adopt a legislator led widening of the regulatory perimeter, in contrast to the much faster regulator led widening demonstrated by FinCEN.

[176] cf Ryder (n100) at p.50.
[177] FinCEN, 'FinCEN's Strategic Plan' <https://www.fincen.gov/about/fincens-strategic-plan> accessed 02 September 2019.
[178] Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, Regulation 10(2)(a).

6.7.2. Securities Exchange Commission

The GAO identified that the SEC will need to regulate "*if a broker-dealer were to accept payments in*"[179] cryptocurrencies and there were money laundering concerns, or if a broker-dealer holds cryptocurrencies either for themselves or on behalf of a customer.[180] The mission of the SEC is "*to protect investors,* [and] *maintain fair, orderly, and efficient markets*;"[181] therefore the SEC will act in cases where virtual currencies are used to commit offences against investors and markets. An example of such action can be seen in *SEC v. Shavers*;[182] which concerned a Ponzi scheme where the victims invested with Bitcoin. As well as bringing prosecutions the SEC also issues alerts and guidance to market participants; two notable alerts were issued in 2014,[183] as well as two other alerts which related to a mining scheme which used a virtual currency called 'Gemcoins'[184] and another warning relating to 'fantasy stocks' which may also use virtual currencies.[185] A further responsibility for the SEC will be to review the registration of companies wishing to offer cryptocurrency related securities, a prominent example being the Gemini Bitcoin exchange, which was recently opened

[179] United States Government Accountability Office, 'Virtual Currencies: Emerging Regulatory, Enforcement, and Consumer Protection Challenges' <http://gao.gov/assets/670/663678.pdf> accessed 04 September 2019 at p.17.
[180] ibid.
[181] US Securities Exchange Commission, 'About the SEC' <http://www.sec.gov/about/whatwedo.shtml> accessed 04 December 2015.
[182] Securities and Exchange Commission v. Trendon T. Shavers and Bitcoin Savings and Trust, Civil Action No. Civil Action No. 4:13-CV-416.
[183] US Securities Exchange Commission, 'Investor Alert: Ponzi Schemes Using Virtual Currencies' <https://www.investor.gov/news-alerts/investor-alerts/investor-alert-ponzi-schemes-using-virtual-currencies> accessed 18 December 2015 and US Securities Exchange Commission, 'Investor Alert: Bitcoin and Other Virtual Currency-Related Investments' <http://www.investor.gov/news-alerts/investor-alerts/investor-alert-bitcoin-other-virtual-currency-related-investments> accessed 18 December 2015.
[184] US Securities Exchange Commission, 'SEC Halts $32 Million Scheme That Promised Riches From Amber Mining' <https://www.investor.gov/news-alerts/press-releases/sec-halts-32-million-scheme-promised-riches-amber-mining> accessed 18 December 2015.
[185] US Securities Exchange Commission, 'Investor Alert: Beware of Fantasy Stock Trading Websites Offering Real Returns' <https://www.investor.gov/news-alerts/investor-alerts/investor-alert-beware-fantasy-stock-trading-websites> accessed 18 December 2015.

in New York and founded by the Winklevoss twins.[186] These examples show that the SEC will address issues involving cryptocurrencies when there is an impact on the areas it has responsibility for, but the SEC is not the principal regulator for AML compliance, which is FinCEN. In the UK it is the responsibility of the FCA to set AML rules for all financial institutions.[187]

6.7.3. Commodities Futures Trading Commission (CFTC)

The GAO found that the responsibilities of the CFTC "*depend partly on whether bitcoin or other virtual currencies meet the definition of a commodity under the Commodity Exchange Act.*"[188] In 2015 the CFTC submitted their position to the GAO, "*CFTC officials said the agency would not make a formal determination* [on whether their enforcement of the BSA 1970 included virtual currencies] *until market circumstances require one.*"[189] Since 2017 the CFTC has issued a number of advisory notices on the issue of cryptocurrencies,[190] which has focussed on increasing the awareness of investors to the risks of fraud in cryptocurrency investments. The focus of the CFTC

[186] Gemini, 'What is Gemini?' <https://gemini24.zendesk.com/hc/en-us/articles/204732945-What-is-Gemini-> accessed 18 December 2015.
[187] Money Laundering Regulations 2017, reg.7(a)
[188] As defined in 7 U.S. Code § 1a(9): "The term "commodity" means wheat, cotton, rice, corn, oats, barley, rye, flaxseed, grain sorghums, mill feeds, butter, eggs, Solanum tuberosum (Irish potatoes), wool, wool tops, fats and oils (including lard, tallow, cottonseed oil, peanut oil, soybean oil, and all other fats and oils), cottonseed meal, cottonseed, peanuts, soybeans, soybean meal, livestock, livestock products, and frozen concentrated orange juice, and all other goods and articles, except onions (as provided by section 13–1 of this title) and motion picture box office receipts (or any index, measure, value, or data related to such receipts), and all services, rights, and interests (except motion picture box office receipts, or any index, measure, value or data related to such receipts) in which contracts for future delivery are presently or in the future dealt in." United States Government Accountability Office, 'Virtual Currencies: Emerging Regulatory, Enforcement, and Consumer Protection Challenges' <http://gao.gov/assets/670/663678.pdf> accessed 04 September 2019 at p.18.
[189] United States Government Accountability Office, 'Virtual Currencies: Emerging Regulatory, Enforcement, and Consumer Protection Challenges' <http://gao.gov/assets/670/663678.pdf> accessed 04 September 2019 at p.18.
[190] Available at: CFTC, 'Learn and Protect > Bitcoin > Bitcoin and Other Virtual Currencies' <https://www.cftc.gov/Bitcoin/index.htm> accessed 03 September 2019.

is on "*open, transparent, competitive, and financially sound markets,*"[191] therefore its focus is not primarily to address money laundering. The aims of the CFTC are to "*protect market users and their funds, consumers, and the public from fraud, manipulation, and abusive practices related to derivatives and other products*"[192] which means their enforcement actions will relate to those issues. Recent enforcement actions by the CFTC concern failure to supervise employees,[193] unauthorised trading,[194] false claims of certification,[195] and other instances of fraud.[196] Where the CFTC has acted against cryptocurrency related businesses, it has been for fraudulent activity in conjunction with cryptocurrencies, rather than money laundering, as demonstrated by the recent action against Diamonds Trading Investment House and First Options Trading,[197] where the defendants impersonated a CFTC officer and sent forged documents purportedly from the CFTC.[198] As identified by the GAO the CFTC will act in relation to the trading of commodities, and federal courts have ruled that cryptocurrencies can be commodities, such as in *CFTC* v *Patrick McDonnell and*

[191] CFTC, 'Mission and Responsibilities' <https://www.cftc.gov/About/MissionResponsibilities/index.htm> accessed 03 September 2019.
[192] ibid.
[193] CFTC, 'CFTC Orders Vision Financial Markets LLC to Pay a $200,000 Penalty to Settle Charges that It Failed to Supervise Its Employees' (Washington, United States, 12 July 2019) <https://www.cftc.gov/PressRoom/PressReleases/7973-19> accessed 03 September 2019.
[194] CFTC, 'CFTC Orders Dean Katzelis and Shahin Maleki d/b/a Essex Futures to Pay a $500,000 Penalty to Settle Charges of Unauthorized Options Trading, Failure to Supervise, and Other Violations' (Washington, United States, 12 July 2019) <https://www.cftc.gov/PressRoom/PressReleases/7972-19> accessed 03 September 2019.
[195] CFTC, 'CFTC Issues Order Finding that Korea Exchange, Inc. Made a False and Misleading Certification to the CFTC' (Washington, United States, 12 July 2019) <https://www.cftc.gov/PressRoom/PressReleases/7971-19> accessed 03 September 2019.
[196] CFTC, 'Commodity Pool and its President Ordered to Pay $1.2 Million, Banned from Markets for Futures Fraud' (Washington, United States, 12 July 2019) <https://www.cftc.gov/PressRoom/PressReleases/7948-19> accessed 03 September 2019.
[197] CFTC, 'Federal Court Permanently Enjoins Defendants and Orders Them to Pay Penalties and Restitution for Bitcoin Solicitation Fraud, Impersonating a CFTC Investigator, and Sending Forged CFTC Documents' (Washington, United States, 10 July 2019) <https://www.cftc.gov/PressRoom/PressReleases/7965-19> accessed 03 September 2019.
[198] ibid.

others,[199] but the CFTC have not acted in money laundering cases, this remains the responsibility of FinCEN. The CFTC issues AML guidance to the institutions it regulates, but this guidance takes its lead from the guidance of FinCEN.[200] In the UK, the FCA would still be the equivalent regulator, but has resisted applying regulation, it is the designated regulator of cryptocurrency services providers since January 2020.[201]

6.7.4. Department of Homeland Security and Justice

As with fiat currencies, cryptocurrencies can be used to commit crime in a number of ways, therefore law enforcement agencies may have to deal with cases involving cryptocurrencies. The DoJ advised the GAO that there are two areas of interest for such agencies. Firstly, where cryptocurrencies have been used to launder money and a prosecution is sought against and individual,[202] and secondly where cryptocurrency businesses have committed money laundering offences.[203] Based on this approach it would appear that these law enforcement agencies will continue in much the same way as they have in the past, their involvement with cryptocurrencies will naturally occur when crimes involve cryptocurrencies. Examples of money laundering convictions which involve cryptocurrencies can be found through press releases by

[199] Commodity Futures Trading Commission v. Patrick K. McDonnell, and Cabbagetech, Corp. D/B/A Coin Drop Markets, Case No 1: 18-CV-361 (E.D.N.Y. Mar. 6, 2018).
[200] CFTC, 'Anti-Money Laundering' <https://www.cftc.gov/IndustryOversight/AntiMoneyLaundering/index.htm> accessed 03 September 2019.
[201] HM Government 'Economic Crime Plan' (12 July 2019) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/816215/2019-22_Economic_Crime_Plan.pdf> accessed 23 October 2019 at 4.9.
[202] United States Government Accountability Office, 'Virtual Currencies: Emerging Regulatory, Enforcement, and Consumer Protection Challenges' <http://gao.gov/assets/670/663678.pdf> accessed 04 September 2019 at p.19.
[203] ibid.

the DoJ; the search terms 'Bitcoin money laundering' returns over 270 results.[204] Example cases vary in complexity and value, just as all criminal cases will, from an international gang being investigated for 18 months,[205] to a one-man operation of a much smaller scale.[206] The prosecutions for money laundering using cryptocurrencies demonstrate that the offences do not need reform to as cryptocurrency transactions clearly satisfy the widely drafted criminal offences within Title 18 of the United States Code.[207] As identified in chapter five,[208] UK law enforcement agencies have also obtained prosecutions for money laundering using cryptocurrencies,[209] demonstrating that the criminal offences are applicable to cryptocurrencies.

6.7.5. Perceived Threats of Cryptocurrencies and Gaps in Regulation

Aside from the applicability of the law to cryptocurrencies, there are a number of more general concerns that the GAO has raised over the use of cryptocurrencies. These

[204] Department of Justice, 'Search: Query= bitcoin + money + laundering' <https://search.justice.gov/search?utf8=%E2%9C%93&affiliate=justice&sort_by=&query=bitcoin+money+laundering> accessed 19 October 2019.
[205] Department of Justice, U.S. Attorney's Office Western District of Washington, 'Multi-State International Drug Trafficking Organization Targeted in 18-Month Investigation' (Washington, United States, 6 December 2018) <https://www.justice.gov/usao-wdwa/pr/multi-state-international-drug-trafficking-organization-targeted-18-month-investigation> accessed 04 September 2019.
[206] Department of Justice, U.S. Attorney's Office Central District of California, '"Bitcoin Maven" Sentenced to One Year in Federal Prison in Bitcoin Money Laundering Case' <https://www.justice.gov/usao-cdca/pr/bitcoin-maven-sentenced-one-year-federal-prison-bitcoin-money-laundering-case> accessed 04 September 2019.
[207] 18 USC §1956-57.
[208] See chapter five and 5.3.1.
[209] *R* v *Teresko* [2018] Crim LR 81, Crown Prosecution Service, 'More than £1.2million of Bitcoin seized from drug dealer' (19 July 2018) <https://www.cps.gov.uk/south-east/news/more-ps12-million-bitcoin-seized-drug-dealer> accessed 11 September 2019 and BBC News, 'Liverpool 'dropout' jailed for Silk Road dark web site' (12 April 2019) <https://www.bbc.co.uk/news/uk-england-merseyside-47913780> accessed 11 September 2019 and National Crime Agency, 'Student behind $100m dark web site jailed for 5 years 4 months' (12 April 2019) <https://www.nationalcrimeagency.gov.uk/news/student-behind-100m-dark-web-site-jailed-for-5-years-4-months?highlight=WyJiaXRjb2luIiwiYml0Y29pbnMiXQ==> accessed 11 September 2019.

threats include volatility,[210] anonymity,[211] lack of bank involvement,[212] and the international nature of cryptocurrencies.[213] The issue of volatility is in relation to the value of the cryptocurrencies, against fiat currency. This issue is addressed in chapter three where cryptocurrencies are compared to fiat currencies and traditional money; the volatile value may be seen a bar against cryptocurrencies being considered money.

The increased anonymity of cryptocurrencies is clearly a concern from an anti-money laundering perspective; if the parties to a transaction cannot be identified then any reporting of that transaction is of minimal use. The anonymity attached to cryptocurrencies is addressed by the GAO in their 2014 report, which described such currencies as pseudonymous,[214] as although the users name is not known, other details are published on the blockchain;[215] such as their Bitcoin address, the time of the transaction, and the amount. Furthermore, the GAO claim that data analysis techniques may reveal the identity of a user, and that investigators may obtain identifying information through exchanges of Bitcoin for Dollars or vice versa. Finally the report points to research by Meiklejohn *et al*,[216] who "*we were able to identify 1.9 million public keys with some real-world service or identity,*"[217] however, Meiklejohn *et al* found "*in many cases the identity was not a real name, but rather (for example) a*

[210] United States Government Accountability Office, 'Virtual Currencies: Emerging Regulatory, Enforcement, and Consumer Protection Challenges' <http://gao.gov/assets/670/663678.pdf> accessed 04 September 2019 at p.22.
[211] ibid at p.20.
[212] ibid at p.22.
[213] ibid.
[214] ibid at p.6.
[215] The public ledger of Bitcoin. See chapter three for explanation of the blockchain.
[216] Sarah Meiklejohn, et al, "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names," (2013) 38(6) ;Login: 10.
[217] ibid at p.14.

username on a forum."[218] The anonymity of cryptocurrencies may be eroded by the aforementioned techniques, but the fact such extra measures need to be taken in order to pursue users of cryptocurrencies will always present an extra level of difficulty, and complexity, to cases involving cryptocurrencies. A further example of investigative techniques being developed to combat cryptocurrency anonymity is demonstrated by Juhász *et al* who identified 22,363 users 1,797 associated IP addresses.[219] Juhász *et al* argue their "*method is cheap in terms of resources,*"[220] and their "*algorithms are relatively easy to implement and can be combined with other Bitcoin-transaction related information.*"[221] The research of Meiklejohn *et al* and Juhász *et al* demonstrates that investigative tools can be developed to combat the anonymity of cryptocurrencies.

The lack of bank involvement is identified as an issue as there will be a far reduced level of protection to the users of cryptocurrencies, compared to those using fiat currencies and traditional financial institutions. The inclusion of cryptocurrency exchanges in the regulatory regime will go some way to protect consumers, but the decentralised nature of some cryptocurrencies means there is no central organisation acting as an administrator for the currency, so there is no way to insure the holdings of consumers in the way that the Federal Deposit Insurance Corporation operates for banks.

[218] ibid.
[219] P. L. Juhász, J. Stéger, D. Kondor and G. Vattay, 'A Bayesian approach to identify Bitcoin users' (2018) 13(12) PLoS ONE 1 at p.13.
[220] ibid at p.18.
[221] ibid.

Lastly the international nature of virtual currencies will always be a concern for individual jurisdictions; virtual currencies are either operated by private companies, or in the case of cryptocurrencies, operated by algorithms. Cryptocurrencies do not recognise borders, so it is difficult for one jurisdiction to regulate. The GAO report accepts that regulations imposed by the US will mean "*federal financial regulatory and law enforcement agencies face challenges in enforcing these requirements and investigating and prosecuting transnational crimes that may involve virtual currencies.*"[222] The GAO encourage co-operation with international counterparts but fears that some individuals may choose to "*operate out of countries that have weak legal and regulatory regimes or that are less willing to cooperate with U.S. law enforcement*

At the present time there are no specific reforms planned for the US AML approach, or for the treatment of cryptocurrencies. The current practice of each agency releasing its own guidance looks set to continue, though the GAO have recommended that potential consumer protection should addressed through the Consumer Financial Protection Bureau and that interagency assistance should be given.[223]

6.8. Compliance with Financial Action Task Force guidance

The most recent FATF mutual evaluation report of the USA, in 2016, predates the 2019 FATF guidance on virtual assets, and given how recently the FATF guidance

[222] United States Government Accountability Office, 'Virtual Currencies: Emerging Regulatory, Enforcement, and Consumer Protection Challenges' <http://gao.gov/assets/670/663678.pdf> accessed 04 September 2019 at p.22.
[223] ibid at p.40.

has been released, it is not reasonable to expect full compliance. However, as identified in chapter four,[224] the US has frequently implemented AML measures before they become international standards. Therefore, it is reasonable to assess the level to which the US is already compliant with the FATF guidance. The terminology used by FATF differs to that if the US. The FATF use the term 'virtual asset' (VA), which is defined as a "*digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes.*"[225] The agencies of the US predominantly use the term virtual currencies,[226] but the use of this term is the equivalent of the FATF term 'virtual asset'. The FATF guidance also uses the term 'Virtual Asset Service Provider' (VASP)[227] to describe businesses providing services for cryptocurrency users. The approach of FinCEN has been to recognise cryptocurrency businesses as 'money services businesses.[228] The use of different term by the FATF and the US is immaterial, as the definitions of the terms are similar, and the US definitions will be compliant with the FATF guidance. The FATF guidance addresses the majority of the 40 Recommendations, stating that "[a]*lmost all of the*

[224] See chapter four at 4.7.
[225] Financial Action Task Force, 'Guidance for A Risk-Based Approach to Virtual Currencies' <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf> accessed 01 August 2016, para 33 at p13.
[226] As demonstrated throughout the GAO report on in 2014: United States Government Accountability Office, 'Virtual Currencies: Emerging Regulatory, Enforcement, and Consumer Protection Challenges' <http://gao.gov/assets/670/663678.pdf> accessed 04 September 2019. The term is also used by FinCEN: FinCEN, 'Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies' (9 May 2019) <https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf> accessed 04 September 2019. The CFTC refer to Bitcoin directly, but also use the term: CFTC, 'Bitcoin and Other Virtual Currencies' https://www.cftc.gov/Bitcoin/index.htm> accessed 04 September 2019.
[227] Financial Action Task Force, 'Guidance for A Risk-Based Approach to Virtual Currencies' <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf> accessed 01 August 2016, Acronyms at p3.
[228] FinCEN, 'Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies' <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf> accessed 04 September 2019.

FATF Recommendations are directly relevant"[229] to addressing the money laundering risks posed.

Recommendation 1 requires countries to undertake a risk assessment and apply the risk-based approach,[230] which the 2019 guidance states should now include VAs and VASPs. As identified by the GAO report, and the recognition of cryptocurrencies by FinCEN, the US is clearly assessing the risks posed, including those relating to money laundering. The risk assessment should identify the relevant authorities that should regulate VAs and VASPs, and the treatment of these products and services should be consistent.[231] The inclusion of cryptocurrency exchanges in FinCEN regulation demonstrates compliance with this, FinCEN is the FIU of the US, and the treatment of VASPs is consistent with other money service businesses.

FATF Recommendations advise that all "*funds or value-based terms in the Recommendations, such as "property," "proceeds," "funds," "funds or other assets," and other "corresponding value,"* [232] should be interpreted to include VAs.[233] The US has not amended its criminal offences to explicitly include VAs, but the existing

[229] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2019 para 55 at p19.
[230] See Recommendation 1 and the relevant explanatory note: Financial Action Task Force, 'The FATF Recommendations' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> accessed 04 September 2019.
[231] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2019 para 58 at p19.
[232] ibid at para 65 at p20.
[233] ibid.

legislation is drafted so widely that the law will apply to VAs. §1956[234] and §1957[235] refer to transactions, which does not preclude cryptocurrency satisfying the offences. The applicability of offences has been proven by the successful money laundering convictions obtained by various DoJ District Attorneys, as discussed at 6.7.4. The example cases vary from an international gang being investigated for 18 months,[236] to smaller scale offences such as one-man operations.[237] The prosecutions for money laundering using cryptocurrencies demonstrate that the offences do not need reform, as cryptocurrency transactions clearly satisfy the widely drafted money laundering offences. The US is clearly compliant with FATF Recommendations 3, 4, and 5 pertaining to the criminalisation of money laundering,[238] confiscation of criminal proceeds,[239] and terrorist financing.[240] The US is also compliant with the guidance on Recommendation 6 which concerns asset freezing,[241] although this is usually impossible for cryptocurrencies, and Recommendation 7 which relates to sanctions,[242] which again would be difficult to enforce in relation to cryptocurrencies.

[234] 18 USC §1956.
[235] 18 USC §1957.
[236] Department of Justice, U.S. Attorney's Office Western District of Washington, 'Multi-State International Drug Trafficking Organization Targeted in 18-Month Investigation' (Washington, United States, 6 December 2018) <https://www.justice.gov/usao-wdwa/pr/multi-state-international-drug-trafficking-organization-targeted-18-month-investigation> accessed 04 September 2019.
[237] Department of Justice, U.S. Attorney's Office Central District of California, '"Bitcoin Maven" Sentenced to One Year in Federal Prison in Bitcoin Money Laundering Case' <https://www.justice.gov/usao-cdca/pr/bitcoin-maven-sentenced-one-year-federal-prison-bitcoin-money-laundering-case> accessed 04 September 2019.
[238] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2019 para 66 at p21.
[239] ibid at para 67 at p21.
[240] ibid at para 69 at p21.
[241] ibid at para 70 at p21.
[242] ibid at para 71 at p21.

As well as ensuring applicable criminalisation of money laundering through cryptocurrencies, the 2019 guidance addresses AML regulation as well. The FATF guidance requires preventative measures to apply to VASPs.[243] In determining that cryptocurrency exchanges are treated as money services businesses,[244] FinCEN has extended the BSA 1970 to cover VASPs in line with the FATF guidance, which satisfies Recommendation 15.[245] FinCEN's remit and regulatory powers satisfy Recommendations 26 and 27, so by FinCEN adopting the regulation of VASPs, it is compliant with 2019 FATF guidance in this respect.[246] FinCEN regulates compliance with BSA 1970 requirements, so, under FinCEN regulation, VASPs are required to complete CDD processes, complying with Recommendation 10 in line with the 2019 guidance.[247] FinCEN provide guidance to money services businesses to aide with compliance, the requirements are condensed into factsheets for quick reference.[248] The factsheets from FinCEN cover the general requirements of a money service business, including having an AML compliance program, record keeping, and submitting CTRs and SARs,[249] specifically when a report is required.[250] As identified at 6.7.1, FinCEN has taken enforcement action against non-compliant VASPs on 3 occasions,[251] demonstrating its commitment to ensuring VASPs adhere to AML

[243] ibid at para 86 at p23.
[244] FinCEN, 'Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies' <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf> accessed 04 September 2019.
[245] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2019 para 91 at p23.
[246] ibid.
[247] ibid.
[248] FinCEN, 'A Quick Reference Guide for Money Services Businesses' (Washington, United States, September 2007) <https://www.fincen.gov/sites/default/files/shared/bsa_quickrefguide.pdf> accessed 04 September 2019.
[249] ibid at p.1.
[250] ibid at p.2.
[251] FinCEN, 'FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger' (Washington, 5 May 2015) <https://www.fincen.gov/sites/default/files/enforcement_action/2016-08-02/20150505.pdf> accessed

regulation. The enforcement actions of FinCEN have included punishments for not registering with FinCEN, a requirement which satisfies FATF expectation that VASPs are required to register with a designated authority.[252]

In summary, the US can be seen to be ahead of international best practice, recognising cryptocurrency businesses in 2013 and applying AML regulation. By applying regulation to cryptocurrency exchanges, the US is already compliant with the FATF guidance of 2019.

6.9. Recommendations for the United Kingdom

Both the UK and the US have money laundering offences which can be committed using cryptocurrencies. The focus of the wording if the offences are different, in the UK offence focuses on the movement of property, and criminal property is defined in wide terms. Criminal property in the UK is anything that "*constitutes a person's benefit from criminal conduct or it represents such a benefit*",[253] which "*the alleged offender knows or suspects*"[254] is such a benefit. The definition recognises that the proceeds of crime is often broken up to avoid detection, as such the criminal property may

02 September 2019, FinCEN, 'In the Matter of BTC-E a/k/a Canton Business Corporation and Alexander Vinnik' (Vienna, United States, 07 June) <2017https://www.fincen.gov/sites/default/files/enforcement_action/2017-07-27/Assessment%20for%20BTCeVinnik%20FINAL2.pdf> accessed 02 September 2019, and FinCEN, 'In the Matter of Eric Powers' (Vienna, United States, 18 April 2019) https://www.fincen.gov/sites/default/files/enforcement_action/2019-04-18/Assessment%20Eric%20Powers%20Final%20for%20Posting%2004.18.19_1.pdf> accessed 02 September 2019.

[252] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2019 para 78 at p22.

[253] Proceeds of Crime Act 2002, Part 7, s.340(3)(a).

[254] ibid s.340(3)(b).

represent a benefit "*in whole or part*"[255] and can be direct or indirect.[256] This wide definition of criminal property can therefore encompass the broad array of assets which may be used to disguise illegal gains. The US offences instead focus on transactions. The UK offences are simpler than in the US where the money laundering offences require a 'specified unlawful activity'[257] to have taken place, as listed in §1956(c)(7).[258] The successful convictions in both the UK and the US demonstrate the offences are applicable to cryptocurrencies, and there are no reasons for the UK to reform the Proceeds of Crime Act 2002[259] to adopt the US money laundering offences.

The UK requires regulated institutions to adhere to similar AML regulation as the US, with the exception of CTRs, the UK does not enforce compulsory reporting and instead focuses on SARs. The differences with regard to cryptocurrency service providers are stark, the UK does not currently impose AML regulation on cryptocurrency service providers, whereas the US does, through FinCEN. The US response to the AML threats posed by cryptocurrencies was implemented soon after cryptocurrencies grew in prominence and was achieved without the need for legislative reform. This was achieved by FinCEN in 2013, when it determined that cryptocurrency exchanges and administrators were too be viewed as money services businesses, and therefore need to comply with AML regulation.[260] A similar approach could be implemented in the UK

[255] ibid s.340(3)(a).
[256] ibid.
[257] 18 USC §1956(a)(1).
[258] 18 USC §1956(c)(7).
[259] Proceeds of Crime Act 2002.
[260] FinCEN, 'Guidance - FIN-2013-G001 - Issued: March 18, 2013 - Subject: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies' <https://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf> accessed 06 August 2019 at p2.

if Regulation 3 of the Money Laundering Regulations[261] were to be interpreted differently. A money services business is an "*an undertaking which by way of business operates a currency exchange office, transmits money (or any representations of monetary value) by any means or cashes cheques which are made payable to customers.*"[262] Were the FCA to take the approach of FinCEN, and determine that cryptocurrency service providers satisfy this definition, then AML regulation could be implemented in a similar way to in the US. The UK sought opinions on the US approach to regulating cryptocurrencies, as part of the 2015 public consultation. Respondents were "positive, reporting that regulation has increased the legitimacy of digital currency firms, helped firms establish banking partnerships and investment, and deterred criminals."[263] Criticisms of the US approach were made in relation to a perceived "*lack of clarity about which categories of business activity are captured by the FinCEN requirements, and some said that the process of registering in multiple American states has been burdensome and has forced smaller firms to exit the market*."[264] The issue of state regulation is not relevant to a UK transposition of the US approach, but lack of clarity regarding what businesses are covered could be problematic. The guidance of the FATF should be followed, by considering the definition of a cryptocurrency service provider as the same as that of the term 'VASP' in the FATF guidance,[265] confusion over regulated businesses should be avoided.

[261] Money Laundering Regulations 2017, Regulation 3.
[262] ibid Regulation 3(1)(d).
[263] GOV.UK, 'Digital currencies: response to the call for information' <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf> accessed 11 October 2019 at p.19.
[264] ibid.
[265] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 September 2019 at para 33(c).

Although compliant with FATF guidance, the US regulation of cryptocurrencies is missing the majority of cryptocurrency transactions, which take place on a peer-to-peer format within individual cryptocurrency networks. The quality of the financial intelligence gained through regulating cryptocurrency service providers should be supported by monitoring the blockchain. Cryptocurrencies offer a level of anonymity, but as argued by the GAO in the US; data analysis techniques may reveal the identity of a user, and investigators may obtain identifying information through exchanges of Bitcoin for Dollars, or vice versa.[266] Traditional AML measures cannot be applied to blockchain transactions, as there is no human involvement, except for the two transacting parties, but a plethora of blockchain APIs are available to enable automated analysis of the blockchain.[267] At present it is not clear if the financial intelligence available through the blockchain is being utilised for AML purposes, but it is a valuable resource that the UK and the US should benefit from.

It is recommended that the UK retains its current money laundering offences as they are as effective as the US offences. The FCA should consider widening its interpretation of a 'money services business' so as to include cryptocurrency service providers and bring these entities into the regulatory perimeter of the FCA. It is recommended that the UK go further than the US and monitor the blockchains of cryptocurrencies, so as to avoid a significant number of transactions taking place outside of the financial system, with no regulatory scrutiny.

[266] United States Government Accountability Office, 'Virtual Currencies: Emerging Regulatory, Enforcement, and Consumer Protection Challenges' <http://gao.gov/assets/670/663678.pdf> accessed 04 September 2019 at p.6.
[267] Examples can be found at Blockchain Luxembourg, 'Bitcoin Developer APIs' <https://www.blockchain.com/api> accessed 26 September 2019.

6.10. Summary

This chapter establishes that US money laundering offences can be committed using cryptocurrencies, which is confirmed by the successful prosecutions which have been obtained. Money laundering through cryptocurrencies is criminalised in the same way as other forms of money laundering, with no need for the law to be amended, or new offences to be created. The convictions in the US prove that money laundering it taking place using cryptocurrencies, but the exact extent is difficult to determine.

The current position of the US is to try and balance the advantages of cryptocurrencies with the risks posed. There is concern over the lack of bank involvement, the potential volatility of the value of cryptocurrency, and the issues with anonymity. However, there are potential benefits such as reduced costs, faster transactions, increased privacy and the potential to incorporate the blockchain technology as an innovation in ledgering.

With regards to preventative measures, cryptocurrencies are subject to AML regulations in the US. Individual users are not subject to FinCEN regulation, just as individual users of the traditional financial system are not regulated. AML regulation is applied to cryptocurrency businesses, which are deemed to be money services businesses, as outlined by FinCEN,[268] therefore such businesses must adhere to CTR, SAR, and KYC requirements. The approach of the US towards money

[268] FinCEN, 'Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies' <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf> accessed 04 September 2019.

laundering is a risk-based one, as such the size and complexity of a company's AML program must be adequate in relation to the size and nature of the business being operated. If the risks associated with cryptocurrencies rise, then users and exchanges may receive more attention. The application of CTRs to cryptocurrencies is problematic for two reasons, firstly such reports are of limited value in terms of financial intelligence, CTRs just add to the mass of data being collected by FIUs and adding a further source of CTR reports will provide FinCEN with even more reports to process. Secondly, and more specific to cryptocurrencies, is that the volatility of cryptocurrency values will complicate CTR submissions as the $10,000 threshold may be breached one day but not the next. Despite the difficulties it is not unreasonable to apply CTRs to cryptocurrency businesses if they remain vigilant to transaction values compared to the US Dollar. Different problems exist in complying suspicious activity reporting, as regulated entities are likely to adopt a defensive reporting approach to avoid sanctions, which diminishes the quality of the SARs submitted. The implementation of the SARs regime should be aided by complying with KYC protocols, but cryptocurrencies provide users with mechanisms to conceal their identity,[269] so applying KYC requirements to cryptocurrency businesses will be more difficult than for traditional financial institutions. The difficulties in obtaining accurate customer information mean it is more difficult for a cryptocurrency business to determine whether a transaction is suspicious, therefore they may over report to protect themselves from enforcement action from FinCEN, and the resulting financial penalties.

[269] The anonymity attached to cryptocurrencies is addressed by the US Government Accountability Office in their 2014 report, which described such currencies as pseudonymous, as the although the users name is not known, other details are published on the blockchain; such as their Bitcoin address, the time of the transaction, and the amount: United States Government Accountability Office, 'Virtual Currencies: Emerging Regulatory, Enforcement, and Consumer Protection Challenges' <http://gao.gov/assets/670/663678.pdf> accessed 04 September 2019 at p.6.

FinCEN is responsible for implementing AML regulation, and as the FIU, it receives CTRs and SARs. FinCEN has taken a proactive approach to the threat posed by cryptocurrencies, by determining cryptocurrency businesses as money services businesses, this brought some cryptocurrency transactions within the remit of its regulation. In doing so regulated businesses have had to comply with BSA 1970 requirements, and FinCEN has taken enforcement action on non-complicit institutions. The approach of FinCEN is commendable, but it has not utilised the public ledger technology in order to further widen its intelligence gathering ability, by only applying regulation to cryptocurrency businesses. FinCEN still ignores transactions that take place within cryptocurrency networks, as these transactions are peer-to-peer and do not go through regulated institutions. In order to better utilise reports from cryptocurrency businesses, FinCEN needs to analyse the public ledgers of cryptocurrencies. The next chapter will consider the response of Australia to the money laundering threats posed by cryptocurrencies.

Chapter 7. Australia

7.1. Overview

In this chapter, the applicability of Australia's money laundering offences and preventative measures to cryptocurrencies are assessed. Firstly, the money laundering offences are outlined, and it is determined that it is possible to commit these offences using cryptocurrencies. After applying the offences, the preventive measures are then be assessed; Australia's anti-money laundering (AML) regime is analysed, and the AML regulation of cryptocurrency transactions and cryptocurrency service providers is assessed. As part of the assessment of the AML regime, the relevant authorities are also considered, first in terms of their role in the AML regime, and then considering how the relevant authorities are addressing cryptocurrencies. The chapter illustrates that Australia has addressed money laundering in accordance with international best practice, it is compliant with Financial Action Task Force (FATF) guidance, and in line with world leaders such as the United States (US). Australia has adopted a legislator led widening of the AML regulatory perimeter, which is a contrast to the regulator led approach in the US. The recent AML reforms are analysed, particularly the regulation of cryptocurrency service providers and Australia's compliance with the guidance of FATF on applying a risk-based approach to cryptocurrencies.[1] While Australia's reforms are commended, it is also noted that the weaknesses of international guidance are transferred to Australia, and the potential intelligence available through publicly available blockchains is not utilised, as pre-existing AML measures are applied to cryptocurrencies, rather than a tailored

[1] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2019.

approach. The conclusions of this chapter are similar to those of chapter six in relation to the US. It is recommended that the United Kingdom (UK) bring its AML regulation up to the same standard as Australia, but that it then goes further to benefit from the wealth of financial intelligence available on publicly available blockchains.

7.2. AML Approach

The approach to money laundering in Australia is similar to the UK and the US;[2] there are a number of money laundering offences which criminalise the activity, and there are preventative measures centred around know your customer requirements and suspicious activity reports. Australia began addressing money laundering in 1984, within a year of the US.[3] The key differences between the Australian approach and that of the US and UK are the structure of the legislation, and the way in which penalties are formulated. Despite these differences, the applicability of the offences is similar, and Australia is largely compliant with the FATF Recommendations.

7.3. Criminalising Money Laundering

Australia has 19 money laundering offences, contained in subdivisions 400.3-9 of the criminal code;[4] subdivision 400.9 is a single offence, and subdivisions 400.3-8 each contain three offences.[5] This may appear to be a large number of offences, but it is a result of the Criminal Code categorising money laundering offences by the amounts

[2] See chapter six.
[3] N. Ryder, *Money laundering – an endless cycle? A comparative analysis of the anti-money laundering policies in the United States of America, the United Kingdom, Australia and Canada* (Routledge, London, 2012) at 5.1.
[4] Criminal Code Act 1995 Subdivision 400.3-9.
[5] ibid.

of money involved. Money laundering offences in Australia are arranged very differently to the UK and the US. The UK and the US have a small number of offences, and sentencing provisions allow for the appropriate sentence to be imposed, whereas in Australia the same three offences are repeated 6 times to prescribe sentencing guidelines depending on the value of money or property involved. As stated, under each subdivision there are three offences. Taking Subdivision 400.3 as an example, the first relates to the knowledge of the offender; a person is guilty of an offence if they deal with "*money or other property*"[6] and they either believe it to be the "*proceeds of crime*",[7] or intends it to "*become an instrument of crime.*"[8] In this offence the knowledge of the offender is the most important factor; they must *believe* the money, or property, to be the proceeds of crime. The FATF observe that money laundering penalties in Australia are dependant in the level of fault,[9] as such the high level of knowledge required for this offence means it carries the highest penalty. The grading of the offences can be seen when the second and third offences are considered. The second offence requires less knowledge than the first, instead the offender must be "*reckless as to the fact that the money or property is the proceeds of crime.*"[10] The third offence has the lowest knowledge threshold, a person will be guilty if they are "*negligent as to the fact that the money or property is proceeds of crime*"[11] The lower the required level of knowledge required for the offence, the lesser the sentence, as can be seen in Figure 10 below.

[6] Criminal Code Act 1995 Subdivision 400.3 (1)(a).
[7] Criminal Code Act 1995 Subdivision 400.3 (1)(b)(i).
[8] Criminal Code Act 1995 Subdivision 400.3 (1)(b)(ii).
[9] Financial Action Task Force, 'Anti-money laundering and counter-terrorist financing measures - Australia, Fourth Round Mutual Evaluation Report' <https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Report-Australia-2015.pdf> accessed 23 July 2019 at a.3.9.
[10] Criminal Code Act 1995 Division 400.3 (2)(c).
[11] Criminal Code Act 1995 Division 400.3 (3)(c).

With regard to committing money laundering offences using cryptocurrencies, it must be determined whether cryptocurrencies satisfy the definition of either "*money or other property.*"[12] As has already been discussed in this thesis, it is difficult for cryptocurrencies to be defined as money due to their changing value, which restricts their ability to satisfy the unit of account and store of value functions of money.[13] Therefore cryptocurrencies must satisfy the definition of property. The Criminal Code defines property as: "*real or personal property of every description, whether situated in Australia or elsewhere and whether tangible or intangible, and includes an interest in any such real or personal property.*"[14] This definition is very broad and it is difficult to envisage anything failing to satisfy it; cryptocurrencies are intangible and impossible to possess, but the inclusion of "*interest in*"[15] means that anything of value may be included. Once cryptocurrencies are established as "*money or other property*"[16] there are no other limits to money laundering offences being satisfied using cryptocurrencies.

This format, of three offences requiring decreasing levels of knowledge, is mirrored in Subdivisions 400.4-8, as the amounts of involved decreases so do the penalties; the maximum penalties for each offence in each subdivision can be seen in Figure 10 below.

[12] Criminal Code Act 1995 Subdivision 400.3 (1).
[13] Functions of money are discussed in detail in chapter three at 3.5.1.
[14] Criminal Code Act 1995 Subdivision 400.1(1).
[15] ibid.
[16] ibid.

Figure 10. Maximum Penalties for Money Laundering Offences[17]

Subdivision and Value of money or property involved.	Offence 1	Offence 2	Offence 3
400.3 - $1,000,000 or more	25 years or 1500 penalty units, or both	12 years or 720 penalty units, or both	5 years or 300 penalty units, or both
400.4 - $100,000 or more	20 years or 1200 penalty units, or both	10 years or 600 penalty units, or both	4 years or 240 penalty units, or both
400.5 - $50,000 or more	15 years or 900 penalty units, or both	7 years or 420 penalty units, or both	3 years or 180 penalty units, or both
400.6 - $10,000 or more	10 years or 600 penalty units, or both	5 years or 300 penalty units, or both	2 years or 120 penalty units, or both
400.7 - $1,000 or more	5 years or 300 penalty units, or both	2 years or 120 penalty units, or both	12 months or 60 penalty units, or both
400.8 - any value	12 months or 60 penalty units, or both	6 months or 30 penalty units, or both	10 penalty units

[17] Compiled using Criminal Code Act 1995 Subdivision 400.3-8.

The severity of the punishment depends on the level of knowledge and the value of the assets involved; the maximum prison sentence decreases by five years per Subdivision down the scale, or 300 penalty units. In each Subdivision offence 1 is the most serious, offence 2 is less serious and punishable with half the severity of offence 1, and lastly offence three is the least severe and punishable to 20% of the offence 1 maximum. There is a further money laundering offence at 400.9 which has no knowledge threshold for the offender, instead this offence is committed if "*it is reasonable to suspect that the money or property is proceeds of crime*."[18] If a person deals with property of "*$100,000 or more*"[19] and is convicted, then they may be sentenced to three years imprisonment, or 180 penalty units, or both. If the property is worth less than £100,000 then the punishment is two years imprisonment, or 120 penalty units, or both.[20] If charged with an offence under 400.9, the burden of proof is reversed, it is for the defendant to prove that they had "*no reasonable grounds for suspecting that the money or property was derived or realised, directly or indirectly, from some form of unlawful activity.*"[21]

Penalty units are used by the majority of territories in Australia as a method of issuing fines, with the exception of South Australia. Under the penalty unit system, a fine is calculated by multiplying the value of 1 penalty unit by the number of units imposed; this allows fines to be gradually increased in line with inflation. This was implemented following the recommendation of Review of Commonwealth Criminal Law 1991, which found that "*the erosion of the value of money sooner or later causes the amount*

[18] Criminal Code Act 1995 Subdivision 400.9(1)(b).
[19] Criminal Code Act 1995 Subdivision 400.9(1)(c).
[20] Criminal Code Act 1995 Subdivision 400.9(1A)(c).
[21] Criminal Code Act 1995 Subdivision 400.9(5).

specified [in specific legislation] *to be unrealistic*."[22] Each state, or jurisdiction, may set the value of 1 penalty point, and Figure 11 sets out the value of 1 penalty unit in each jurisdiction:

[22] H. Gibbs, R. Watson and A Menzies, *Review of Commonwealth Criminal Law: Fifth Interim Report* (Commonwealth Attorney-General's Department, 1991).

Figure 11. Value of Penalty Units across Australia[23]

Jurisdiction	Value of 1 Penalty Unit
Australian Capital Territory	$150 (Individual) $750 (Corporation)[24]
Commonwealth[25]	$210[26]
New South Wales	$110[27]
Norther Territory	$155[28]
Queensland	Unless legislation states otherwise: £110 (State Offences) $75 (Local Law Infringements) [29]
South Australia	N/A[30]
Tasmania	$168[31]
Victoria	$ 165.22[32]
Western Australia	Varies depending on the legislation in question.[33]

[23] Correct as of 22 July 2019.
[24] Legislation Act 2001 (ACT), s.133(2).
[25] The Commonwealth jurisdiction is the federal jurisdiction of Australia, it has national effect and the Federal Court has jurisdiction for offences contained in Commonwealth legislation: Federal Court of Australia, The Court's Jurisdiction' <http://www.fedcourt.gov.au/about/jurisdiction> accessed 12 August 2015.
[26] Crimes Act 1914 (Cth), s.4AA(1). This will move to being calculated based on a price index from 1 July 2020: Crimes Act 1914 (Cth), s.4AA(3).
[27] Crimes (Sentencing Procedure) Act 1999 (NSW), s 17.
[28] 2018/2019 value at the top of the table: Northern Territory Government: Department of Attorney General and Justice, 'Penalty Units' <https://nt.gov.au/employ/money-and-taxes/taxes,-royalties-and-grants/territory-revenue-office/penalty-units> accessed 22 July 2019.
[29] Penalties and Sentences Act 1992 (Qld), ss.5-5A.
[30] South Australia does not use the penalty unit system; instead maximum prison sentences have corresponding maximum fines set out in: Acts Interpretation Act 1915 (SA), s.28A.
[31] Penalty units increase yearly based on the formula B x (C□D) where B is $154; C is the value of the CPI figure for Hobart for the December quarter immediately preceding the financial year in which the value of the penalty unit is to apply; and D is the value of the CPI figure for Hobart for the December quarter 2014: Penalty Units and Other Penalties Act 1987 (Tas), s4A(2).
[32] Monetary Units Act (Vic), s.6(a). Up to date Penalty Unit Values are published by the Victoria State Government: Victoria State Government: Treasury and Finance, 'Indexation of Fees and Penalties' <https://www.dtf.vic.gov.au/financial-management-government/indexation-fees-and-penalties> accessed 22 July 2019.
[33] No fixed value for a penalty unit exists in Western Australia. Some legislation sets its own value for a penalty unit such as: Road Traffic (Administration) Act 2008 (WA), s.6(2). Other legislation pegs its

The money laundering offences are contained in the Criminal Code, which is Commonwealth legislation. Commonwealth legislation applies across all Australian jurisdictions, it is federal law,[34] and the current value of 1 penalty unit is $170; therefore, the maximum fine for money laundering is calculated as follows: 1500 x £170 = $255,000. This is much lower than the fines which may be imposed in the US; where each of the three money laundering offences in §1956[35] carry maximum fines of "US*$500,000 or twice the value*"[36] of the funds involved, which equates to approximately AU$700,000.*[37]* However, the maximum sentence is higher than both the UK and the US. In the UK the maximum sentence is 14 years,[38] and sentences in the US are up to twenty years. However, in the US numerous counts may be sentenced concurrently, meaning that actual sentences are often much longer.

The 2015 FATF mutual evaluation report concluded that Australia was compliant with Recommendation 3,[39] which requires members to criminalise money laundering.[40] However, the FATF criticised the effectiveness and implementation of the offences at

penalty unit value to that of the Commonwealth jurisdiction, such as: Australian Crime Commission (Western Australia) Act 2004 (WU), s.3(6).

[34] Commonwealth of Australia Constitution Act, Clause 5.

[35] 18 USC §1956.

[36] 18 USC §1956(a)(1) and (2).

[37] Equating to 709,773.06 AUD: XE, '500,000 USD to AUD = 709,773.06 Australian Dollars' <https://www.xe.com/currencyconverter/convert/?Amount=500%2C000&From=USD&To=AUD> accessed 22 July 2019.

[38] Proceeds of Crime Act 2002, Part 7, s.334.

[39] Financial Action Task Force, 'Anti-money laundering and counter-terrorist financing measures - Australia, Fourth Round Mutual Evaluation Report' <https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Report-Australia-2015.pdf> accessed 23 July 2019 at a.3.12.

[40] Financial Action Task Force, 'The FATF Recommendations' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> accessed 03 September 2019, Recommendation 3 at p.10.

"*the State and Territory level*",[41] and that while Australia has utilised Division 400 offences against natural legal persons, these offences were not being used to pursue corporations.[42] With regards to sentencing, the FATF found that sentences were often "*combined with sentences for predicate offences*"[43] and therefore difficult to assess the sanctions. The FATF praised the structure of Australian money laundering offences, noting that the varying levels of fault allows for "*proportionate sanctions to be applied.*"[44] The Australian criminalisation of money laundering is compliant with both the FATF recommendations and UN Conventions.[45] The focus of prosecutors in Australia was on asset seizures, and the FATF has previously observed money laundering being treated as a "*subsidiary crime*".[46] This suggests that prosecutions for money laundering using cryptocurrencies will take similar form, and will be attached to prosecutions for predicate offences. As Chaikin notes, the conviction rate improved between the 2005 and 2015 FATF evaluations,[47] but the total number of convictions was still low, with 149 custodial sentences.[48] The low number of convictions can be balanced against the relative importance of gaining prosecutions for the predicate offences, Chaikin questions the bias of the FATF, suggesting that it is immaterial which offence a criminal is prosecuted for between the original criminal behaviour and the management of the proceeds of crime.[49] The argument that any conviction is better

[41] Financial Action Task Force, 'Anti-money laundering and counter-terrorist financing measures - Australia, Fourth Round Mutual Evaluation Report' <https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Report-Australia-2015.pdf> accessed 23 July 2019 at a.3.1.
[42] ibid at 3.52.
[43] ibid.
[44] ibid.
[45] cf Ryder (n3) at 5.6.
[46] ibid.
[47] D. Chaikin, 'A Critical Analysis of the Effectiveness of Anti-Money Laundering Measures with Reference to Australia' in C. King, C, Walker and J. Gurulé, *The Palgrave Handbook of Criminal and Terrorism Financing Law* (Palgrave Macmillan, 2018) at p308.
[48] ibid.
[49] ibid at p309.

than no conviction is a valid one, but only where the offender has committed the predicate offence, it is less applicable in organised crime where the money laundering operation is separated from the predicate offences. As identified in chapter five at 5.4.1, Rider observes that money laundering by professional accomplices has been occurring for decades.[50] The importance of pursuing money laundering alone is important as the "*modern money launderer is unlikely to be involved as a member of a criminal organisation*"[51] instead they are likely to be within the financial services industry and "*prepared to make his services available to whoever is willing to pay.*"[52]

Australia has criminalised money laundering in line with the FATF guidelines, and the offences are drafted widely enough so that using cryptocurrencies to disguise proceeds of crime will satisfy the money laundering offences. As identified in chapter five, the UK offences are also applicable to cryptocurrencies, and while the Australian approach to criminalising money laundering is structurally different to the UK, ultimately the same effect is achieved. Given that it is possible to launder money through cryptocurrencies, focus will now turn to the preventative measures designed to prevent and detect money laundering in Australia.

7.4. Preventative Measures

Australia's preventative measures are contained within the Anti-Money Laundering and Counter Terrorist Financing Act 2006 (AML/CTF Act 2006).[53] As in the UK and the US, the key preventive measures are customer identification procedures and

[50] B. Rider, 'The practical and legal aspects of interdicting the flow of dirty money' (1996) 3(3) JFC 234 at 241.
[51] ibid.
[52] ibid.
[53] Anti-Money Laundering and Counter-Terrorism Financing Act 2006.

reporting obligations. Customer due diligence (CDD), also known as know your customer, is identified by Chaikin a one of the "*pillars of the anti-money laundering regime*"[54] and observes that the concept pre-dates recognised AML law.[55] Likewise, Demetriades states that CDD is "*vital for the prevention of money laundering.*"[56] The reporting obligation in Australia take two forms, suspicious matter reports, and threshold transactions, as in the US, threshold transactions are imposed as obligatory reporting regardless of suspicion.

7.4.1. Threshold Transactions

Australia, like the US, makes reporting certain transactions compulsory through Threshold Transaction Report (TTRs). Section 43 of the AML/CTF Act 2006 stipulates that if a reporting entity "*provides, a designated service,*"[57] which "*involves a threshold transaction*"[58] it "*must, within 10 business days after the day on which the transaction takes place, give the AUSTRAC CEO a report of the transaction.*"[59] The threshold is set at $10,000 for either physical currency or an electronic transfer,[60] which is the same threshold used in the US, however the exchange rate means the threshold in Australia is lower in real terms, at approximately 7,000 USD.[61] The threshold for reporting one-off transactions is lower than the one recommended by the FATF, who

[54] D. Chaikin, 'Risk-Based Approaches to Combatting Financial Crime' (2009) 8(2) Journal of Law and Financial Crime 20 at 22.
[55] ibid.
[56] G. Demetriades, '"Is the person who he claims to be?" old fashion due diligence may give the correct answer!' (2016) 19(1) JMLC 79.
[57] Anti-Money Laundering and Counter-Terrorism Financing Act 2006 Part 3 s.43(1)(a).
[58] Anti-Money Laundering and Counter-Terrorism Financing Act 2006 Part 3 s.43(1)(b).
[59] Anti-Money Laundering and Counter-Terrorism Financing Act 2006 Part 3 s.43(2).
[60] Anti-Money Laundering and Counter Terrorist Financing Act 2006 Part 1 s.5: Definitions.
[61] Based on an exchange rate of 1 AUD = 0.7007376: XE, '1 AUD to USD = 0.700376 US Dollars' <https://www.xe.com/currencyconverter/convert/?Amount=1&From=AUD&To=USD> accessed 23 July 2019.

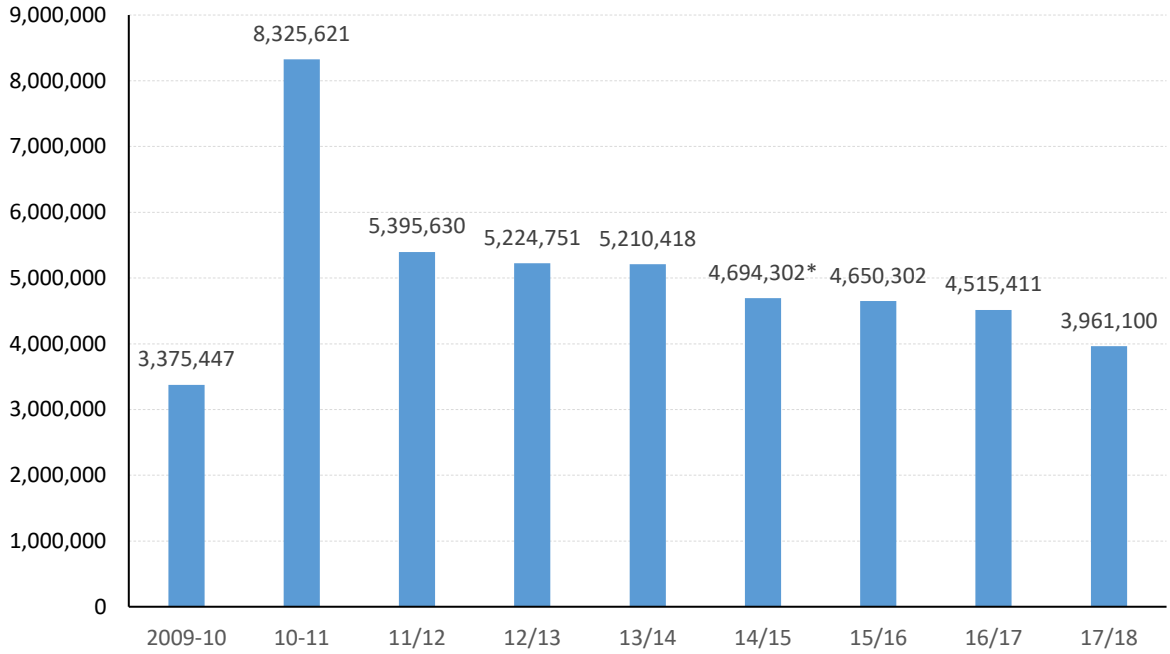
recommend threshold reporting where the transactions exceed USD/EUR 15,000.[62] Australia has set a threshold which is approximately 33% of the value in the FATF guidance. Each country is the best placed to set a threshold for their jurisdiction, based on their application of a risk-based approach, but by setting the threshold lower, more reports will be made to the financial intelligence unit (FIU). Australia's FIU is the Australian Transaction Reports and Analysis Centre (AUSTRAC). Despite the low threshold, TTR volumes have been steadily reducing, as Figure 12 shows. The number of reports was notably higher in 2010/11, which could be related to the transition from reporting under the Financial Transactions Reporting Act 1988,[63] to the AML/CTF Act 2006.[64] The UK does not implement threshold reporting, and given the resourcing limitations identified in the UKFIU, it is not advisable for the UK to adopt this measure. It is not clear how threshold reports will assist the UK in combatting the money laundering threat posed by cryptocurrencies.

[62] US$15,000 equates to approximately AU$21,500: Based on an exchange rate of 1 AUD = 0.7007376 USD: XE, '1 AUD to USD = 0.700376 US Dollars' <https://www.xe.com/currencyconverter/convert/?Amount=1&From=AUD&To=USD> accessed 23 July 2019. €15,000 equates to approximately AU$23,900: Based on an exchange rate of 1 AUD = 0.628131 EUR: XE, '1 AUD to EUR = 0.628131 Euros' <https://www.xe.com/currencyconverter/convert/?Amount=1&From=EUR&To=AUD> accessed 23 July 2019.

[63] Financial Transactions Reporting Act 1988.

[64] Anti-Money Laundering and Counter-Terrorism Financing Act 2006.

Figure 12. Annual Threshold Transaction Report Volume[65]



7.4.2. Reports of Suspicious Matters

Australia requires regulated institutions to report matter which are suspicious, this is the consistent with the UK and the US. Where the UK and the US have specific provisions for reporting suspected money laundering, the Australian AML/CTF Act 2006 includes a widely drafted reporting requirement, which not only requires reporting entities to report if they suspect money laundering, but also if they suspect terrorist

[65] Compiled from AUSTRAC Annual Reports: AUSTRAC, 'AUSTRAC Annual Report 2013-14' <https://parlinfo.aph.gov.au/parlInfo/download/publications/tabledpapers/94f918c0-cc3a-4f86-a7bf-482d563b9daf/upload_pdf/austrac-ar13-14-web-full.pdf;fileType=application%2Fpdf#search=%22Australian%20Transaction%20Reports%20and%20Analysis%20Centre%20report%20for%202013%22> accessed 24 July 2019 at p.32, AUSTRAC, 'AUSTRAC Annual Report 2015-16' <https://www.austrac.gov.au/sites/default/files/2019-05/AUSTRAC_annual_report_2015-16.pdf> accessed 24 July 2019 at p.76, AUSTRAC, 'AUSTRAC Annual Report 2016-17' <https://www.austrac.gov.au/sites/default/files/2019-05/AUSTRAC_annual_report_2016-17.pdf> accessed 24 July 2019 at p.37, and AUSTRAC, 'AUSTRAC Annual Report 2017-18' <https://www.austrac.gov.au/sites/default/files/2019-05/AUSTRAC_annual_report_2017-18.pdf> accessed 24 July 2019 at p.34. *calculated based on a reduction of approximately 44,000 reports from 2014-15 to 2015-16 reported in AUSTRAC, 'AUSTRAC Annual Report 2015-16' <https://www.austrac.gov.au/sites/default/files/2019-05/AUSTRAC_annual_report_2015-16.pdf> accessed 24 July 2019 at p.76, AUSTRAC Annual Report 2014-15 is unavailable.

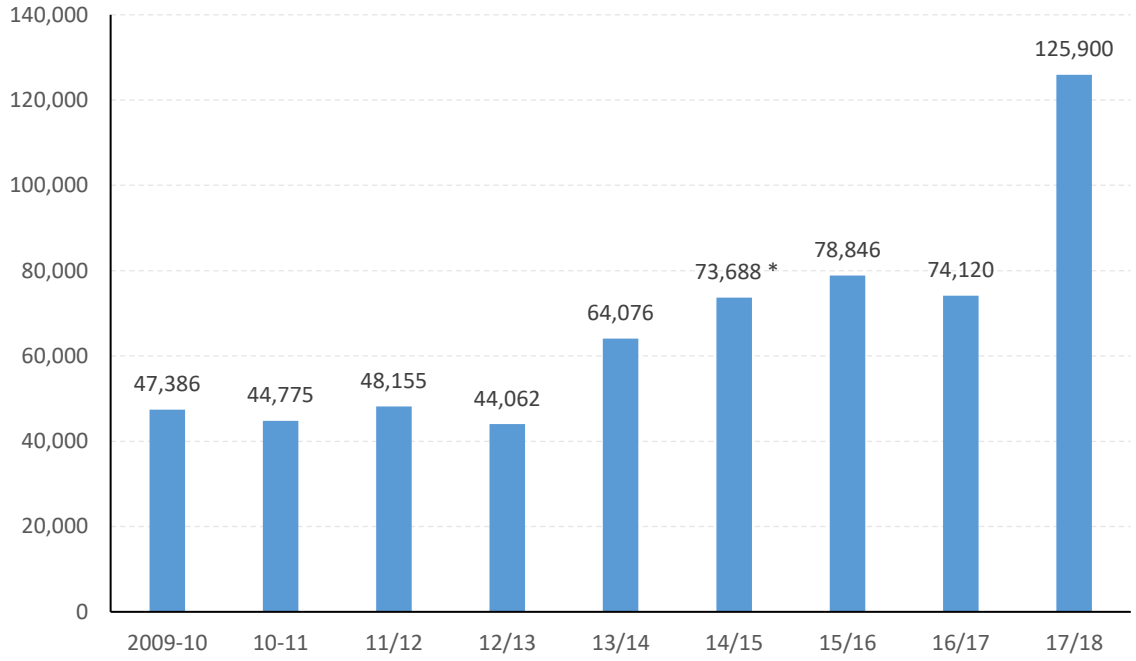
financing, fraud, and tax evasion. A reporting entity must submit a suspicious matter report (SMR) within "*3 business days after the day on which the reporting entity forms the relevant suspicion*."[66]

No legal definition exists for suspicion, but AUSTRAC provides an extensive list of potential situations in which require a SMR to be submitted.[67] The behaviours listed focus on customers acting unusually[68] or out of character,[69] undertaking transactions which are either illogical[70] or lacking business rationale,[71] and transacting in high volume[72] or high value,[73] or making a number of transactions just below the TTR threshold,[74] which is referred to as smurfing.[75] While examples are helpful, this still falls short of a definition of suspicion, which is a common problem for AML regimes, and a problem shared with the UK and US.[76] In the US, a similar approach is taken to Australia, with 'Red Flag' incidents highlighted by the Financial Crimes Enforcement Network (FinCEN)[77] which address similar instances as provided by AUSTRAC.[78] The

[66] Anti-Money Laundering and Counter-Terrorism Financing Act 2006 Part 3 s.41(2)(a).
[67] AUSTRAC, 'AUSTRAC Typologies and Case Studies Report 2014' <https://www.austrac.gov.au/sites/default/files/2019-07/typologies-report-2014.pdf> accessed 24 July 2019 Appendix A.
[68] Examples 1 and 17 refer to unusual transactions: AUSTRAC, 'AUSTRAC Typologies and Case Studies Report 2014' <https://www.austrac.gov.au/sites/default/files/2019-07/typologies-report-2014.pdf> accessed 24 July 2019 Appendix A.
[69] ibid, examples 15 refers to sudden changes in a customer's gambling.
[70] ibid, examples 6 and 16 refer to actions lacking logical reasoning.
[71] ibid, examples 7 and 18 refer to transaction slacking business rationale.
[72] ibid, example 9 refers to frequency, example 6 refers to volume, examples 10 refers to multiple transfers, and example 12 refers to regular or multiple transactions.
[73] ibid, example 6 refers to high-value transfers.
[74] ibid, examples 10 and 13 refer to transactions being just below £10,000.
[75] M. Goldby, 'Anti-Money Laundering Reporting Requirements Imposed by English Law: Measuring Effectiveness and Gauging the Need for Reform' (2013) 4 Journal of Business Law 367 at 394.
[76] Goldby discussed the problematic term suspicious in: M. Goldby, 'Anti-Money Laundering Reporting Requirements Imposed by English Law: Measuring Effectiveness and Gauging the Need for Reform' (2013) 4 Journal of Business Law 367 at 368-373.
[77] FinCEN, 'Reporting Suspicious Activity – A Quick Reference Guide for Money Services Businesses' <https://www.fincen.gov/statutes_regs/guidance/pdf/msbsar_quickrefguide.pdf> accessed 14 December 2015.
[78] See chapter six at 6.4.2 for examples of FinCEN Red Flags.

UK also struggles with the concept of suspicion, which inflates the volume of reports submitted to the FIU.[79] The Law Commission identify the low threshold for suspicion, [80] the criminal liability for failure to report, [81] and the lack of a clear definition[82] as the factors causing over reporting. The volume of reports in Australia is considerably lower than in the UK, as can be seen in Figure 13 below.

Figure 13. Suspicious Matter Report Volume[83]



[79] See chapter five at 5.4.2 for discussion of the UK interpretation of suspicion.
[80] Law Commission, *Anti-money laundering: the SARs regime* (Law Com No 384, 2018) para 5.11.
[81] ibid at para 5.12.
[82] ibid at para 5.13.
[83] Compiled from AUSTRAC Annual Reports: AUSTRAC, 'AUSTRAC Annual Report 2013-14' <https://parlinfo.aph.gov.au/parlInfo/download/publications/tabledpapers/94f918c0-cc3a-4f86-a7bf-482d563b9daf/upload_pdf/austrac-ar13-14-web-full.pdf;fileType=application%2Fpdf#search=%22Australian%20Transaction%20Reports%20and%20Analysis%20Centre%20report%20for%202013%22> accessed 24 July 2019 at p.32, AUSTRAC, 'AUSTRAC Annual Report 2015-16' <https://www.austrac.gov.au/sites/default/files/2019-05/AUSTRAC_annual_report_2015-16.pdf> accessed 24 July 2019 at p.76, AUSTRAC, 'AUSTRAC Annual Report 2016-17' <https://www.austrac.gov.au/sites/default/files/2019-05/AUSTRAC_annual_report_2016-17.pdf> accessed 24 July 2019 at p.37, and AUSTRAC, 'AUSTRAC Annual Report 2017-18' <https://www.austrac.gov.au/sites/default/files/2019-05/AUSTRAC_annual_report_2017-18.pdf> accessed 24 July 2019 at p.34. *calculated based on an

It can be seen in Figure 13 above, that the volume of reports has been consistent, approximately 75,000 SMRs per year between 2014-2017, having risen from an average of around 45,000 during 2010-2013, however, there has been a dramatic rise in SMRs 2017/18. Even with the recent rise in numbers, these volumes are far lower than the in the UK where over 400,000 suspicious activity reports are filed each year.[84] Australian SMRs figures for 2018/19 are not available at the time of writing, and it is not possible to ascertain whether the 2017/18 volume is a sign of a new norm; it could be a reaction to the high-profile enforcement action from AUSTRAC. In November 2017 Tabcorp was fined $45million,[85] and in June 2018 Commonwealth Bank of Australia was fined $700million,[86] in what were viewed as landmark rulings.[87] Tabcorp's failings included not having a compliant AML program for over three years[88] and failing to submit SMRs either "*on time or at all on 105 occasions.*"[89] Similarly, Commonwealth Bank of Australia's failings included, but were not limited to, three years of failing to monitor 778,370 accounts,[90] continuing business with customers it was aware were suspected of money laundering,[91] and failing to submit SMRs

increase of approximately 7% in SMRs from 2014-15 to 2015-16 reported in AUSTRAC, 'AUSTRAC Annual Report 2015-16' <https://www.austrac.gov.au/sites/default/files/2019-05/AUSTRAC_annual_report_2015-16.pdf> accessed 24 July 2019 at p.76, AUSTRAC Annual Report 2014-15 in unavailable.

[84] See Figure 6 in chapter five at 5.4.2 for annul SARs volumes in the UK.

[85] Chief Executive Officer of Australian Transaction Reports and Analysis Centre v TAB Limited (No 3) [2017] FCA 1296.

[86] Chief Executive Officer of the Australian Transaction Reports and Analysis Centre v Commonwealth Bank of Australia Limited [2018] FCA 930.

[87] P Durkin, '70pc jump in suspicious money laundering transactions: AUSTRAC' *Financial Review* (Melbourne, 18 October 2018) <https://www.afr.com/business/banking-and-finance/70pc-jump-in-suspicious-money-laundering-transactions-austrac-20181018-h16szs> accessed 24 July 2019.

[88] AUSTRAC, 'Record $45 million civil penalty ordered against Tabcorp' (16 September 2019) <https://www.austrac.gov.au/record-45-million-civil-penalty-ordered-against-tabcorp> accessed 22 October 2019.

[89] ibid.

[90] AUSTARC, 'AUSTRAC and CBA agree $700m penalty' (4 June 2018) <https://www.austrac.gov.au/austrac-and-cba-agree-700m-penalty> accessed 22 October 2019.

[91] ibid.

involving transactions totalling over $10million.[92] These sanctions could prove to be a spur for other regulated entities to adhere to reporting requirements, as suggested by a 70% increase in SMRs in 2018,[93] but it could also be that reporting entities are adopting a defensive reporting strategy, rather than engaging with the AML provisions. It is not possible for this thesis to prove defensive reporting is taking place, but Australia has a history of over-reporting. Jensen observed in 2005 that AUSTRAC received a "*very high volume of data compared to other FIUs around the world*"[94] which was in part down to TTRs, as these are mandatory regardless of suspicion. As identified in chapters five and six in relation to the UK and US, the issue of defensive reporting has been identified by Levi in the 1990s,[95] by McNeil in the early 2000s,[96] and Ryder in 2012.[97] Given the severity of the potential sanctions for non-compliance, it is likely that cryptocurrency businesses which are regulated by AUSTRAC, will adopt a similar approach to the institutions in the traditional financial system. The effects of applying the SMR regime to cryptocurrencies cannot be assessed yet due to the limited timeframe, and lack of published data, but it demonstrates an attempt to apply AML regulation to cryptocurrency activity, and the UK could follow Australia's lead.

[92] ibid.
[93] P Durkin, '70pc jump in suspicious money laundering transactions: AUSTRAC' *Financial Review* (Melbourne, 18 October 2018) <https://www.afr.com/business/banking-and-finance/70pc-jump-in-suspicious-money-laundering-transactions-austrac-20181018-h16szs> accessed 24 July 2019.
[94] N. Jensen, 'Technology and Intelligence' (2005) 8(3) JMLC 227 at 236.
[95] M. Levi, 'Evaluating the "New Policing": Attacking the Money Trail of Organized Crime' (1997) 30(1) Australian and New Zealand Journal of Criminology 1 at 9.
[96] C. McNeil, 'The Australian Anti-Money Laundering Reform in the International Context' (2007) 22(6) Journal of International Banking Law and Regulation 340 at 341.
[97] cf Ryder (n3) at 5.8.

7.4.3. Customer Due Diligence

The AML/CTF Act 2006 requires reporting entities to comply with CDD requirements, as does the AML legislation of the UK and the US. Australia is different from the other two jurisdictions in that it requires all reporting entities to complete a written risk assessment. Under s.165 of the AML/CTF Act 2006, a civil penalty may be imposed if a written risk assessment is not submitted.[98] The risk assessment should seek to identify,[99] mitigate,[100] and manage[101] the potential risks of money laundering affecting the reporting entity's business.

Reporting entities are also expected to gather specific information from their customers in order to identify them; s.27 of Part 2 of the AML/CTF Act 2006[102] requires regulated entities to verify the identity of their customers, and complete ongoing due diligence.[103] As identified in chapter four, Chaikin finds fault with CDD, particularly for its Western approach, arguing that this is ineffective for ethic groups who use different naming systems.[104] Additionally the assumption that customers will be honest can be questioned; there are no legal requirements for customers to provide full disclosure of the names they use or the accounts they have opened.[105] As identified in chapter five,[106] Irwin and Dawson highlight that "*cybercriminals are likely to be comfortable*

[98] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, Part 13 Division 8 s.165
[99] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, Part 13 Division 8 s.165(6)(b)(i).
[100] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, Part 13 Division 8 s.165(6)(b)(ii).
[101] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, Part 13 Division 8 s.165(6)(b)(iii).
[102] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, Part 2.
[103] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, Part 2, s.27.
[104] cf Chaikin (n54) at 23.
[105] ibid.
[106] See chapter five at 5.4.1.

obtaining fraudulent documents"[107] which can defeat CDD, and that the high cost of implementing extensive identification processes is not proportionate to those making small cryptocurrency payments.[108] CDD requirements are also vulnerable to professional money launders, long prior to the existence of CDD individuals have offered services to 'clean' money, as observed by Rider.[109] Such individuals will be likely to pass CDD checks without drawing attention to themselves, undermining the AML measures. Cryptocurrencies provide a further tool to money launderers who do not commit the predicate offences. It has been identified already in this thesis that cryptocurrencies provide users with mechanisms to conceal their identity,[110] therefore applying CDD requirements to cryptocurrency businesses will be more difficult than for the traditional financial institutions. Irwin and Turner recommend a more joined up approach for cryptocurrencies, calling for "*information sharing between multiple stakeholders from the law enforcement, financial intelligence units, cyber security organisations and fintech industry.*"[111] Improved CDD data will aid in determining when a SMR is required, but there are currently no signs such an approach is forthcoming.

The Australian approach is risk-based, so the level of information required from each customer will depend on the risks involved; however, a minimum level of information

[107] A. S. M. Irwin, and C. Dawson, 'Following the cyber money trail: Global challenges when investigating ransomware attacks and how regulation can help' (2019) 22(1) JMLC 110 at 125.
[108] ibid.
[109] cf Rider (n50) at 241.
[110] The anonymity attached to cryptocurrencies is addressed by the US Government Accountability Office in their 2014 report, which described such currencies as pseudonymous, as the although the users name is not known, other details are published on the blockchain; such as their Bitcoin address, the time of the transaction, and the amount: United States Government Accountability Office, 'Virtual Currencies: Emerging Regulatory, Enforcement, and Consumer Protection Challenges' <http://gao.gov/assets/670/663678.pdf> accessed 16 December 2015 at p.6.
[111] A. S. M. Irwin and A. B. Tuner, 'Illicit Bitcoin transactions: challenges in getting to the who, what, when and where' (2018) 21(3) JMLC 297 at 310.

is required from all customers. The minimum information includes the customer's name,[112] date of birth,[113] and address.[114] In addition to the minimum information, each reporting entity must utilise its risk assessment to determine when additional CDD information is required.[115] The risk-based approach is also employed in both the UK and the US, and it is recommended by the FATF and the EU. The level of risk associated with cryptocurrencies is difficult to quantify. The applicability of these measures to cryptocurrencies needs to be considered to determine whether there are gaps in the law that may be exploited for money laundering purposes.

7.5. Applicability of Preventative Measures to Cryptocurrencies

For the purpose of the money laundering offences in Australia, cryptocurrencies will satisfy the requirement for dealings "*with money or other property,*"[116] and the offences are applicable This was not the case for AML measures, as cryptocurrencies service providers fell outside of the list of designated services of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006.[117] This was highlighted in the 2016 statutory review of the Anti-Money Laundering and Counter-Terrorism Financing Act

[112] Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1) Para 4.2.3.(1).
[113] Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1) Para 4.2.3.(2).
[114] Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1) Para 4.2.3.(3).
[115] Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1) Para 4.2.5.
[116] Criminal Code Act 1995 Subdivision 400.3(1)(a).
[117] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.6.

2006.[118] It was noted that the only possible way for cryptocurrencies to be regulated was through the definition of 'e-currency' in s.6,[119] which did not cover "*decentralised crypto-currencies such as Bitcoin, because crypto-currencies are backed by an algorithm rather than a physical thing*."[120] This gap was also highlighted by the Attorney General's Department report on the statutory review. [121] The statutory review recommended that the definition of an e-currency should be expanded to include convertible digital currencies, specifically to cover cryptocurrencies.[122] The 2016 statutory review led to the Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2017,[123] which became the Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017.[124] The 2017 amendment inserted "*digital currency*"[125] into the definitions section, and the definition of a digital currency follows that of the FATF. A digital currency performs the functions of money,[126] while not issued by a government or authority,[127] and it is interchangeable with money.[128] Importantly, to distinguish from shop vouchers or local currencies, the definition also requires the currency to be available to the public without restriction on its use as consideration.[129] The 2017 amendment also inserted the terms "*registered digital*

[118] Australian Government Department of Home Affairs, 'Report on The Statutory Review of The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 And Associated Rules and Regulations' <https://www.homeaffairs.gov.au/how-to-engage-us-subsite/files/report-on-the-statutory-review-of-the-anti-money-laundering.pdf> accessed 16 July 2019.
[119] ibid at p.45.
[120] ibid.
[121] ibid at p.46.
[122] ibid at p.49.
[123] Parliament of Australia, 'Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2017'
<https://parlinfo.aph.gov.au/parlInfo/download/legislation/billsdgs/5592699/upload_binary/5592699.pdf;fileType=application/pdf> accessed 16 July 2019.
[124] Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017.
[125] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.5.
[126] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.5, Digital Currency (a)(i).
[127] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.5, Digital Currency (a)(ii).
[128] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.5, Digital Currency (a)(iii).
[129] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.5, Digital Currency (a)(iv).

currency exchange provider"[130] and "*registrable digital currency exchange service*"[131] which recognise the existence of cryptocurrency service providers.

In addition to providing statutory definitions for the purposes of money laundering legislation, the 2017 amendment adds digital currency exchange services to the list of designated services, which are regulated by the Act.[132] The 2017 reforms mean that Australia is compliant with the FATF guidance issued in 2019,[133] long before the guidance was released. This demonstrates that Australia is proactive in seeking to understand cryptocurrencies, the risks they pose, and how to regulate them. Legislators in Australia are also utilising guidance from consultation papers and international organisations. The UK should look to the approach taken in Australia as an example of good practice to follow. Australia's AML regulation of cryptocurrencies is not complete, but by adhering to FATF guidance, a clear, and welcome, starting point has been established, from which it can build more tailored regulation. As has been identified throughout this thesis, combatting money laundering, and any crime for that matter, has two clear requirements, appropriate laws, and appropriate enforcement. Having considered the applicability of Australian legislation, attention now must turn to the relevant authorities that are responsible for enforcing the law.

[130] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.5.
[131] ibid.
[132] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.6(2) Item 50A.
[133] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2019.

7.6. Authorities

In this section, the relevant authorities which make up Australia's AML approach will be identified. After that the relevant authorities' responses to cryptocurrencies will be analysed. Regulatory bodies can be categorised into primary and secondary authorities; primary authorities set AML policy, and secondary authorities are enforcement agencies, regulatory agencies and financial intelligence units. A third category, tertiary authorities, is also recognised by Ryder;[134] tertiary agencies may include "*trade associations and professions which are threatened by illegal transactions*."[135] Cryptocurrencies are in their infancy compared to industries and professions within the traditional financial system, but the Australian Digital Commerce Association (ADCA) is identified here as a tertiary body. While an array of authorities have responsibilities for tackling money laundering in Australia, this section will identify the relevant authorities with regards to cryptocurrencies and money laundering.

7.6.1. Primary

Attorney General's Department

Australia only has one primary agency, as recognised by the FATF's mutual evaluation report in 2015;[136] the Attorney General's Department (AGD), which manages AML policy and makes recommendations, as identified by Ryder.[137] The FATF identify the

[134] cf Ryder (n3) at p.25.
[135] ibid.
[136] Financial Action Task Force, 'Australia – Mutual Evaluation Report – April 2015' <http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Report-Australia-2015.pdf> accessed 05 September 2019 at p.36.
[137] cf Ryder (n3) at p.110.

AGD as having "*policy responsibility for AML/CTF*"[138] as well as being "*Australia's central authority for extradition and mutual legal assistance in criminal matters*."[139] The AGD states that it "*delivers programs and policies to maintain and improve Australia's law and justice framework,*"[140] in this capacity, similarly to HM Treasury in the UK, AGD will conduct public consultations, and make recommendations based on these consultations. The AGD's most recent review of the AML/CTF regime was published in April 2016,[141] and recommends simplifying reporting procedures and strengthening enforcement measures.[142] The report also identified money laundering risks posed by cryptocurrencies,[143] which is discussed at 7.7.3 below.

7.6.2. Secondary

Australian Transaction Reports and Analysis Centre (AUSTRAC)

AUSTRAC is "*Australia's financial intelligence unit* (FIU) *with regulatory responsibility for anti-money laundering and counter-terrorism financing*."[144] As the FIU, all TTRs and SAR's are sent to AUSTRAC, and AUSTRAC then attempts to "*join the dots to provide a complete financial intelligence picture,*"[145] and the *"resulting financial*

[138] Financial Action Task Force, 'Australia – Mutual Evaluation Report – April 2015' <http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Report-Australia-2015.pdf> accessed 05 September 2019 at p.36.
[139] ibid.
[140] Attorney General's Department, 'About Us' <http://www.ag.gov.au/About/Pages/default.aspx> accessed 10 July 2015.
[141] Attorney General's Department, 'Report on The Statutory Review of The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 And Associated Rules and Regulations' (April 2016) <https://www.homeaffairs.gov.au/how-to-engage-us-subsite/files/report-on-the-statutory-review-of-the-anti-money-laundering.pdf> accessed 28 October 2019.
[142] ibid at p.3-6.
[143] ibid at p.45.
[144] AUSTRAC, 'About AUSTRAC' <http://www.austrac.gov.au/about-us/austrac> accessed 14 September 2019.
[145] ibid.

intelligence is provided to partner agencies."[146] As has been seen in relation the UK and the US, the numbers of transaction reports sent to the FIU are very high; in 2014-2015 AUSTRAC received 96,369,657 transaction reports,[147] 91,423,681 of which are International Funds Transfer Instruction (IFTI) reports, which are obligatory if "*a reporting entity sends or receives an instruction to or from a foreign country, to transfer money or property*."[148] Similarly to the Financial Conduct Authority (FCA) in the UK, and FinCEN in the US, AUSTRAC makes rules which regulated entities must follow, this power is vested in the CEO of AUSTRAC, but all rule changes are developed with relevant stakeholders.[149] The FATF describe AUSTRAC as a "*well-functioning*"[150] FIU, praising the volume of transaction data AUSTRAC holds and the integration with other authorities, particularly with regards to data sharing.[151] A criticism levelled by the FATF is that the information AUSTRAC maintains is not utilised frequently enough by law enforcement.[152] AUSTRAC has powers of enforcement, through the AML/CFT Act 2006,[153] which it utilised in November 2017 when Tabcorp was fined $45million,[154] and in June 2018 when the Commonwealth Bank of Australia was fined $700million.[155]

[146] ibid.
[147] AUSTRAC, 'AUSTRAC Annual Report: 2014-15' <http://www.austrac.gov.au/sites/default/files/austrac-ar-14-15-web.pdf> accessed 15 September 2019 at p.66.
[148] ibid at p.68
[149] AUSTRAC, 'AML/CTF Rules overview' (27 September 2019) <https://www.austrac.gov.au/business/legislation/amlctf-rules/amlctf-rules-overview> accessed 23 October 2019.
[150] Financial Action Task Force, 'Australia – Mutual Evaluation Report – April 2015' <http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Report-Australia-2015.pdf> accessed 05 September 2019 at p8.
[151] ibid.
[152] ibid.
[153] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, Part 15.
[154] Chief Executive Officer of Australian Transaction Reports and Analysis Centre v TAB Limited (No 3) [2017] FCA 1296.
[155] Chief Executive Officer of the Australian Transaction Reports and Analysis Centre v Commonwealth Bank of Australia Limited [2018] FCA 930.

However, the large fines in recent years are viewed in the press as landmark rulings,[156] and the list of AUSTRAC enforcement actions is short, particularly when compared to FinCEN in the US[157] and the FCA in the UK.[158] As outlined in below at 7.7.4. AUSTRAC is responsible for the AML regulation of cryptocurrency service providers and the FCA may look to the experiences of AUSTRAC in executing its own regulation from 2021.[159]

Australian Criminal Intelligence Commission (ACIC)

The Australian Criminal Intelligence Commission (ACIC) is the national criminal intelligence agency of Australia.[160] The purpose of the ACIC is to "*collect intelligence to improve the national ability to respond to crime impacting Australia*",[161] it operates on a national level and with international counterparts.[162] The ACIC is comparable to the National Crime Agency (NCA) in the UK, specialising in organised crime and being the "*conduit for sharing criminal information and intelligence between all state, territory and Commonwealth law enforcement agencies.*"[163] As the ACIC identify, "[m]*oney*

[156] P Durkin, '70pc jump in suspicious money laundering transactions: AUSTRAC' *Financial Review* (Melbourne, 18 October 2018) <https://www.afr.com/business/banking-and-finance/70pc-jump-in-suspicious-money-laundering-transactions-austrac-20181018-h16szs> accessed 24 July 2019.
[157] FinCEN have published 70 enforcement actions since 2006: FinCEN, 'Enforcement Actions' (18 April 2019) <https://www.fincen.gov/news-room/enforcement-actions> accessed 23 October 2019.
[158] The FCA have issued a similar number of fines in 2019 to total number of actions AUSTRAC has taken in its lifetime: FCA, '2019 Fines' (11 October 2019) <https://www.fca.org.uk/news/news-stories/2019-fines> accessed 23 October 2019.
[159] HM Government 'Economic Crime Plan' (12 July 2019) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/816215/2019-22_Economic_Crime_Plan.pdf> accessed 23 October 2019 at 4.9.
[160] Australian Crime Intelligence Commission, 'About Us' (17 May 2019) <https://www.acic.gov.au/about-us> accessed 29 July 2019.
[161] ibid.
[162] ibid.
[163] ibid.

laundering is the common element in almost all serious and organised crime"[164] therefore it is of paramount concern to the ACIC. The ACIC is a law enforcement authority, it will investigate cryptocurrencies with regard to organised crime, but does not have a supervisory role over any regulated entities.

Australian Federal Police (AFP)

Policing is principally undertaken at a state level, especially if the crime concerned is wholly committed in one state; the role of the AFP is to enforce "*Commonwealth criminal law* [and] *contribute to combating organised crime.*"[165] The AFP is also "*Australia's international law enforcement and policing representative.*"[166] The AFP is the head of the Criminal Asset Confiscation Taskforce (CACT), which pursues criminal assets and seeks to seize these assets; it successfully seized $62.5 million in 2012-2013.[167] In its role as Australia's international law enforcement and policing representative, the AFP is Australia's Terrorism Financing Investigations Unit (TFIU).[168] As with the ACIC, the AFP is not a supervisory authority, but will take part in money laundering investigations. UK police have achieved successes in pursuing money laundering where cryptocurrencies have been used, and examples of best practice should be shared between international counterparts.

---

[164] Australian Crime Intelligence Commission, 'Money laundering' (27 February 2019) <https://www.acic.gov.au/about-crime/organised-crime-groups/money-laundering> accessed 23 October 2019.
[165] Australian Federal Police, 'Our Organisation' <https://www.afp.gov.au/about-us/our-organisation> accessed 14 September 2019.
[166] ibid.
[167] Australian Federal Police, 'Criminal Asset Confiscation Taskforce' <https://www.afp.gov.au/sites/default/files/PDF/criminal-assets-confiscation-taskforce-brochure.pdf> accessed 14 September 2019.
[168] Financial Action Task Force, 'Australia – Mutual Evaluation Report – April 2015' <http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Report-Australia-2015.pdf> accessed 05 September 2019 at p.36.

7.6.3. Tertiary

Australian Digital Commerce Association (ADCA)

A recognisable tertiary body representing cryptocurrencies in Australia is the ADCA,[169] which describes itself as the "*industry body that represents Australian businesses and other organisations participating in the digital economy through blockchain technology*."[170] The ADCA promotes the use of blockchain in both private and public sectors in Australia,[171] and published a code of conduct[172] in February 2016,[173] which it updated in November 2016. The code of conduct addresses money laundering, and its provisions are in line with the guidance from the FATF. It is clearly a positive step that such a code of conduct exists, and is endorsed by a national industry association, but the code is a voluntary one,[174] and as such does not carry any force. The ADCA occupies a similar position to Crypto UK, which is the "*self-regulatory trade association*"[175] for the crypto currency sector in the UK.

[169] Australian Digital Commerce Association, 'About' <https://adca.asn.au/about/> accessed 19 July 2019.
[170] ibid.
[171] ibid.
[172] Australian Digital Commerce Association, 'Australian Digital Currency Industry Code of Conduct' <https://adca.asn.au/wp-content/uploads/2019/02/Australian-Digital-Currency-Industry-Code-of-Conduct-Board-Approved-Text-30-Nov-2016.pdf> accessed 19 July 2019.
[173] A. Margossian, M. Bagnall, R. Mitra and I. Halforty, 'Australia' in M. S. Sackheim and N. A. Howell (eds), *The Virtual Currency Regulation Review* (London, Law Business Research Ltd, 2018)
[174] The title page of the code states that it is voluntary: Australian Digital Commerce Association, 'Australian Digital Currency Industry Code of Conduct' <https://adca.asn.au/wp-content/uploads/2019/02/Australian-Digital-Currency-Industry-Code-of-Conduct-Board-Approved-Text-30-Nov-2016.pdf> accessed 19 July 2019 at p1.
[175] Crypto UK, 'About Us' <https://cryptouk.io/about/> accessed 23 October 2019.

7.7. AML Regulation of Cryptocurrencies

As is the case in the UK and the US, policy makers and legislators have considered the development of cryptocurrencies in Australia,[176] particularly the tax treatment of Bitcoin. However, Australia has gone further than the UK and the US, and has addressed cryptocurrencies through legislation. Reforms to the AML/CTF Act 2006[177] have widened the scope of AML regulation in Australia to cover cryptocurrency service providers; the approach of the relevant authorities will be considered in this section. In chapter five is was seen that the US application of AML regulation to cryptocurrencies was regulator led, this section analyses the Australian response, which has been legislator led. The UK should consider the response of Australia as a useful example when legislating with regard to cryptocurrencies, as the UK will be required to legislate in order to implement the EU's 5th Anti-Money Laundering Directive, which widens the AML regulatory perimeter to include cryptocurrency service providers.

[176] Examples to be discussed below include: Australian Tax Office, 'Tax Treatment Of Crypto-Currencies In Australia – Specifically Bitcoin' <https://www.ato.gov.au/General/Gen/Tax-treatment-of-crypto-currencies-in-Australia---specifically-bitcoin/> accessed 17 September 2019, Parliament of Australia, 'Digital Currency – Game Changer or bit player' (August 2015) <http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Digital_currency/~/media/Committees/economics_ctte/Digital_currency/report.pdf> accessed 21 October 2019, Parliament of Australia, 'Government Response to the Inquiry into Digital currency' <http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Digital_currency/~/media/Committees/economics_ctte/Digital_currency/report.pdf> accessed 10 July 2019, and Attorney General's Department, 'Report on The Statutory Review of The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 And Associated Rules and Regulations' (April 2016) <https://www.homeaffairs.gov.au/how-to-engage-us-subsite/files/report-on-the-statutory-review-of-the-anti-money-laundering.pdf> accessed 28 October 2019.

[177] Anti-Money Laundering and Counter-Terrorism Financing Act 2006

7.7.1. Australian Taxation Office

The ATO initially issued guidance on the "*tax treatment of crypto-currencies in Australia – specifically Bitcoin*"[178] in 2014, and found such cryptocurrencies not to be money.

> "*The ATO's view is that Bitcoin is neither money nor a foreign currency, and the supply of bitcoin is not a financial supply for goods and services tax (GST) purposes. Bitcoin is, however, an asset for capital gains tax (CGT) purposes.*"[179]

GST is a 10% tax rate, and this ruling by the ATO had a number of implications for the use of cryptocurrencies in the course of a business. Firstly, when receiving Bitcoins in payment for goods and services "*a business may be charged GST on that Bitcoin*."[180] Additionally a business would incur tax liability when paying for good and services using Bitcoin. As the 2014 ruling stated that "*GST is payable on the supply of bitcoin made in the course or furtherance of your enterprise*,"[181] GST would be payable for any cryptocurrency exchange services provided. It is not unreasonable to expect all businesses to pay tax where appropriate; the issue for cryptocurrency service providers is that the 2014 ruling led to them be being taxed twice. The ATO has since changed its position in relation to cryptocurrencies and GST, from 1st July 2017 sales

[178] Australian Tax Office, 'Tax Treatment of Crypto-Currencies in Australia – Specifically Bitcoin' <https://www.ato.gov.au/General/Gen/Tax-treatment-of-crypto-currencies-in-Australia---specifically-bitcoin/> accessed 17 June 2019.
[179] ibid.
[180] ibid.
[181] ibid.

and purchases of cryptocurrencies are not subject to GST.[182] This removes the issue of double taxation and shows an adaptable approach from the Australian authorities. The tax treatment of Bitcoin, and the negative feedback it received, was a factor in instigating Australia's legislative reform, and the 2014 ruling was highlighted to parliament during the consultations on reform.[183]

7.7.2. Australian Parliament

Criticisms of the 2014 ATO ruling were made clear to a parliament committee when the issue of regulating cryptocurrencies was considered; the Bitcoin Foundation and Bitcoin Association of Australia[184] submitted their concerns to the Senate Economics References Committee in 2015,[185] arguing that "*GST would be applied to the goods or services being provided, in addition to the 'supply' of the digital currency used as payment*."[186] It was argued by Bitcoin supporters that double taxation of cryptocurrencies, such as Bitcoin, effected the competitiveness of Australian based companies dealing in cryptocurrencies; "*CoinJar, an Australian digital finance start-up, noted that the ATO's GST ruling had rendered it 'uncompetitive against non-Australian rivals'."*[187] In light of these arguments, and other submissions from

[182] Australian Tax Office, 'GST and Digital Currency' <https://www.ato.gov.au/business/gst/in-detail/your-industry/financial-services-and-insurance/gst-and-digital-currency> accessed 17 September 2019.
[183] Parliament of Australia, 'Digital Currency – Game Changer or bit player' (August 2015) <http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Digital_currency/~/media/Committees/economics_ctte/Digital_currency/report.pdf> accessed 21 October 2019 at para 4.8.
[184] Now known as Blockchain Australia: Blockchain Australia, 'Home' <https://blockchainaustralia.org/> accessed 19 July 2019.
[185] Parliament of Australia, 'Digital Currency – Game Changer or bit player' (August 2015) <http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Digital_currency/~/media/Committees/economics_ctte/Digital_currency/report.pdf> accessed 21 October 2019 at para 4.8.
[186] ibid at para 4.8.
[187] ibid at para 4.13.

cryptocurrency service providers and academics,[188] the committee recommended "*digital currency should be treated as money for the purposes of the goods and services tax*."[189] The committee recommend that this should be achieved by "*amending the definition of money in the A New Tax System (Goods and Services Tax) Act 1999 and including digital currency in the definition of financial supply in A New Tax System (Goods and Services Tax) Regulations 1999*."[190] In light of the recommendations from the committee report, the Government response stated that the double taxation issue would be addressed,[191] as the withdrawing of the ATO 2014 ruling demonstrates this. The approach of the Australian Government has been reactive and flexible to cryptocurrencies, shown through its use of recommendations from the committee report.

The committee reviewed a wide range of issues pertaining to cryptocurrencies, both risks and benefits. In relation to the benefits of cryptocurrencies, the committee found little benefit to the speed and cost savings that cryptocurrencies offer; the committee considered that although "*digital currencies offer numerous advantages, their benefits are not as significant in the Australian context.*"[192] The Australian Payments Clearing Association (APCA) argued "*Australia's payment system is already overwhelmingly digital in nature, with only about 18 per cent of Australian currency existing in physical*

[188] ibid at pp.28-30.
[189] ibid at para 4.35.
[190] ibid.
[191] Parliament of Australia, 'Government Response to the Inquiry into Digital currency' <http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Digital_currency/~/media/Committees/economics_ctte/Digital_currency/report.pdf> accessed 10 July 2019 at p2.
[192] Parliament of Australia, 'Digital Currency – Game Changer or bit player' (August 2015) <http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Digital_currency/~/media/Committees/economics_ctte/Digital_currency/report.pdf> accessed 21 October 2019 at para 3.7.

form." The committee report also cites the already low cost of transactions in Australia, claiming that there "i*s little room for digital currencies to improve on domestic point-of-sale purchases, which account for around 40 per cent of all transactions by value*."[193] The committee did see benefits from cryptocurrencies, particularly the distributed public ledger introduced by Bitcoin,[194] and the APCA advice to the committee was that this was "*worth exploring and understanding the implications of.*"[195] The committee identified a number of risks relating to cryptocurrencies, not dissimilar to the concerns of the US, the key risks identified were: tax evasion,[196] financial stability,[197] price volatility,[198] pseudo-anonymity,[199] and criminal activity.[200]

The committee found that the taxation issues were similar to that of cash as it may go unreported,[201] this is clearly a money laundering concern as transactions within blockchains will not be reported. By including cryptocurrency service providers in the regulatory remit of AUSTRAC, a proportion of transactions will be reported, but the majority of transactions within cryptocurrency networks will remain unregulated and outside of the AML regime. This is because transactions within cryptocurrency networks are entirely automated, and there is no opportunity for the transaction to be reported before it is completed.

[193] ibid at para 3.8.
[194] ibid at para 3.9.
[195] ibid at para 3.10.
[196] ibid at para 3.20.
[197] ibid at para 3.23.
[198] ibid at para 3.27.
[199] ibid at para 3.29.
[200] ibid at para 3.31.
[201] ibid at para 3.20.

The committee considered the issue of financial stability but this was largely dismissed due to the size of cryptocurrency holdings, and transactions, in relation to fiat currency, being relatively small compared to fiat currency.[202] Additionally, the price volatility argument was discussed; the committee received numerous submissions that "*referred to the price instability of Bitcoin*,"[203] which may mean cryptocurrencies are "*not be suited for direct consumer interaction.*"[204] A counter argument was also submitted, arguing that the increased use of cryptocurrencies worldwide means that the "*volatility is reducing*."[205] The committee stopped short of describing cryptocurrencies as anonymous, instead a similar term as in the US was used; pseudo-anonymous.[206] This is because "*[d]igital currencies such as Bitcoin do not provide complete anonymity for users,*"[207] but the use of a public key, rather than the users identity, does act as a layer of disguise to the users. As a result, the committee was informed that the AFP is "*concerned that pseudo-anonymity and the ability to conduct digital currency transactions outside the regulated financial framework would make it difficult to determine the true owners of digital currencies*."[208] The AFP also submitted advice in relation to the criminal risks posed by cryptocurrencies, identifying four main types of crimes being investigated, which were; theft of Bitcoin via hacking;

[202] ibid at para 3.23.
[203] ibid at para 3.27.
[204] ibid.
[205] ibid.
[206] The anonymity attached to cryptocurrencies is addressed by the US Government Accountability Office in their 2014 report, which described such currencies as pseudonymous, as the although the users name is not known, other details are published on the blockchain; such as their Bitcoin address, the time of the transaction, and the amount: United States Government Accountability Office, 'Virtual Currencies: Emerging Regulatory, Enforcement, and Consumer Protection Challenges' <http://gao.gov/assets/670/663678.pdf> accessed 16 December 2015 at p.6.
[207] Parliament of Australia, 'Digital Currency – Game Changer or bit player' (August 2015) <http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Digital_currency/~/media/Committees/economics_ctte/Digital_currency/report.pdf> accessed 21 October 2019 at para 3.29.
[208] ibid at para 3.30.

the payment for the importation of illicit narcotics using Bitcoin via major online black marketplaces such as Silk Road; Bitcoin being used as payment in domestic supply and trafficking of narcotics; and money laundering and dealing with the proceeds of crime via Bitcoin.[209] It is clear that the Australian authorities are concerned about the potential to launder money through cryptocurrencies, but the committee heard from the AFP that despite the risks "*digital currencies were not currently a significant operational issue*,"[210] but if "*digital currencies become more widely used, it could become an issue in the future*."[211] The committee gave a cautious conclusion, acknowledging both the benefits and the risks of cryptocurrencies. The committee supported the application of AML regulation to cryptocurrencies; it recommended a "*statutory review considers applying AML/CTF regulations to digital currency exchanges.*"[212]

The advice of the committee was adopted, a statutory review in 2016 ultimately led to an amendment of the AML/CTF Act 2006 in 2017.[213] The 2017 amendment inserted "*digital currency*"[214] into the definitions section, and the definition of a digital currency follows that of the FATF, focussing on the functions of money being performed, but without a government or authority backing the currency.[215] The terms "*registered*

[209] Parliament of Australia, 'Digital Currency – Game Changer or bit player' (August 2015) <http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Digital_currency/~/media/Committees/economics_ctte/Digital_currency/report.pdf> accessed 21 October 2019 at para 3.35.
[210] ibid at para 3.43.
[211] ibid.
[212] ibid at para 6.37.
[213] Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017.
[214] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.5.
[215] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.5: Digital Currency.

digital currency exchange provider"[216] and "*registrable digital currency exchange service*"[217] were also added to the 2006 Act, which recognise the existence of service based cryptocurrency service providers. The list of designated services which are regulated by the AML/CTF Act 2006 now covers cryptocurrency exchange services.[218] The 2017 reforms mean that Australia is compliant with the FATF guidance issued in 2019,[219] before the guidance was released. The UK has undertaken consultations on broader issue of cryptocurrencies,[220] and the more specific issue of AML regulation of cryptocurrencies.[221] The responses in the UK consultations were similar to that of the Australian consultation process, cryptocurrencies were identified as having potentially criminal uses,[222] and found to pose money laundering risks due to the levels of anonymity.[223] However, despite the UK consulting at a similar time to Australia, it did not go on to enact reforms to address cryptocurrency money laundering concerns until it was required to by the EU's 5th Anti-Money Laundering Directive. The reforms to the AML/CTF Act 2006 demonstrate proactivity from the Australian law makers, in commissioning reviews and being ahead of international best practice, compared the lacklustre reaction in the UK. The Australian reforms are limited, as the effect of the updated legislation is to simply apply existing AML regulation to cryptocurrency service

[216] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.5.
[217] ibid.
[218] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.6(2) Item 50A.
[219] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2019.
[220] GOV.UK, 'Digital currencies: response to the call for information' <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf> accessed 11 March 2016
[221] Financial Conduct Authority, 'Guidance on Cryptoassets: Feedback and Final Guidance to CP 19/3' (London, July 2019) <https://www.fca.org.uk/publication/policy/ps19-22.pdf> accessed 23 September 2019.
[222] GOV.UK, 'Digital currencies: response to the call for information' <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf> accessed 11 March 2016 at p.11.
[223] ibid.

providers, which indicates a lack of understanding of cryptocurrencies. The UK should follow the start that Australia has made in applying AML regulation to cryptocurrencies, which it is required to do by the EU's 5th Anti-Money Laundering Directive. [224]

7.7.3. Attorney General's Department

The Attorney General's Department (AGD) undertook a statutory review of the AML/CTF Act 2006 in 2016,[225] the subsequent report identified similar money laundering risks posed by cryptocurrencies, as those identified by the Senate Economics References Committee,[226] particularly that the AML/CTF Act 2006 did not regulate cryptocurrencies.[227] In light of the money laundering risks of cryptocurrencies, the AGD recommended that AUSTRAC monitored the risks posed by new payment methods, that the AML/CTF Act 2006 be amended to cover digital wallets and digital currencies not backed by a physical thing. The AGD also said that the Act should also be amended so as to include activities relating to digital currencies in the list of designated services.[228] The AGD made it clear that cryptocurrencies should be brought under the AML/CTF regime, but did differ from the Senate report on one detail,

[224] Council Directive 2018/843/EU 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 L 156/43 at para 53.
[225] Attorney General's Department, 'Report on The Statutory Review of The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 And Associated Rules and Regulations' (April 2016) <https://www.homeaffairs.gov.au/how-to-engage-us-subsite/files/report-on-the-statutory-review-of-the-anti-money-laundering.pdf>accessed 28 October 2019.
[226] Parliament of Australia, 'Digital Currency – Game Changer or bit player' (August 2015) <http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Digital_currency/~/media/Committees/economics_ctte/Digital_currency/report.pdf> accessed 21 October 2019.
[227] Attorney General's Department, 'Report on The Statutory Review of The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 And Associated Rules and Regulations' (April 2016) <https://www.homeaffairs.gov.au/how-to-engage-us-subsite/files/report-on-the-statutory-review-of-the-anti-money-laundering.pdf> accessed 26 July 2019 at p.45.
[228] ibid at p.50.

amending the definition of money. The AGD made no mention of the Senate Economics References Committee's recommendation to amend the definition of money, which would have caused cryptocurrencies to become one of the designated services of the AML/CTF Act 2006.[229] The AGD instead proposed an amendment of the definition of 'e-currency' in order to make AML measures applicable to cryptocurrency service providers. It can be seen from the 2017 amendments to the AML/CTF Act 2006, that instead of taking the AGD's suggestion, the term "*digital currency*"[230] has been inserted into the definitions section, which addresses the recommendation that digital currencies should be covered by the Act. The AGDs recommendation in relation to the inclusion of digital currency services being included on the list of designated services was followed, so digital currencies are now regulated by the Act. The AGD's role does not involve directly enforcing the law, its recommendations for reform have been implemented and it is AUSTRACs responsibility to regulate and enforce the AML/CTF 2006.

7.7.4. Australian Transaction Reports and Analysis Centre

AUSTRAC made submissions to the Senate Economics References Committee, providing advice on the risk they pose and the potential ways in which they may be regulated. AUSTRAC recognised the risks posed by digital currencies, but did not see digital currencies as such a threat that would see AUSTRAC demanding to government that "[i]*t is imperative that you give us sight over this."*[231] Similarly to the

[229] Anti-Money Laundering and Counter Terrorist Financing Act 2006 Part 1 s.6, Table 1.
[230] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.5.
[231] Parliament of Australia, 'Digital Currency – Game Changer or bit player' (August 2015) <http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Digital_currency/~/

AGD, AUSTRAC also told the committee that regulating cryptocurrencies would require legislative change, and that more was required than just changes to the regulations that AUSTRAC administer.[232] In light of the amendments to the AML/CTF Act 2006, cryptocurrency services are now the responsibility of AUSTRAC for AML regulation. AUSTRAC provide guidance to digital currency exchange businesses,[233] which is similar to the advice that is given to other regulated entities. Requirements include completing a risk assessment, training employees, complying with CDD requirements, and appointing an AML/CTF compliance officer who will be responsible for submitting SMRs and TTRs to AUSTRAC.[234] The 70% increase in SMRs sent to AUSTRAC are not attributable to including digital currency exchanges, as the changes were only implemented on 3rd April 2018, which would be less than half of the period covered by the 2017/18 report.[235] The strong enforcement actions by AUSTRAC against Commonwealth Bank of Australia and Tabcorp[236] may indicate a change in enforcement approach by AUSTRAC which could lead to larger fines in the future. In the UK the FCA has taken on the equivalent role to AUSTRAC from January 2020,[237]

media/Committees/economics_ctte/Digital_currency/report.pdf> accessed 21 October 2019 at para 6.30.

[232] ibid at para 6.29

[233] AUSTRAC, 'A guide to preparing and implementing an AML/CTF program for your digital currency exchange business' <https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/guide-preparing-and-implementing-amlctf-program-your-digital-currency-exchange-business> accessed 26 July 2019.

[234] ibid at p.3.

[235] AUSTRAC, 'AUSTRAC Annual Report 2017-18' <https://www.austrac.gov.au/sites/default/files/2019-05/AUSTRAC_annual_report_2017-18.pdf> accessed 24 July 2019.

[236] The Commonwealth Bank of Australia and Tabcorp were sanctioned with large fines for money laundering failings: Chief Executive Officer of Australian Transaction Reports and Analysis Centre v TAB Limited (No 3) [2017] FCA 1296, Chief Executive Officer of the Australian Transaction Reports and Analysis Centre v Commonwealth Bank of Australia Limited [2018] FCA 930, and P Durkin, '70pc jump in suspicious money laundering transactions: AUSTRAC' Financial Review (Melbourne, 18 October 2018) <https://www.afr.com/business/banking-and-finance/70pc-jump-in-suspicious-money-laundering-transactions-austrac-20181018-h16szs> accessed 24 July 2019.

[237] HM Government 'Economic Crime Plan' (12 July 2019) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/816215/2019-22_Economic_Crime_Plan.pdf> accessed 23 October 2019 at 4.9.

and could observe the approach taken by AUSTRAC, and assist newly regulated entities in a similar way to the guidance issued by AUSTRAC.[238] AUSTRAC has been praised by the FATF for its management of intelligence,[239] and based on the recommendation of Irwin and Turner, AUSTRAC should lead a more joined up approach for cryptocurrencies, as it is best placed to implement "*information sharing between multiple stakeholders from the law enforcement, financial intelligence units, cyber security organisations and fintech industry.*"[240]

7.7.5. Australian Criminal Intelligence Commission

The Australian Criminal Intelligence Commission (ACIC) is a not a recognised member of the Australian Intelligence Community, but it is the national criminal intelligence agency of Australia.[241] In ACIC has a number of projects, which are investigating and gathering information on cryptocurrencies, but the issue is not being addressed by a dedicated body. In its 2017-18 Annual Report, the ACIC reported that it had made presentations on cryptocurrencies as part of 'Project Longstrike',[242] claimed to have improved intelligence and understanding of cryptocurrencies as part of 'Project Whitebeam',[243] and produced "*intelligence products*"[244] on the "*use of bitcoin as an*

[238] AUSTRAC, 'A guide to preparing and implementing an AML/CTF program for your digital currency exchange business' <https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/guide-preparing-and-implementing-amlctf-program-your-digital-currency-exchange-business> accessed 26 July 2019.
[239] Financial Action Task Force, 'Australia – Mutual Evaluation Report – April 2015' <http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Report-Australia-2015.pdf> accessed 05 September 2019 at p8.
[240] cf Irwin and Tuner (n111) at 310.
[241] Australian Crime Intelligence Commission, 'About Us' <https://www.acic.gov.au/about-us> accessed 29 July 2019.
[242] Australian Crime Intelligence Commission, 'Australian Criminal Intelligence Commission Annual Report 2017-18' <https://acic.govcms.gov.au/sites/g/files/net3726/f/acic_2017-18_ar_digital.pdf?v=1539748074> accessed 29 July 2019 at p.25.
[243] ibid at p.27.
[244] ibid at p.86.

alternative to traditional money laundering" as part of 'Project Cryogenic'.[245] Reporting from ACIC is too vague to draw conclusions from; the intelligence the ACIC gather is sensitive, so unlikely to be shared. The role of the ACIC is to work with "*state and territory, national and international partners on investigations and to collect intelligence to improve the national ability to respond to crime impacting Australia.*"[246] The role of the ACIC is comparable to the NCA in the UK, which has had some successes in pursuing money launderers who use cryptocurrencies.[247] Also comparable to the NCA, the broad nature of the ACIC's role means their focus and resources are not targeted solely towards cryptocurrencies and money laundering.

7.8. Compliance with Financial Action Task Force guidance

Australia's most recent mutual evaluation from the FATF predates the 2019 FATF guidance on virtual assets. It would not be appropriate to expect full compliance with FATF guidance so soon after the publication of the guidance, but it is helpful to consider to what degree Australia is already compliant. The FATF uses different terminology to Australia. The FATF use the term 'virtual asset' (VA), which is defined as a "*digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes.*"[248] Australia uses the term "*digital currency*",[249] but the definition in the AML/CTF Act 2006 would satisfy the FATF term

[245] ibid at p.87.
[246] Australian Crime Intelligence Commission, 'About Us' <https://www.acic.gov.au/about-us> accessed 29 July 2019.
[247] National Crime Agency, 'Student behind $100m dark web site jailed for 5 years 4 months' (12 April 2019) <https://www.nationalcrimeagency.gov.uk/news/student-behind-100m-dark-web-site-jailed-for-5-years-4-months?highlight=WyJiaXRjb2luIiwiYml0Y29pbnMiXQ==> accessed 11 September 2019.
[248] Financial Action Task Force, 'Guidance for A Risk-Based Approach to Virtual Currencies' <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf> accessed 01 August 2016, para 33 at p13.
[249] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.5: Digital Currency.

'virtual asset'. The FATF guidance also uses the term 'Virtual Asset Service Provider' (VASP),[250] to describe businesses providing services for cryptocurrency users. Australia uses the terms "*registered digital currency exchange provider*"[251] and "*registrable digital currency exchange service*"[252] to describe cryptocurrency service providers. While the FATF and Australia use different terms, the definitions of the terms are similar, and the Australian definitions will be compliant with the FATF guidance. The FATF guidance addresses the majority of the 40 Recommendations, stating that "[a]*lmost all of the FATF Recommendations are directly relevant*"[253] to addressing the money laundering risks posed.

Recommendation 1 concerns countries undertaking a risk assessment and applying the risk-based approach.[254] The 2019 guidance states that money laundering risk assessments should now include VAs and VASPs. The assessment should identify the relevant authorities that should regulate VAs and VASPs, and the treatment of these products and services should be consistent.[255] Australia has been including VAs and VASPs in a number of annual reports, the ACIC have included comments on VAs

[250] Financial Action Task Force, 'Guidance for A Risk-Based Approach to Virtual Currencies' <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf> accessed 01 August 2016, Acronyms at p3.
[251] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.5.
[252] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.5.
[253] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2019 para 55 at p19.
[254] See Recommendation 1 and the relevant explanatory note: Financial Action Task Force, 'The FATF Recommendations' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> accessed 04 September 2019.
[255] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2019 para 58 at p19.

in both of its annual reports,[256] and AUSTRAC have included VAs and VASPs in their annual report of 2017-18.[257]

The FATF Recommendations advise that countries should consider all "*funds or value-based terms in the Recommendations, such as "property," "proceeds," "funds," "funds or other assets," and other "corresponding value," as including VAs*."[258] Australia has not amended its criminal offences to explicitly include VAs, but the existing legislation is drafted so widely that the law will apply to VAs. As discussed at 7.3, the Criminal Code defines property as: "*real or personal property of every description, whether situated in Australia or elsewhere and whether tangible or intangible, and includes an interest in any such real or personal property.*"[259] This definition is very broad and it is difficult to envisage anything failing to satisfy it; cryptocurrencies are intangible and impossible to possess but the inclusion of "*interest in*"[260] means that anything of value may be included. The wide definition means that Australia would be compliant with FATF Recommendations 3, 4, and 5, pertaining to criminalisation of money laundering,[261] confiscation of criminal proceeds,[262] and terrorist financing.[263] Australia

[256] Australian Crime Intelligence Commission, 'Australian Criminal Intelligence Commission Annual Report 2017-18' <https://acic.govcms.gov.au/sites/g/files/net3726/f/acic_2017-18_ar_digital.pdf?v=1539748074> accessed 29 July 2019 examples at p.25, 27 and 86 and Australian Crime Intelligence Commission, 'Australian Criminal Intelligence Commission Annual Report 2016-17' <https://acic.govcms.gov.au/sites/g/files/net1491/f/acic_2016-17_annual_report.pdf?v=1508387578> accessed 29 July 2019 at p119.
[257] AUSTRAC, 'Annual Report 2017/18' <https://www.austrac.gov.au/sites/default/files/2019-05/AUSTRAC_annual_report_2017-18.pdf> accessed 29 July 2019 examples at p.8, 11 and 26.
[258] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2019 para 65 at p20.
[259] Criminal Code Act 1995 Subdivision 400.1(1).
[260] ibid.
[261] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2019 para 66 at p21.
[262] ibid at para 67 at p21.
[263] ibid at para 69 at p21.

would also be compliant for Recommendation 6 which concerns asset freezing,[264] but this is usually impossible for cryptocurrencies, and Recommendation 7 which relates to sanctions,[265] which again are difficult to enforce in relation to cryptocurrencies.

The 2019 FATF guidance also recommends that VASPs are covered by AML regulation, which Australia has already achieved as the term 'digital currency' has been added the definitions in the AML/CTF Act 2006.[266] Additionally, the terms "*registered digital currency exchange provider*"[267] and "*registrable digital currency exchange service*" have been added to the Act.[268] The 2017 amendments brings VAs and VASPs into the regulatory remit of AUSTRAC, making Australia compliant with Recommendations 26 and 27, in accordance with the 2019 FATF guidance.[269] By being subject to AUSTRAC supervision, VASPs are required to complete CDD processes, so Recommendation 10 is adopted in line with the 2019 guidance,[270] and AUSTRAC provide advice to newly regulated businesses on how to comply with their obligations.[271] VASPs being regulated entities means such businesses are required to

[264] ibid at para 70 at p21.
[265] ibid.
[266] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.5: Digital Currency.
[267] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.5.
[268] ibid.
[269] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2019 para 86 at p23.
[270] ibid at para 91 at p24.
[271] AUSTRAC, 'A guide to preparing and implementing an AML/CTF program for your digital currency exchange business' <https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/guide-preparing-and-implementing-amlctf-program-your-digital-currency-exchange-business> accessed 26 July 2019.

have risk management systems in place,[272] comply with reporting requirements,[273] and share information with AUSTRAC as the FIU of Australia.[274]

As identified at 7.6.2, AUSTRAC is the FIU of Australia, and it is responsible for the enforcement of the AML/CTF Act 2006, which, in light of the 2017 amendments, includes cryptocurrency service providers. AUSTRAC publish annual reports detailing the number of reports they receive, and these reports now include those from digital currency service providers, this makes Australia compliant with the 2019 FATF guidance on implementing Recommendation 33. In summary, Australia can be seen to be ahead of international best practice, legislating in 2017 and already being compliant with the FATF guidance of 2019.

7.9. Recommendations for the United Kingdom

Australia has taken a different approach to criminalising money laundering compared to the UK, but the contrasting approaches achieve similar effects. There are no plans for the UK to reform its money laundering offences, and therefore it is not likely that the UK will adopt the scaling model used in Australia. A fundamental difference between the UK and Australia is seen in the way penalties are imposed, the penalty point system is something which is peculiar to Australia, and there is nothing to indicate

[272] As stipulated in the AUSTARC guidance: AUSTRAC, 'A guide to preparing and implementing an AML/CTF program for your digital currency exchange business' <https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/guide-preparing-and-implementing-amlctf-program-your-digital-currency-exchange-business> accessed 26 July 2019. In compliance with FATF guidance in applying Recommendation 12: Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2019 para 104 at p27.
[273] ibid at para 124 at p31.
[274] ibid at para 129 at p32.

that the UK would seek to adopt this. The penalty point system is implemented across criminal law in the majority of Australian territories, and it would require extensive reform for the UK to adopt. The differing values of a penalty unit across Australia raises concerns in relation to fairness, which are not the focus of this thesis.

The AML regulation in Australia, much like the AML regulation of the US, is similar to that of the UK, with the exception of threshold reporting, which the UK does not enforce, instead the UK focuses on suspicious activity reporting. Also like the comparison between the UK and the US, the differences with regard to cryptocurrency service providers are stark, as the UK does not currently impose AML regulation on cryptocurrency service providers, whereas Australia does, this will change once the deadline for cryptocurrency service providers to register with the FCA passes in January 2021.

Australia enforces similar AML regulation to the US with regards to cryptocurrency service providers, and both jurisdictions are compliant with the latest FATF guidance, but the routes taken to regulate cryptocurrency service providers were different. While the approach of FinCEN in the US negated the need for legislative reform, by declaring that cryptocurrency exchanges and administrators were too be viewed as money services businesses and needed to comply with AML regulation,[275] the Australian approach has been to legislate. Australia has been efficient in its legislative reform, by

[275] FinCEN, 'Guidance - FIN-2013-G001 - Issued: March 18, 2013 - Subject: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies' <https://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf> accessed 06 August 2019 at p2.

amending of the Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2006 in 2017.[276] The 2017 amendment inserted "*digital currency*",[277] "*registered digital currency exchange provider*",[278] and "*registrable digital currency exchange service*"[279] to the 2006 Act. The list of designated services which are regulated by the 2006 Act now covers cryptocurrency exchange services,[280] and AUSTRAC is responsible for enforcing AML regulation. The UK has not created or amended its own legislation to cover cryptocurrencies, as observed in chapter five. The UK Parliament has passed comparably few Acts in the past decade and has been distracted by the withdrawal from the EU. While UK legislators have been idle, the EU has passed the 5th Anti-Money Laundering Directive,[281] which addresses cryptocurrencies and requires Member States to apply AML regulation to cryptocurrency service providers. Other than making the FCA responsible for the AML regulation of cryptocurrency businesses, it is unclear how the UK intends to implement the Directive, but by regulating cryptocurrency service providers, the UK will have taken a similar approach to Australia and bring the UK in line with international best practice as set out by the 2019 FATF guidance.[282]

[276] Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017.
[277] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.5.
[278] ibid.
[279] ibid.
[280] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.6(2) Item 50A.
[281] Council Directive 2018/843/EU 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 L 156/43.
[282] Financial Action Task Force, 'Guidance for A Risk-Based Approach to Virtual Currencies' <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf> accessed 01 August 2016.

As with the US, although Australia is compliant with FATF guidance, the regulation of cryptocurrencies is not covering peer-to-peer transactions within individual cryptocurrency networks, which is where the majority of cryptocurrency transactions take place. The quality of the financial intelligence gained through regulating cryptocurrency service providers should be supported by monitoring the blockchain. Traditional AML measures cannot be applied to blockchain transactions, as there is no human involvement, except for the two transacting parties, but by utilising blockchain APIs, automated analysis of the blockchain could be implemented.[283] At present it is not clear if the financial intelligence available through the blockchain is being used for AML purposes, but it is a valuable resource that all jurisdictions should utilise

It is recommended that the UK retains its current money laundering offences as the UK criminal law is not compatible with the format adopted by Australia. The UK Parliament and the FCA should make it clear how the 5th Anti-Money Laundering Directive will be implemented, but meeting the current international standards alone is not enough. It is recommended that the UK goes further than the Australia, and monitors the blockchains of cryptocurrencies, so as to avoid a significant number of transactions taking place outside of the financial system, without regulatory scrutiny.

[283] Examples can be found at Blockchain Luxembourg, 'Bitcoin Developer APIs' <https://www.blockchain.com/api> accessed 26 September 2019.

7.10. Chapter Summary

Australia has addressed money laundering in accordance with international best practice, it is compliant with core Recommendations of the FATF by criminalising money laundering and implementing preventative measures. When compared to the approach of the US, Australia's offences take a notably different form, but achieve the same effect. Laundering money using cryptocurrencies will satisfy the money laundering offences without the need for reform, no new gap in the law has been created with regards to the criminal offences. A further difference noted between Australia and the US is that while the US prescribes maximum fines in US$, Australia has instead developed a penalty points system. The use of penalty points appears more complicated than simply designating fines, but it is clear that this system better future proofs money laundering offences as fines can be raised in accordance with inflation by raising the value of a penalty point, rather than having to amend each law.

With regard to preventative measures, again, Australia is in line with international standards, the FATF Recommendations are followed, and similarities are seen between the Australian approach and the US one. As in the US, Australia requires regulated entities to submit reports on both suspicious activity and transactions over a specified threshold. It is noted that the number of SARs submitted in Australia has risen sharply in 2018, potentially due to strong enforcement action from Australian regulators. Australia adopts a single regulator approach to AML, with AUSTRAC being responsible for enforcing the AML/CTF Act 2006, this is a much simpler approach compared to the US which adopts a multi-regulator approach. Despite the recent high-profile fines of Common Wealth Bank of Australia and Tabcorp, the fines imposed by

the US dwarf those figures, such as the fine of over US$1bn against Standard Chartered in April 2019.[284]

Australia has been proactive in reforming its AML/CTF legislation to cover the emergence of cryptocurrency service providers. The 2017 amendments have widened the scope of the AML/CTF Act 2006 to cover cryptocurrency services providers, this has been achieved in a succinct manner by inserting new definitions and followed a clear consultation period. The weaknesses of the amendments are that the coverage remains at the fringes of cryptocurrency networks. While the legislation is in line with the guidance of the FATF, it shows a limitation in the understanding of cryptocurrencies, as observed in chapter four.[285] The public ledgers which cryptocurrencies produce should be utilised to be able to dovetail with the intelligence being gathered through regulated entities. As recommended by Irwin and Turner, a more joined up approach is required for cryptocurrencies,[286] with "*information sharing between multiple stakeholders from the law enforcement, financial intelligence units, cyber security organisations and fintech industry.*"[287] AUSTRAC are the best placed authority to implement such an approach in Australia.

It has been noted that Australia has seen an upsurge in SMRs, which will more likely rise further as the regulation is applied to a new sector. Given the existing concerns

[284] United States Department of Justice, 'Standard Chartered Bank Admits to Illegally Processing Transactions in Violation of Iranian Sanctions and Agrees to Pay More Than $1 Billion' <https://www.justice.gov/opa/pr/standard-chartered-bank-admits-illegally-processing-transactions-violation-iranian-sanctions> accessed 05 August 2019.
[285] See chapter four and 4.10.3.
[286] cf Irwin and Tuner (n111) at 310.
[287] ibid.

over defensive reporting, it is not unforeseeable that regulated cryptocurrency exchanges will produce a high volume of reports due to their services satisfying the characteristics of being high-risk under the risk-based approach, and due to the fear of high fines for compliance failings. By expanding the AML measures to cryptocurrency service providers, CDD is now required, which is potentially problematic as the majority of customers will be using services remotely. The weaknesses of CDD have been highlighted, particularly that it is relatively easy for service users to give false details; this becomes even easier in remote transactions and with the pseudonymous nature of cryptocurrencies.

In conclusion, Australia has reacted to the development of cryptocurrencies in line with international best practice and has taken proactive steps to regulate this developing area. AUSTRAC provides a good comparison to the UK Financial Conduct Authority, as both are the sole enforcers of AML in their jurisdictions. The UK can learn from the Australian approach, both in its strengths in the succinct reform of the law, and in its weaknesses in relation to utilising the wealth of information available on public ledgers.

Chapter 8. Conclusions and Recommendations

The question this thesis seeks to answer is:

> How can the UK learn from international guidance and the approaches of the United States and Australia to address the money laundering risks posed by cryptocurrencies?

The aim of this research is to analyse cryptocurrencies, specifically the legal understanding of cryptocurrencies, and to assess how the money laundering risks should be addressed. This thesis argues that a tailored approach is needed towards the regulation, and monitoring of cryptocurrencies, and that simply transposing existing regulations onto cryptocurrencies will not be effective.

This chapter sets out the findings from this research, cryptocurrencies are identified, and it is recommended that the United Kingdom (UK) adopts the term cryptocurrencies, instead of cryptoassets. It is observed that the United Nations (UN) has been overtaken by the Financial Action Task Force (FATF) and the European Union (EU) in the setting of model anti-money laundering (AML) legislation, this change in international leadership took place in the 1990s and 2000s as the FATF and EU became more prescriptive and the UN focussed on its wider aims. It is recommended that the UK implements the 5th EU Anti-Money Laundering Directive, and in the process adheres to FATF guidance, but it is suggested that the UK goes further than the current international best practice as peer-to-peer transactions remain unregulated. The UK could adopt either a regulator led, or legislator led widening of the regulatory perimeter, but it is unlikely the Financial Conduct Authority (FCA) will take the same proactive steps that the Financial Crime Enforcement Network

(FinCEN) has in the US. Therefore, the UK will take a legislator led approach, such as the approach of Australia, to widening the regulatory perimeter to cover cryptocurrencies, as it implements the 5th EU Anti-Money Laundering Directive.

The UK has been lacklustre in its response to cryptocurrencies, but it is advised that it goes further than its contemporaries and addresses the regulatory gaps present in existing regulation of cryptocurrencies. The wealth of data available from the blockchain is being ignored, so developing technology and utilising application programming interfaces (APIs) is needed in order to employ the data for AML purposes.

8.1. Defining cryptocurrencies

Cryptocurrencies are best identified by the FATF as part of their typology of virtual currencies. Cryptocurrencies are decentralised convertible virtual currencies, and in order for them to be decentralised, they operate based on the Bitcoin model of a distributed ledger. Figure 14 demonstrates that all virtual currencies can be placed within a grid of 4 squares, where the columns are a choice between centralised or decentralised and the rows denote the convertibility of the virtual currency. Fiat currencies are not included in the grid as they are not solely virtual, but if they were to be included they would be centralised convertible currencies as they are administrated by a central bank.

Figure 14. FATF Categories of Virtual Currency[1]

	Centralised	Decentralised
Convertible	Linden Dollars (used in Second Life) are an example of a convertible virtual world currency; users may exchange their currency for US Dollars. The currency is centralised, Linden Labs (the developer of Second Life) act as administrators.	Examples of decentralised currencies include Bitcoin and Dogecoin. These are convertible for fiat currency but not controlled by a central administrator.
Non-Convertible	World of Warcraft (WoW) gold is non-convertible virtual world currency; users may not convert this into a fiat currency. WoW gold is controlled by the game developers, Blizzard	None exist.[2]

8.1.1. Cryptocurrencies Distinguished from Money

Money is not a fixed concept, as it develops over time, and its form has changed from physical to electronic. *Moss v Hancock*[3] clearly seeks to define money by its functions, of which the law is primarily concerned with the medium of exchange function. Socio-

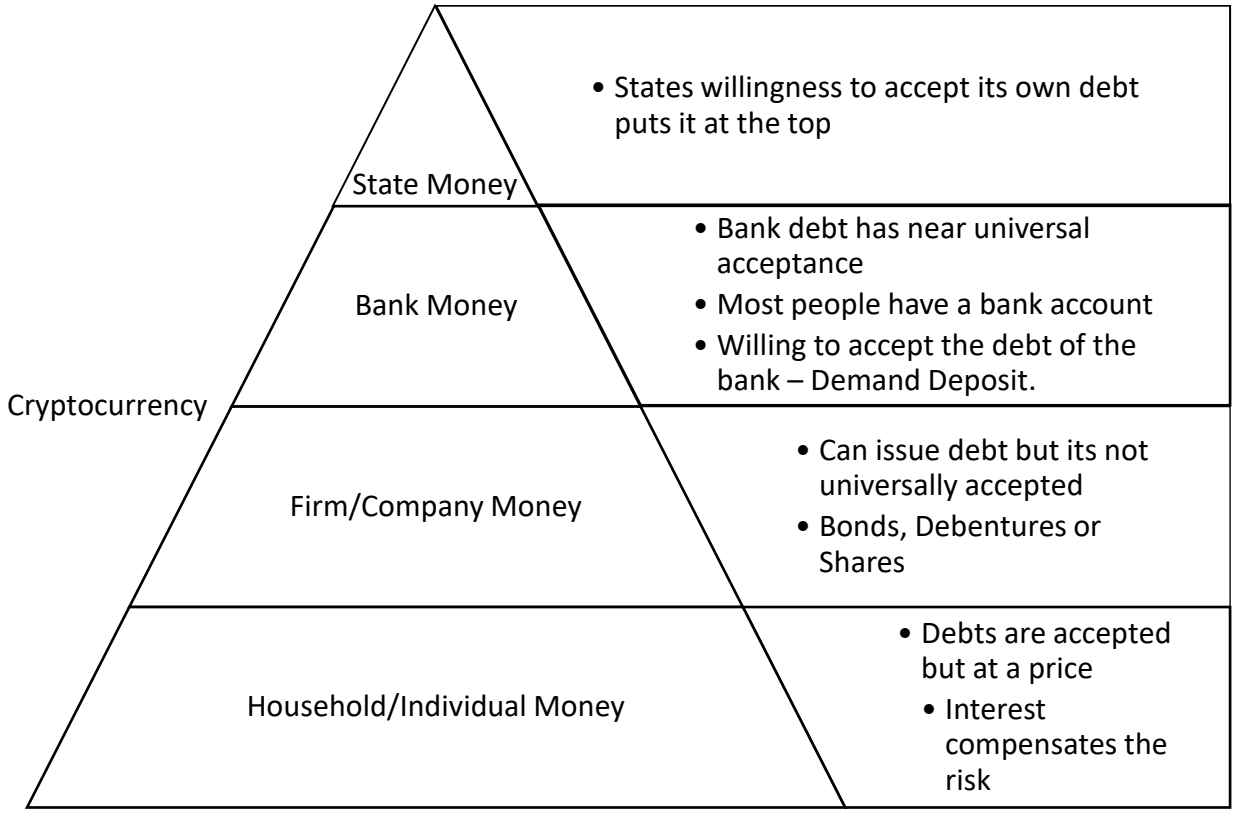
[1] Financial Action Task Force, 'Virtual Currencies – Key Definitions and Potential AML/CFT Risks' <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 27th November 2014.
[2] ibid.
[3] [1899] 2 QB III.

economics recognises medium of exchange as the main function, but also considers money as a store of value and a unit by which value is determined. The function-based approach adopted by the law allows it to be flexible, and the law does not prescribe what money is, and as such cryptocurrencies may have the potential to become money. However, at present the fluctuations in the value of cryptocurrencies, and their treatment by users as an investment vehicle rather than as a medium of exchange, means that cryptocurrencies are not currently viewed as money in the same way as fiat money.

As cryptocurrencies do not satisfy all of the functions of money, it is difficult to conclude that they are money in same way as fiat money is money. Cryptocurrencies can be placed on Bell's hierarchy of money.[4] Instead of cryptocurrencies being viewed as highly as 'State Money', it is more likely that by satisfying some of the functions of money, cryptocurrencies sit lower on the hierarchy, as shown in Figure 15.

[4] See chapter three at 3.4.3 for a discussion of Bell's hierarchy.

Figure 15. Placing Cryptocurrency on Bell's Hierarchy of Money[5]



Cryptocurrencies have no state to act as the driver of the money, and there are no state debts to pay with cryptocurrencies. Cryptocurrencies are best placed as either company money or bank money. Cryptocurrencies could be considered a company money of relatively high liquidity, or a bank money with comparably low liquidity; with the potential to become as usable as other bank money if acceptability increases. It is helpful to determine the nature of cryptocurrencies against existing concepts, but the most important issue for this thesis is how they are treated by regulators. In order for regulation to be consistent, the terminology used should be harmonized to ensure each regulator is clear in what they are referring to.

[5] Produced based on: S. Bell, 'The Role of the State and the Hierarchy of Money' (2001) 25 Cambridge Journal of Economics 149.

8.1.2. Terminology

Confusion exists as to the accepted terminology to use when referring to cryptocurrencies, with a number of different terms being used by international and supranational organisations, such as the FATF and the EU, and nationally by the UK, the US, and Australia. This thesis recommends the term 'cryptocurrencies' as this term specifically refers to exclusively digital virtual currencies, which operate based on cryptography as a decentralised network using a distributed ledger. The term 'virtual assets', used by the FATF, is too broad as the term could also include virtual currencies which are centralised, and can be regulated through regulation of that central authority. Cryptocurrencies are a specific subset of virtual currencies, which require unique AML measures due to their decentralised nature, level of anonymity, and monetary value. The EU uses the term 'virtual currencies' and Australia uses the term 'digital currency',[6] both of which suffer from the same shortcomings of the FATF term, as they do not sufficiently define cryptocurrencies. The agencies of the US also predominantly use the term 'virtual currencies',[7] but the terminology used by the various authorities in the US is not consistent.

8.1.3. Recommendations for the UK

The lack of consistency in the terminology used to refer to cryptocurrencies is unhelpful as it can lead to confusion as to exactly what each term covers. The UK uses

[6] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.5.
[7] As demonstrated throughout the GAO report on in 2014: United States Government Accountability Office, 'Virtual Currencies: Emerging Regulatory, Enforcement, and Consumer Protection Challenges' <http://gao.gov/assets/670/663678.pdf> accessed 04 September 2019. The term is also used by FinCEN: FinCEN, 'Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies' (9 May 2019) <https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf> accessed 04 September 2019. The CFTC refer to Bitcoin directly, but also use the term: CFTC, 'Bitcoin and Other Virtual Currencies' https://www.cftc.gov/Bitcoin/index.htm> accessed 04 September 2019.

the term ‘cryptoassets’,[8] yet another variation on the terms used by the FATF, the EU, the US, and Australia, and potentially adds to the confusion. The term ‘assets’ appears deliberate as the FCA does not accept cryptocurrencies as currency or money.[9] The term ‘cryptocurrencies’ is the best term to use, as this specifically refers to decentralised convertible virtual currencies, which is the class of virtual currencies which pose a money laundering risk, as accepted by all of the organisations and jurisdictions considered in this thesis.

8.2. International Anti-Money Laundering Landscape

An analysis of the history and development of AML measures reveals a change in leadership with regard to international best practice. From the 1960s until the late 1980s the UN was the leading international body tackling money laundering and setting accepted minimum standards for legislation. The efforts of the UN were intertwined with its attempts to curtail the international drugs trade.[10] Since the creation of the FATF in 1989, the UN has taken a much less prominent role in combatting money laundering, as the FATF has assumed the role of leading international best practice. The FATF has a clearer AML focus than the UN, the FATF was created “*in response to mounting concern over money laundering*”[11] among the G7,[12] and was solely concerned with the money laundering “*threat posed to the banking system and to financial institutions*.”[13] The FATF and its Recommendations demonstrate a shift

[8] Financial Conduct Authority, ‘Guidance on Cryptoassets – Consultation Paper’ <https://www.fca.org.uk/publication/consultation/cp19-03.pdf> accessed 19 March 2019 at 2.3.
[9] ibid at 2.7.
[10] See chapter four and 4.7. and N. Ryder, *Financial Crime in the 21st Century: Law and Policy* (Edward Elgar, Cheltenham, 2011) at p.15.
[11] Financial Action Task Force, ‘History of the FATF’ <http://www.fatf-gafi.org/about/historyofthefatf/> accessed 27 September 2019.
[12] ibid.
[13] ibid.

away from the drugs trade, and towards treating money laundering as a standalone issue. The FATF has taken on counter terrorist financing as part of its mission, but it remains more focussed on money laundering than the UN, which has much broader aims.

The FATF is not alone in setting AML best practice, it is joined by the EU which, in its various forms, has been developing its AML standards since the 1970s.[14] The EU's recommendations in 1980 were ahead of their time, but, unfortunately, were not utilised.[15] Despite this, the EU has promoted the harmonisation of AML regulation across Member States, the latest example of this is the 5th Anti-Money Laundering Directive which came into force in January 2020. The EU is a prominent international organisation developing AML standards, and is able to enforce compliance with its AML legislation across Member States. The FATF does not have sanctioning powers, but it has utilised blacklisting to promote compliance with its Recommendations. While the UN began the global AML fight, it is clear that the EU and the FATF have been the leading forces in developing international best practice and enforcing standards in recent decades.

8.2.1. Recommendations for the UK

The UK has ratified all of the relevant UN conventions relating to money laundering, it is also compliant with the 4th Anti-Money Laundering Directive and largely compliant

[14] N. Ryder, *Money laundering – an endless cycle? A comparative analysis of the anti-money laundering policies in the United States of America, the United Kingdom, Australia and Canada* (Routledge, London, 2012) at p.18.
[15] W. Gilmore, *Dirty Money – The Evaluation of International Measures to Counter Money Laundering and the Financing of Terrorism* (Council of Europe, Brussels, 2004) at p161.

with the FATF Recommendations, as identified in the most recent mutual evaluation report.[16] The UK has implemented the 5th Anti-Money Laundering Directive, and once the reforms come into force, it will be compliant with the latest guidance from the FATF. It is recommended that the UK continues to keep pace with international standards, but that the UK does not simply meet the minimum regulation of cryptocurrencies required by the FATF and the EU. Instead, the UK should seek to address the gaps left by the model legislation of the FATF and the EU. The UK should harness the wealth of data within the distributed ledgers of cryptocurrencies and use this to assist its FIU in detecting money laundering. There are promising developments in this area as in January 2020 the Regulatory Policy Committee approved the UK transposition of the 5th Anti-Money Laundering Directive as fit for purpose, and noted that the UK was going beyond the minimum requirements.[17] The FCA will regulate businesses which conduct cryptocurrency-to-cryptocurrency exchanges, as well as cryptocurrency-to-fiat currency exchanges. While promising, enforcement remains to be seen; the deadline for relevant businesses to register with the FCA is January 2021.

8.3. Money Laundering Offences

Cryptocurrencies present a problem for the application of existing AML measures, but the criminalisation of money laundering in the UK, the US and Australia effectively

[16] FATF, 'Anti-money laundering and counter-terrorist financing measures – United Kingdom, Fourth Round Mutual Evaluation Report' (Paris, December 2018) <fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-Kingdom-2018.pdf> accessed 11 September 2019.

[17] Regulatory Policy Committee, 'Transposition of the Fifth Anti-Money Laundering Directive HM Treasury' (London, 16 January 2020) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/863735/2020-01-16-RPC-HMT-4432_1_-Transposition_of_the_Fifth_Anti-Money_Laundering_Directive.pdf> accessed 28 July 2020.

covers the use of cryptocurrencies. Definitions of cryptocurrencies vary against existing assets, property, and money, but the offences in each jurisdiction are drafted broadly to apply to all proceeds of crime. Although the applicability of money laundering offences is clear, how to process confiscated cryptocurrencies presents three clear issues; accessing the cryptocurrencies in a criminal's wallet, determining how to covert the cryptocurrency into fiat currency, and the changes in the value of the cryptocurrency in the length of time from confiscation to conversion. Successful confiscation has largely been due to circumstantial luck, such as freezing the cryptocurrency assets of an individual having caught them with their "*fingers on the keyboard*"[18] in the case of *West*. A likely method of seizing illicit cryptocurrency, which was also used against West, is to use a court order requiring the convicted individual to give up the cryptocurrency or face further jail time.[19] Once the cryptocurrency is confiscated there are currently two options for authorities wishing to convert the currency, they can either use a cryptocurrency exchange or sell the cryptocurrency at public auction. Hall observes that the US approach is to use public actions, whereas Dutch authorities use exchanges.[20] The third issue is more pertinent due to the volatility in the value of cryptocurrencies, it is seen in chapter five at 5.3.2 that the UK experience in this has been positive, but the fluctuations in value mean that it would be highly likely that future seizures of cryptocurrency could be worth far less at the time of conversion than at the time of seizure.

[18] Mattha Busby, 'Bitcoin worth £900,000 seized from hacker to compensate victims' The Guardian (London, 23 August 2019).
[19] ibid.
[20] J Hall, 'Restraint orders: R. v Teresko (Sergejs) Kingston Crown Court: HH Judge Lodder QC: unreported 11 October 2017' (2018) 1 CLR 81 at 82.

8.3.1. Recommendations for the UK

The UK money laundering offences do not require reform for the purpose of applying to cryptocurrencies, the drafting of the offences is wide enough to obtain convictions, as demonstrated by the prosecutions of *Teresko*,[21] *White*,[22] and *West*.[23] The UK approach with regards to converting confiscated cryptocurrency is inconsistent; in the *Teresko* case an exchange was used,[24] but in 2019 a UK police force used the public auction method for the first time.[25] It is recommended that the UK processes cryptocurrency seizures faster so as to be able to realise the value of the confiscated goods at the correct value, however it is currently unclear which method of conversion is preferred.

8.4. Applying Anti-Money Laundering Regulation to Cryptocurrencies

Australia and the US demonstrate that regulation of cryptocurrency service providers is possible, and adapting an AML approach to include cryptocurrency service providers can be achieved in a timely fashion. Both jurisdictions have widened their AML regulation to require cryptocurrency service providers to adhere to customer due diligence and reporting requirements, and shown that cryptocurrency service

[21] Crown Prosecution Service, 'More than £1.2million of Bitcoin seized from drug dealer' (19 July 2018) <https://www.cps.gov.uk/south-east/news/more-ps12-million-bitcoin-seized-drug-dealer> accessed 11 September 2019.
[22] BBC News, 'Liverpool 'dropout' jailed for Silk Road dark web site' (12 April 2019) <https://www.bbc.co.uk/news/uk-england-merseyside-47913780> accessed 11 September 2019 and National Crime Agency, 'Student behind $100m dark web site jailed for 5 years 4 months' (12 April 2019) <https://www.nationalcrimeagency.gov.uk/news/student-behind-100m-dark-web-site-jailed-for-5-years-4-months?highlight=WyJiaXRjb2luIiwiYml0Y29pbnMiXQ==> accessed 11 September 2019.
[23] BBC News, 'Prolific Sheerness hacker ordered to pay back £922k' (23 August 2019) <https://www.bbc.co.uk/news/uk-england-kent-49450676> accessed 24 September 2019.
[24] cf Hall (n20) at 82.
[25] Wilsons Auctions, '£500k of bitcoin seized from UK criminal to be auctioned, with no reserve!' (19 September 2019) <https://www.wilsonsauctions.com/news/500k-of-bitcoin-seized-from-uk-criminal-to-be-auctioned-with-no-reserve/> accessed 30 September 2019.

providers can be regulated in the same way as traditional financial institutions. Though the end result has been the same in both jurisdictions, they have each taken a different method to developing their AML regulation. In the US, FinCEN has taken the lead in a regulatory led widening of the regulatory perimeter, compared to Australia where Parliament has delivered a legislator led widening of the regulatory perimeter.

8.4.1. Regulator Led Widening of the Regulatory Perimeter

A regulator can widen its regulatory perimeter by the way it chooses to interpret definitions in existing legislation. FinCEN did this in 2013, as it determined that cryptocurrency exchanges and administrators were to be viewed as money services businesses, and therefore need to comply with AML regulation.[26] The FinCEN guidance was clear that while a regular user will not be subject to FinCEN regulation,[27] exchanges and administrators would need to comply with FinCEN regulation.[28] A similar approach could be implemented in the UK if Regulation 3 of the Money Laundering Regulations[29] were to be interpreted differently by the FCA. Under the Money Laundering Regulation 2017 a 'money services business' is an "*an undertaking which by way of business operates a currency exchange office, transmits money (or any representations of monetary value) by any means or cashes cheques which are made payable to customers.*"[30] Were the FCA to take the approach of FinCEN, and determine that cryptocurrency service providers satisfy this definition, then AML

[26] FinCEN, 'Guidance - FIN-2013-G001 - Issued: March 18, 2013 - Subject: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies' <https://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf> accessed 06 August 2019 at p2.
[27] ibid.
[28] ibid.
[29] Money Laundering Regulations 2017, Regulation 3.
[30] ibid, Regulation 3(1)(d).

regulation could, and should, have been implemented in a similar way to the regulation in the US. The UK has considered the US approach in 2015 as part of a public consultation, in which respondents were positive about the increased legitimacy regulation brings and the deterrence of crime.[31]

Criticisms of the US approach, and with it the regulator led approach, were made in relation to a perceived "*lack of clarity about which categories of business activity are captured by the FinCEN requirements, and some said that the process of registering in multiple American states has been burdensome and has forced smaller firms to exit the market*."[32] The issue of state regulation is not applicable to the UK, but the concerns over clarity are relevant, and indicate an issue with the ad hoc nature of regulator led regulatory changes. A regulator is likely to be reactive, and the changes may be piecemeal rather than planned and formalised. It is clear that a cryptocurrency exchange is a money services business, but wallets are more complicated, and Bitcoins can be stored privately offline. It is also unclear when an individual is no longer an individual, and becomes a business; thresholds are not set. The guidance of the FATF should be followed; by considering the definition of a cryptocurrency service provider as the same as that of the term 'VASP' in the FATF guidance,[33] the confusion will be addressed as the activities which are considered to satisfy the term VASP are clearly defined.

[31] GOV.UK, 'Digital currencies: response to the call for information' <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf> accessed 11 March 2016 at p.19.
[32] ibid.
[33] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 September 2019 at para 33(c).

The principal benefit of regulator led changes to regulation is the speed at which the regulatory gap can be covered, the US was able to implement AML regulation upon cryptocurrency service providers much faster than Australia. The US response to the AML threats posed by cryptocurrencies was implemented soon after cryptocurrencies grew in prominence, and was achieved without the need for legislative reform. However, the Australian approach has been much clearer by adding new legal definitions to its AML legislation.

8.4.2. Legislator Led Widening of the Regulatory Perimeter

The alternative to regulator led changes to regulation is legislative reform, an approach which was taken by Australia. Australia has been efficient in its legislative reform, by amending the Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2006.[34] The 2017 amendment inserted "*digital currency*",[35] "*registered digital currency exchange provider*",[36] and "*registrable digital currency exchange service*"[37] to the 2006 Act. The list of designated services which are regulated by the 2006 Act now covers cryptocurrency exchange services,[38] and AUSTRAC is responsible for enforcing the AML regulation. The advantages of legislative reform are that the resulting law should be clear, and fully address the gaps in the law. The legislative process will vary by jurisdiction, but common characteristics are readings in Parliaments and Senates, and advice from select committees. This allows for time and care to be taken to achieve the correct wording to the reform, and consider any

[34] Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017.
[35] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.5.
[36] ibid.
[37] ibid.
[38] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.6(2) Item 50A.

consequences of the reform. The 2017 amendments to Australian law were the result of a statutory review by the Attorney General's Department[39] and a public consultation by the Parliament.[40] Subsequently a Bill was produced which proceeded through the normal scrutiny prior to enactment. Such a detailed process demonstrates a commitment by the relevant authorities in Australia to providing the correct response to the development of cryptocurrencies. The resultant reform meant that Australia was compliant with FATF guidance on cryptocurrencies before the detailed 2019 guidance was published. The definitions are clear, and in line with international standards. The UK has not created its own legislation to cover cryptocurrencies, but it has implemented the 5th Anti-Money Laundering Directive. As observed in chapter five, the UK Parliament has passed comparably few Acts in the past decade, partly due to the ongoing issue of leaving the EU.

The EU has also instigated a legislator led widening of the regulatory perimeter through the 5th Anti-Money Laundering Directive. The Directive adds "*virtual currency exchange platforms as well as custodian wallet providers to the list of obliged entities within the scope of the* [4th] *Directive*;"[41] which mirrors the guidance of the FATF with regards to bringing points of intersection between virtual currencies and the traditional financial system under the scope of EU AML regulations. The UK has implemented

[39] Attorney General's Department, 'Report on The Statutory Review of The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 And Associated Rules and Regulations' (April 2016) <https://www.homeaffairs.gov.au/how-to-engage-us-subsite/files/report-on-the-statutory-review-of-the-anti-money-laundering.pdf>accessed 28 October 2019.
[40] Parliament of Australia, 'Digital Currency – Game Changer or bit player' (August 2015) <http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Digital_currency/~/media/Committees/economics_ctte/Digital_currency/report.pdf> accessed 21 October 2019
[41] EUROPA, 'Revision of the Fourth Anti-Money-Laundering Directive' <http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/607260/EPRS_BRI%282017%29607260_EN.pdf> accessed 10 September 2019.

the 5th Directive through an amendment to the 2017 Money Laundering Regulations, but it is unclear how the UK intends to implement the Directive in practice. By regulating cryptocurrency service providers, the UK will take a similar approach to Australia and bring the UK up to international best practice as set out by the 2019 FATF guidance.[42]

8.4.3. Recommendations for the UK

Based on the UK's previous behaviour observed in chapter four,[43] it is anticipated that the UK will keep pace with international AML standards. The FCA has failed to take the initiative in the way FinCEN has in the US, instead the approach of the FCA has been to take a hands-off approach. The FCA indicated that it does not regulate cryptocurrencies, and individuals use them at their own risk.[44] The FCA could have interpreted the definition of a 'money services business' more proactively to address a regulatory gap, but it did not. The UK has also had ample time to adopt a legislator led approach to cryptocurrencies, as has been implemented in Australia. It is accepted that there have been a number of elections in short succession in the UK in the past decade, hampering the enacting of legislation. However, Australia has had 4 elections in the last 10 years and not produced a majority government, yet it still managed to pass legislation regulating cryptocurrencies. While UK legislators have been inactive,

[42] Financial Action Task Force, 'Guidance for A Risk-Based Approach to Virtual Currencies' <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf> accessed 01 August 2016.
[43] See chapter 4, specifically 'History of Anti-Money Laundering Law at 4.7.
[44] Financial Conduct Authority, 'Guidance on Cryptoassets: Feedback and Final Guidance to CP 19/3' (London, July 2019) <https://www.fca.org.uk/publication/policy/ps19-22.pdf> accessed 23 September 2019 at 2.19-29.

the EU has passed the 5th Anti-Money Laundering Directive,[45] which addresses cryptocurrencies and requires Member States to apply AML regulation to cryptocurrency service providers. The UK is following the legislator led model, but via the supranational legislation of the EU, as the UK has amended legislation in order to implement the 5th Anti-Money Laundering Directive. The exact nature of the UK's departure from the EU is unclear, but the UK has a history of implementing EU directives and following international best practice as demonstrated in chapter four at 4.7, so it is anticipated that the UK will continue to keep pace with EU AML law through complying with FATF standards.

While EU has taken a positive step, it presents the same short comings as identified in relation to the FATF guidance, the measures would apply to exchanges for fiat currency, and leave a large proportion of the cryptocurrency network outside of AML regulation. It is recommended that the UK goes further than simply implementing the 5th Anti-Money Laundering Directive, instead it needs to consider the remaining gaps in regulation, and address the blockchain. It is not possible to simply transpose existing AML regulation to distributed ledgers, as there is a lack of human involvement due to automated transactions. The blockchain presents regulatory challenges, but also opportunities for developments in AML supervision and detection.

[45] Council Directive 2018/843/EU 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 L 156/43.

8.5. Analysing the Blockchain using APIs

The wealth of data available through public ledgers is being ignored by the current approach to regulating cryptocurrencies. The focus of regulatory reform has been placed on the intersections between fiat currency and cryptocurrency, but this will only gather financial intelligence from a proportion of cryptocurrency transactions. As defined by Lilly money laundering is "*the process whereby the identity of dirty money that is the proceeds of crime and the real ownership of these assets is transformed so that the proceeds appear to originate from a legitimate source.*"[46] This process is clearly going to be aided by a plethora of unmonitored networks by which criminals can undertake numerous transactions without human involvement. It is not possible to apply existing AML regulation to cryptocurrency transactions, because the users transact directly rather than through a financial intermediary, therefore there is no institution to apply customer due diligence or file a suspicious activity report. A different approach is required, which will not be able to directly intercept or freeze a transaction, but will utilise the data the publicly available distributed ledger provides.

The current FATF guidance only applies to cryptocurrency service providers, but the FATF is aware that more can be done to "*develop technology-based solutions that will improve compliance*"[47] such as application programming interfaces (APIs) to digest and analyse the available information.[48] The FATF appears to be aware of the key weakness to its guidance, yet despite being aware of this in 2015, it has not fully

[46] P. Lilley, *Dirty Dealing: The Untold Truth about Global Money Laundering* (London, Kogan Page, 2006).
[47] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2019 para 51 at p14.
[48] Financial Action Task Force, 'Guidance for A Risk-Based Approach to Virtual Currencies' <http://www.fatf-gafi.org/media/fat2/documents/reports/Guidance-RBA-Virtual-Currencies.pdf> accessed 01 August 2016, para 51 at p14.

addressed this. This weakness was partly addressed in the 2019 guidance, recognising that VASPs providing cryptocurrency exchange services will convert between cryptocurrencies, as well as from fiat to cryptocurrency. Recognising transactions exchanging between cryptocurrencies is helpful in widening the regulatory perimeter, but it does not address the blockchain.

An API can interact with a programme, it can download and process data from that programme. Bitcoin's blockchain can be viewed freely online,[49] and there are numerous blockchain APIs available to enable automated analysis of the blockchain.[50] It is not clear if the financial intelligence available through the blockchain is currently being analysed for AML purposes, but it is a valuable resource that needs to be utilised.

At present a money laundering investigation will only begin when suspicion is aroused, but by automating analysis of the blockchain, money laundering investigations could get a head start, and patterns of transactions could be identified. Blockchain analysis should be the responsibility of the FIU as financial intelligence will be produced, therefore in the UK this will be the NCA.

8.5.1. Recommendations for the UK

The UK should utilise the data available through the blockchain to monitor money laundering and aid investigations. The wealth of transaction data available in a digital

[49] Blockchain Luxembourg, 'Block Explorer' <https://www.blockchain.com/explorer> accessed 30 September 2019.
[50] Examples can be found at Blockchain Luxembourg, 'Bitcoin Developer APIs' <https://www.blockchain.com/api> accessed 26 September 2019.

format, paired with the traditional AML measures applied to cryptocurrency service providers, will begin to address the currently unregulated realm of cryptocurrencies. To do this the UK must address the resourcing issues afflicting the NCA. The FATF have repeatedly found it to be lacking in terms personnel, technology, and "*analytical capability*",[51] which are crucial in order to remain among world leaders tackling money laundering.

At present money laundering investigations are behind the curve, by the time an investigation is launched, the money could be long gone. Analysing the blockchain will allow the NCA to follow cryptocurrencies as the transactions are openly published, a transaction could be reviewed within seconds of the block being created. It is not possible to identify individuals using the blockchain alone, but techniques are being developed to identify users through their public keys.[52]

8.6. Recommendations for further research

More research is required in order to develop APIs and software tools specifically for analysing the distributed ledgers for money laundering purposes, such software needs to include functionality for identifying patterns of transactions which are consistent with money laundering. Further research is also required into techniques which allow users to be identified. There are opportunities for artificial intelligence to be developed, when a body of successful investigations exists, machine learning could help identify money

[51] FATF, 'Anti-money laundering and counter-terrorist financing measures – United Kingdom, Fourth Round Mutual Evaluation Report' (Paris, December 2018) <fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-Kingdom-2018.pdf> accessed 11 September 2019 at para 6.
[52] Sarah Meiklejohn, et al, "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names," (2013) 38(6) ;Login: 10.

laundering techniques and behaviours to potentially automate suspicious activity reports.

8.7. Conclusion

Cryptocurrencies do not satisfy definitions of money, but their characteristics warrant regulatory attention. The FATF and the EU lead the international approach to regulating cryptocurrencies, but their guidance is focussed on the intersections between cryptocurrencies and fiat currencies, which leaves the majority of cryptocurrency transactions unregulated. The UK must go further than the FATF and EU measures, and should monitor the blockchain so as to avoid missing important financial intelligence. It is unlikely the FCA will take the initiative in the same way FinCEN has in the US, instead the UK will take a legislator led approach to widening the regulatory perimeter through implementing the 5th Anti-Money Laundering Directive and enacting further legislation. The NCA currently lacks the required resources to be able to address cryptocurrencies and follow the recommendations of this research. Therefore, while unlikely, resources should be provided to the NCA to allow them to develop technology which automates analysis of the distributed ledgers and harvests the wealth of financial intelligence available.

Bibliography

Primary Sources

International Treaties

Convention against Corruption (adopted 21 October 2003, entered into force 14 December 2005) 43 ILM 37.

Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (adopted 20 December 1988, entered into force 11 November 1990) UNTS 1582.

Convention against Transnational Organised Crime (adopted 15 November 2000, entered into force 29 September 2003) UNTS 2225.

Convention on Psychotropic Substances (adopted 21 February 1971, entered into force 16 August 1976) 520 UNTS 1019.

Single Convention on Narcotic Drugs (adopted 30 March 1961, entered into force 13 December 1964) 520 UNTS 151 (Single Convention on Narcotic Drugs).

Vienna Convention on the Law of Treaties (adopted 22 May 1969, entered into force 27 January 1980) 1155 (UNTS) 331.

EU Treaties

Consolidated Version Of The Treaty On The European Union [2012] OJ C326/25.

Consolidated Version Of The Treaty On The Functioning Of The European Union [2012] OJ C326/156.

Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (adopted 08 August 1990, entered into force 01 September 1993) ETS 141.

Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (adopted 16 May 2005, entered into force 01 May 2005 CETS 198.

EU Legislation

Council 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 [2001] OJ L.344/76.

Council Directive 2005/60/EC of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, [2005] OJ L309/15.

Council Directive 2013/36/EU of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC [2013] OJ L176/338.

Council Directive 2015/849/EU 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 [2015] OJ L.141/73.

Council Directive 2018/843/EU 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 L 156/43.

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 L166/77.

EU Case Law

Case 25/62 Plaumann and Co v Commission [1963] ECR 95.

Case T-201/04 Microsoft Corf v Commission [2007] ECR II-3601.

United Kingdom National Legislation

Bribery Act 2010.

Commonwealth of Australia Constitution Act.

Criminal Finances Act 2017.

Criminal Justice Act 1988.

Criminal Justice Act 1993.

Drug Trafficking Offences Act 1986.

Financial Services and Markets Act 2000.

Misuse of Drugs Act 1971.

Money Laundering Regulations 2007.

Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.

Proceeds of Crime Act 1987.

Proceeds of Crime Act 2002.

Prosecution of Offences Act 1985.

Terrorism Act 2000.

Australia National Legislation

Anti-Money Laundering and Counter-Terrorism Financing Act 2006.

Criminal Code Act 1995.

Financial Transactions Reporting Act 1988.

Legislation Act 2001.

Australia State Legislation

Acts Interpretation Act 1915 (SA).

Australian Crime Commission (Western Australia) Act 2004 (WU).

Crimes (Sentencing Procedure) Act 1999 (NSW).

Crimes Act 1914 (Cth).

Monetary Units Act (Vic).

Penalties and Sentences Act 1992 (Qld).

Penalty Units and Other Penalties Act 1987 (Tas).

Road Traffic (Administration) Act 2008 (WA).

United States of America National Legislation

Annunzio–Wylie Money Laundering Act 1992.

Bank Secrecy Act, Pub. L. 91–508.

Code of Federal Regulations Title 31 - Money and Finance: Treasury.

Money Laundering Control Act Pub. L. 99-570.

Uniting and Strengthening America by Providing Appropriate Tools to Restrict, Intercept and Obstruct Terrorism Act 2001, Pub. L. No. 107-56.

Pub. L. No. 99-570, 100 Stat. 3207-18.

Securities Exchange Act 1934.

US Code Title 18 - Crimes and Criminal Procedure.

US Code Title 31 - Money and Finance.

US Code Title 7 – Agriculture.

United Kingdom Case Law

K Ltd v National Westminster Bank plc (Revenue and Customs Commissioners and another intervening) [2006] EWCA Civ 1039.

Moss v Hancock [1899] 2 QB III.

R v Cuthbertson [1981] A.C. 470 HL.

R v Da Silva [2007] 1 WLR 303.

R v Teresko [2018] Crim LR 81 (Unreported).

R v Terry (Westminster Magistrates, 13 July 2012).

Shaaban bin Hussien v Chong Fook Kam [1970] 2 WLR 441.

Shah v HSBC Private Bank (UK) Ltd [2012] EWHC 1283.

Australia Case Law

Chief Executive Officer of Australian Transaction Reports and Analysis Centre v TAB Limited (No 3) [2017] FCA 1296.

Chief Executive Officer of the Australian Transaction Reports and Analysis Centre v Commonwealth Bank of Australia Limited [2018] FCA 930.

United States of America Case Law

Commodity Futures Trading Commission v. Patrick K. McDonnell, and Cabbagetech, Corp. D/B/A Coin Drop Markets, Case No 1 18-CV-361 (E.D.N.Y. Mar. 6, 2018).

Securities and Exchange Commission v. Trendon T. Shavers and Bitcoin Savings and Trust, Civil Action No. 4:13-CV-416.

United States v $ 4,255,625.39, 551(Suppl. 314) (1982) 23.

United States v. Campbell, 997 F.2d 854, 857. 4th Cir 1992.

United States v. Hawkey, 148 F.3d 920 8th Cir.1998.

United States v Jewell 532 F.2d 697 (9th Cir.1976).

United States v Sadighi and Rayhani Unreported (9th Cir. 1999).

United States v Santos 128, S. Ct. 2020, 2025, 2031 (2008) affirming 461 F. 3d 886 (7th Cir. 2006).

United States v Stewart 185 F.3d 112 (3rd Cir. 1999).

United States v. Trapilo 130 F.3d 547. 2nd Cir. 1997.

United States v. Ulbricht 858 F.3d 71, 82–83 (2d Cir. 2017).

Secondary Sources

Books and Chapters in Edited Collections

Aristotle*, Politics*, Book 1, Ch.9.

Castronova E, *Virtual Worlds: A First Hand Account of Market and Society of the Cyberian Frontier* (SSRN, 2001).

Chaikin D, 'A Critical Analysis of the Effectiveness of Anti-Money Laundering Measures with Reference to Australia' in C. King, C, Walker and J. Gurulé, *The Palgrave Handbook of Criminal and Terrorism Financing Law* (Palgrave Macmillan, 2018).

Chambers Jones C, and Hillman H, *Financial Crime and Gambling in a Virtual World: A new Frontier in Cybercrime* (Edward Elgar, 2014).

Cotterrell R*, Law's Community* (OUP 1995).

Craig P and de Búrca G, *EU Law: Text Cases and Materials* (6th edn, Oxford University Press, 2015).

Dadomo C and Quénivet N, *European Union Law* (Hall & Stott Publishing, 2015).

De Sanctis FM, *Football, gambling, and money laundering: a global criminal justice perspective* (Springer, New York 2014).

Encyclopaedia Britannica Inc. *Britannica Book of the Year (2015)* (Encyclopaedia Britannica, 2015).

Foley D, 'Money in Economic Activity' in M. Milgate and P. Newman (eds) *The New Palgrave: Money* (W.W. Norton, 1987).

Fox D, *Property Rights in Money* (OUP, 2008).

Freidman L, *Crime and Punishment in American History* (Basic Books 1934).

General Accounting Office, *Money Laundering: Needed Improvements for Reporting Suspicious Transactions Are Planned* (Washington, DC: General Accounting Office, 1995).

Gibbs H, Watson R and Menzies A, *Review of Commonwealth Criminal Law: Fifth Interim Report* (Commonwealth Attorney-General's Department, 1991).

Gilmore WC, *Dirty Money – The Evaluation of International Measures to Counter Money Laundering and the Financing of Terrorism* (Council of Europe, Brussels, 2004).

Gilmore WC, *Dirty Money: The Evolution of Money Laundering Counter-Measures* (Strasbourg, Council of Europe Press, 1995).

Hudson A, *The Law of Finance* (Sweet and Maxwell, 2013).

Huizinga J, Homo Ludens: *A Story of the Play-Element in Culture* (Beacon Press, 1938).

Hunter E, 'Australia', in M Simpson, N Smith and A Srivastava (eds*), International Guide to Money Laundering Law and Practice* (Haywards Heath, Bloomsbury Professional, 2010).

Hurst JW, *A Legal History of Money in the United States* 1774-1970 (University of Nebraska Press, 1973).

Karha J, 'How to Make Comparable Things: Legal Engineering at the Service of Comparative Law' in Hoecke Mv*, Epistemology and methodology of Comparative Law* (Hart Publishing 2004).

Keynes JM, *A Treatise on Money* (Harancourt Brace, 1930).

King C, 'Asset Recovery: An Overview' in King C, Walker C and Gurulé J, *The Palgrave Handbook of Criminal and Terrorism Financing Law, Volume 1* (Palgrave Macmillan, 2018).

Kiyotaki N and Wright R, 'Acceptability, Means of Payment and Media of Exchange' in J. Eatwell, M. Milgate and P. Newman (eds) *The New Palgrave: Money* (W.W. Norton, 1987).

Knapp GF, *The State Theory of Money* (Macmillan, 1924).

Lastowka G, *Virtual Justice: The New Laws of Online Worlds* (Yale University Press, 2010).

Levi M, Naylor and P. Williams, *Financial Havens, Banking Secrecy and Money Laundering* (New York, 1998).

Low L et al, 'Country Report: The US Anti-Money Laundering System' in M. Pieth and G. Aiolfi*, A Comparative Guide to Anti-Money Laundering* (Edward Elgar, 2004).

Madinger J, *Money Laundering: A Guide for Criminal Investigators: Third Edition* (CRC Press, 2016).

Mann T (ed), *Australian Law Dictionary* (Oxford University Press 2010).

Margossian A, Bagnall M, Mitra R and Halforty I, 'Australia' in M. S. Sackheim and N. A. Howell (eds), *The Virtual Currency Regulation Review* (London, Law Business Research Ltd, 2018).

Marx K, *Capital: Vol 1* (London, Penguin, 1976).

Mason M and Mason J, *Writing Law Dissertations: An Introduction and Guide to the Conduct of Legal Research* (Pearson 2007).

Mclellan D, *Karl Marx* (London, Harper Collins, 1975).

Minsky HP, *Stabilizing an Unstable Economy* (Yale University Press, 1986).

North DC, *Institutions, Institutional Change and Economic Performance* (Cambridge University Press, 1990).

Lilley P, *Dirty Dealing: The Untold Truth about Global Money Laundering* (London, Kogan Page, 2006).

Pearce D, Campbell E and Harding D ('Pearce Committee'*), Australian Law Schools: A Discipline Assessment for the Commonwealth Tertiary Education Commission* (Australian Government Publishing Service, 1987).

Proctor C (ed), *Mann on the Legal Aspects of Money* (7th Edition, Oxford University Press, 2005).

Robinson J, *The Laundrymen* (London, Pocket Books, 1995).

Ryder N, *Financial Crime in the 21st Century: Law and Policy* (Edward Elgar, Cheltenham, 2011).

Ryder N*, Money laundering – an endless cycle? A comparative analysis of the anti-money laundering policies in the United States of America, the United Kingdom, Australia and Canada* (Routledge, London, 2012).

Simpson M, Smith N and Srivastava A (eds), *International Guide to Money Laundering Law and Practice* (Haywards Heath, Bloomsbury Professional, 2010).

Smith A, *An Inquiry Into the Nature and Causes of The Wealth of Nations* (The Cannon Edition, New York, The Modern Library, 1937).

Stewart DG, *Royal Commission of Inquiry into Drug Trafficking* (Canberra, Australia Government Printing Services, 1983).

Thomas JP and Roppolo WV, 'United States of America' in A. Srivastava, M. Simpson and N. Moffat, *International Guide to Money Laundering Law and Practice* (Bloomsbury, 2013).

Unger B and Linde D vd, *Research Handbook On Money Laundering* (Edward Elgar, Cheltenham, 2013).

Unger B, *The Scale and Impacts of Money Laundering* (Edward Elgar, Cheltenham, 2007).

Wray LR, *Money and Credit in Capitalist Economics: The Endogenous Money Approach* (Edward Elgar, 1990).

Zagaris B, *International White Collar Crime: Cases and Materials* (New York: Cambridge University Press, 2010).

Journal Articles

Alexander K, 'The International Anti-Money-Laundering Regime: The Role of the Financial Action Task Force' (2001) 4(3) JMLC 231.

Alexander R, 'How to Regulate Bitcoin – the Debate Continues' (2018) 39(3) Comp Law 65.

Alexander R, Insider Dealing and Money Laundering in the EU: Law and Regulation (Aldershot: Ashgate, 2007).

Alford D, ‘Anti-Money Laundering Regulations: A Burden on Financial Institutions’ (1994) 19(3) North Carolina Journal of International Law and Commercial Regulation 437.

Bell MW, ‘Toward a Definition of “Virtual Worlds”’ (2008) 1(1) Journal of Virtual Worlds Research 1.

Bell S, ‘The Role of the State and the Hierarchy of Money’ (2001) 25 Cambridge Journal of Economics 149.

Blau CW Et Al., Investigation and Prosecution of Illegal Money Laundering: A Guide to the Bank Secrecy Act, U.S. Department of Justice, Criminal Division (1983).

Bradshaw A, Sense and Sensibility: Debates and Developments in Socio-Legal Research Methods’ in P Thomas (ed) Socio-Legal Studies (Aldershot, Ashgate-Dartmouth, 1997).

Brendan James Gilbert, ‘Getting to Conscionable: Negotiating Virtual Worlds’ End User License Agreements without Getting Externally Regulated’ (2009) 4(4) JICLT 238.

Brenner S, ‘Fantasy Crime’ (2008) 11(1) V and J Ent & Tech L 1.

Buchanan B, ‘Money laundering – a global obstacle’ (2004), 18(1) Research in International Business and Finance 115.

Carr I, ‘Fighting corruption through the United Nations Convention on Corruption 2003: a global solution to a global problem?’ (2005) 11(1) Int. T.L.R. 24.

Cassella SD, ‘Reverse money laundering (2003) 7(1) Journal of Money Laundering 92.

Castronova E, ‘The Right to Play’ (2004) 49 NYL Sch L Rev 185.

Chaikin D, ‘Risk-Based Approaches to Combatting Financial Crime’ (2009) 8(2) Journal of Law and Financial Crime 20.

Chaum, D, ‘Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms’ [1981] 24(2) Communications of the ACM 84.

Chaum.D, ‘Blind Signatures for Untraceable Payments’ in Chaum. D, Rivest. RL, Sherman, AT (ed), ‘Advances in Cryptology’ (Session III, Springer US, 1982).

Demetriades G, ‘”Is the person who he claims to be?” old fashion due diligence may give the correct answer!’ (2016) 19(1) JMLC 79.

Doyle T, ‘Cleaning Up Anti-Money Laundering Strategies: Current FATF Tactic Needlessly Violate International Law’ (2002) 24 Houston Journal of International Law 297.

Feldman AM, ‘Bilateral Trading Processes, Pairwdse Optimality and Pareto Optimality’ (1973) 40(4) Review of Economic Studies 463.

Fortson R, ‘Intensifying anti-money laundering laws - the last 30 years’ (2016) 4 Arch Rev 6.

Gallant MM, ‘Money Laundering Consequences: Recovering Wealth, Piercing Secrecy, Disrupting Tax Havens And Distorting International Law’ (2014) 17(3) JMLC 296.

Geva B, ‘Disintermediating Electronic Payments: Digital Cash and Virtual Currencies’ (2016) 31(12) JIBLR 661.

Goldby M, ‘Anti-Money Laundering Reporting Requirements Imposed by English Law: Measuring Effectiveness and Gauging the Need for Reform’ (2013) 4 Journal of Business Law 367.

Goodhart CAE, ‘What is the essence of money?’ 2005 29 Cambridge Journal of Economics 817.

Graham G, ‘Seychelles 'haven for money laundering'’ Financial Times (London 2 February 1996) 3.

Hall J, ‘Restraint orders: R. v Teresko (Sergejs) Kingston Crown Court: HH Judge Lodder QC: unreported 11 October 2017’ (2018) 1 CLR 81.

Houben R, ‘Cryptocurrencies from a money laundering and tax evasion perspective’ (2019) 30(5) International Company and Commercial Law Review 261.

Innes AM, ‘What is Money’ (1913) 30 Banking LJ 377.

Irwin ASM and Tuner AB, ‘Illicit Bitcoin transactions: challenges in getting to the who, what, when and where’ (2018) 21(3) JMLC 297.

Irwin ASM, and Dawson C, ‘Following the cyber money trail: Global challenges when investigating ransomware attacks and how regulation can help’ (2019) 22(1) JMLC 110.

Irwin ASM, Kim-Kwang RC, and Liu L, ‘An analysis of money laundering and terrorism financing typologies’ (2012) 15(1) JMLC 85.

Irwin ASM, Slay J, Kim-Kwang RC, Lui L, ‘Money laundering and terrorism financing in virtual environments: a feasibility study’ (2014) 17(1) JMLC 50.

Jacobs R, ‘European Union: Virtual Currencies – Warning’ (2018) 33(3) JIBLR 29.

Jensen N, ‘Technology and Intelligence’ (2005) 8(3) JMLC 227.

Jones RA, ‘The Origin and Development of Media of Exchange’ (1976) 84 (4, Part 1) August Journal of Political Economy 757.

Juhász PL, Stéger J, Kondor D and Vattay G, ‘A Bayesian approach to identify Bitcoin users’ (2018) 13(12) PLoS ONE 1

Kennedy A, ‘Dead Fish across the Trail: Illustrations of Money Laundering Methods’ (2005) 8(4) JMLC 305.

Kennedy R, ‘Law in Virtual Worlds’ (2009) 12(10) Journal of Internet Law 3.

Kerr OS, ‘Criminal Law in Virtual Worlds’ [2008] Chi Legal F 415.

Kluczyński M, ‘Prevention of Money Laundering in the Fight Against Human Trafficking and Smuggling of Migrants’ (2013) 5(2) Internal Security 83.

Lane J, ‘Bitcoin, Silk Road and the Need for a New Approach to Virtual Currency Regulation’ (2013-2014) 8 Charleston Law Review 511.

Lastowka G and Hunter D, ‘Virtual Crimes’ (2004) 49 NYL Sch Rev 294.

Leong A, ‘Chasing dirty money: domestic and international measures against money laundering’ (2007) 10(2) Journal of Money Laundering Control 140.

Levi M, ‘Evaluating the “New Policing”: Attacking the Money Trail of Organized Crime’ (1997) 30(1) Australian and New Zealand Journal of Criminology 1.

McDowell J and Novis G, ‘The Consequences Of Money Laundering And Financial Crime’ (2001) 6(2) Economic Perspectives 6.

McNeil C, ‘The Australian Anti-Money Laundering Reform in the International Context’ (2007) 22(6) Journal of International Banking Law and Regulation 340.

Meiklejohn S, et al, “A Fistful of Bitcoins: Characterizing Payments Among Men with No Names,” (2013) 38(6) ;Login: 10.

Menger K, ‘On Origins of Money’ (1892) 2(6) Economic Journal 293.

Mitsilegas V and Gilmore B, ‘The EU legislative framework against money laundering and terrorist finance: a critical analysis in light of evolving global standards’ (2007) 56(1) International and Comparative Law Quarterly 119 at 120

Morris-Cotterill N, ‘The International Effect of Money Laundering Laws’ (1996) 4(1) Journal of Financial Regulation & Compliance 67.

Ping He, ‘A Typological Study on Money Laundering’ (2010) 13(1) JMLC 15.

Radford RA, ‘The Economic Organisation of a P.O.W. Camp’ (1945) November Economica, 189.

Reuter P and Greenfield VA, ‘Measuring Global Drug Markets: How Good Are the Numbers and Why Should We Care about Them?’ (2001) 2(159) World Economics 73.

Reynolds P and Irwin ASM, ‘Tracking digital footprints: anonymity within the bitcoin system’ (2017) 20(2) JMLC 172.

Rider B, ‘The practical and legal aspects of interdicting the flow of dirty money’ (1996) 3(3) JFC 234.

Roberge I, ‘Misguided Policies in the War on Terror? The Case for Disentangling Terrorist Financing from Money Laundering’ (2007) 27(3) Political Studies Associations 196.

Ryder N, ‘The Financial Services Authority and Money Laundering: A Game of Cat and Mouse’ (2008) 67(3) Cambridge LJ 635.

Ryder N, ‘To Confiscate or not to Confiscate? A Comparative Analysis of the Confiscation of the Proceeds of Crime Legislation in the United States and the United Kingdom’ [2013] 8 JBL 767.

Simser J, ‘Money laundering: emerging threats and trends’ (2013) 16(1) JMLC 41.

Southall. E and Taylor. M, ‘Bitcoins’ [2013] 19(6) Computer and Telecommunications Law Review 177.

Sproule DW, and St-Denis P, ‘The UN Trafficking Convention: An Ambitious Step’ (1989) 27 Canadian Yearbook of International Law 263.

Stessens G, ‘The FATF ‘Black List’ of Non-Cooperative Countries or Territories’ (2001) 14 Leiden Journal of International Law 199.

Stewart DP, ‘Internationalizing the War on Drugs: The UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances’ (1990) 18 Denver Journal of International Law and Policy 387.

Stokes R, ‘Virtual Money Laundering: The Case of Bitcoin and the Linden Dollar’ (2012) 21(3) Information and Communications Technology Law 221.

Thomas J, ‘Quantifying the Black Economy: ‘Measurement Without Theory’ Yet Again?’ (1999) 109(456) The Economic Journal 381.

Tromans R, ‘The World is not Enough: Law for a Virtual Universe’ (2007) 70 Euro Law 21.

Tseng YS, ‘Governing Virtual Worlds: Iteration 2.0’ (2011) 35 J Law & Policy 547.

Unger B, ‘Can Money Laundering Decrease?’ (2013) 41(5) Public Finance Review 658.

van Dunné J, ‘On a clear day, you can see the continent - the shrouded acceptance of good faith as a general rule of contract law on the British Isles’ (2015) 31(1) Const. L.J. 3.

van Hoecke M, ‘Legal Doctrine: Which Method(s) What Kind of Discipline?’ in M. van Hoecke, Methodologies of Legal Research (Bloomsbury, 2011).

Von Kaenel FJ, ‘Willful Blindness: A Permissible Substitute for Actual Knowledge under the Money Laundering Control Act?’ (1993) 71 Wash ULQ 1189.

Walker J and Unger B, ‘Estimating Money Laundering: The Walker Gravity Model’ (2009) 5(821) Review of Law and Economics 53.

Weber B, ‘Bitcoin and the legitimacy crisis of money’ (2016) 41 Cambridge Journal of Economics 17.

Welling SN, ‘Smurfs, Money Laundering, and The Federal Criminal Law: The Crime Of Structuring Transactions’ (1989) 41 Florida Law Review 287.

Zelizer VA, ‘The Social Meaning of Money: “Special Monies”’ (1989) 95(2) 342.

Reports

Attorney General’s Department, ‘Report on The Statutory Review of The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 And Associated Rules and Regulations’ (April 2016) <https://www.homeaffairs.gov.au/how-to-engage-us-subsite/files/report-on-the-statutory-review-of-the-anti-money-laundering.pdf> accessed 28 October 2019.

AUSTRAC, ‘AUSTRAC Annual Report 2013-14’ <https://parlinfo.aph.gov.au/parlInfo/download/publications/tabledpapers/94f918c0-cc3a-4f86-a7bf-482d563b9daf/upload_pdf/austrac-ar13-14-web-full.pdf;fileType=application%2Fpdf#search=%22Australian%20Transaction%20Reports%20and%20Analysis%20Centre%20report%20for%202013%22> accessed 24 July 2019.

AUSTRAC, ‘AUSTRAC Annual Report 2015-16’ <https://www.austrac.gov.au/sites/default/files/2019-05/AUSTRAC_annual_report_2015-16.pdf> accessed 24 July 2019.

AUSTRAC, ‘AUSTRAC Annual Report 2016-17’ <https://www.austrac.gov.au/sites/default/files/2019-05/AUSTRAC_annual_report_2016-17.pdf> accessed 24 July 2019.

AUSTRAC, ‘AUSTRAC Annual Report 2017-18’ <https://www.austrac.gov.au/sites/default/files/2019-05/AUSTRAC_annual_report_2017-18.pdf> accessed 24 July 2019.

AUSTRAC, ‘Annual Report 2017/18’ <https://www.austrac.gov.au/sites/default/files/2019-05/AUSTRAC_annual_report_2017-18.pdf> accessed 29 July 2019.

Australia, Fourth Round Mutual Evaluation Report’ <https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Report-Australia-2015.pdf> accessed 23 July 2019.

Australian Government Department of Home Affairs, ‘Report on The Statutory Review of The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 And Associated Rules and Regulations’ <https://www.homeaffairs.gov.au/how-to-engage-us-subsite/files/report-on-the-statutory-review-of-the-anti-money-laundering.pdf> accessed 16 July 2019.

ECB, ‘Virtual Currency Schemes’ <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> accessed 02 June 2019.

ECB, ‘Virtual Currency Schemes – A Further Analysis’ <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> accessed 29 March 2019.

HM Government ‘Economic Crime Plan’ (12 July 2019) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/816215/2019-22_Economic_Crime_Plan.pdf> accessed 23 October 2019.

HM Treasury, ‘Cryptoassets Taskforce: final report’ (29 October 2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf> accessed 20 September 2019.

HM Treasury, ‘Fintech Sector Strategy: Securing the Future of UK Fintech’ (22 March 2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/692874/Fintech_Sector_Strategy_print.pdf> accessed 20 September 2019.

HM Treasury, ‘UK national risk assessment of money laundering and terrorist financing’ (October 2019) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf> accessed 28 October 2019.

Law Commission, Anti-money laundering: the SARs regime (Law Com No 384, 2018).

Parliament of Australia, ‘Digital Currency – Game Changer or bit player’ (August 2015) <http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Dig

ital_currency/~/media/Committees/economics_ctte/Digital_currency/report.pdf> accessed 21 October 2019.

Parliament of Australia, 'Government Response to the Inquiry into Digital currency' <http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Digital_currency/~/media/Committees/economics_ctte/Digital_currency/report.pdf> accessed 10 July 2019.

Treasury Select Committee, The Run on the Rock, HC56-II 2007-08.

Newspapers

Busby M, 'Bitcoin worth £900,000 seized from hacker to compensate victims' The Guardian (London, 23 August 2019).

Durkin P, '70pc jump in suspicious money laundering transactions: AUSTRAC' Financial Review (Melbourne, 18 October 2018) <https://www.afr.com/business/banking-and-finance/70pc-jump-in-suspicious-money-laundering-transactions-austrac-20181018-h16szs> accessed 24 July 2019.

The Guardian, 'Australian election 2019: live results' (18 May 2019) <https://www.theguardian.com/australia-news/ng-interactive/2019/may/18/live-results-for-the-2019-australian-election-track-the-votes> accessed 09 October 2019.

The Guardian, 'Energy cost of 'mining' bitcoin more than twice that of copper or gold' <https://www.theguardian.com/technology/2018/nov/05/energy-cost-of-mining-bitcoin-more-than-twice-that-of-copper-or-gold> accessed 05 March 2019.

The Guardian, 'Nine Bitcoin alternatives for future currency investments' <http://www.theguardian.com/technology/2013/nov/28/bitcoin-alternatives-future-currency-investments> accessed 17 June 2015.

Treanor J, The Guardian, 'London still world's top financial centre despite Brexit, says survey' <https://www.theguardian.com/business/2017/sep/11/london-financial-centre-brexit-frankfurt-dublin-new-york-donald-trump> accessed 20 July 2018.

Washington Post, '5 Held in Plot to Bug Democrats' Office' <http://www.washingtonpost.com/wp-dyn/content/article/2002/05/31/AR2005111001227.html> accessed 06 September 2019.

Washington Post, 'Bug Suspect Got Campaign Funds' <https://www.washingtonpost.com/politics/bug-suspect-got-campaign-funds/2012/06/06/gJQAyTjKJV_story.html> accessed 06 September 2019.

Online Sources

Attorney General's Department, 'About Us' <http://www.ag.gov.au/About/Pages/default.aspx> accessed 10 July 2015.

AUSTARC, 'AUSTRAC and CBA agree $700m penalty' (4 June 2018) <https://www.austrac.gov.au/austrac-and-cba-agree-700m-penalty> accessed 22 October 2019.

AUSTRAC, 'A guide to preparing and implementing an AML/CTF program for your digital currency exchange business' <https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/guide-preparing-and-implementing-amlctf-program-your-digital-currency-exchange-business> accessed 26 July 2019.

AUSTRAC, 'About AUSTRAC' <http://www.austrac.gov.au/about-us/austrac> accessed 14 September 2019.

AUSTRAC, 'AML/CTF Rules overview' (27 September 2019) <https://www.austrac.gov.au/business/legislation/amlctf-rules/amlctf-rules-overview> accessed 23 October 2019.

AUSTRAC, 'AUSTRAC Typologies and Case Studies Report 2014' <https://www.austrac.gov.au/sites/default/files/2019-07/typologies-report-2014.pdf> accessed 24 July 2019.

AUSTRAC, 'Introduction to Money Laundering' <https://michaelsmithnews.typepad.com/files/money-laundering.pdf> accessed 5 September 2019.

AUSTRAC, 'New Australian laws to regulate cryptocurrency providers' <http://www.austrac.gov.au/media/media-releases/new-australian-laws-regulate-cryptocurrency-providers> accessed 23 July 2018.

AUSTRAC, 'Record $45 million civil penalty ordered against Tabcorp' (16 March 2017) <https://www.austrac.gov.au/record-45-million-civil-penalty-ordered-against-tabcorp> accessed 22 October 2019.

AUSTRAC, 'Strategic analysis brief: Money laundering through real estate' <https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/strategic-analysis-brief-money-laundering-through-real-estate# > accessed 07 September.

Australian Broadcasting Corporation, 'Federal Election 2016' <http://www.abc.net.au/news/federal-election-2016/results/> accessed 27 September 2019.

Australian Crime Intelligence Commission, ‘About Us’ (17 May 2019) <https://www.acic.gov.au/about-us> accessed 29 July 2019.

Australian Crime Intelligence Commission, ‘Australian Criminal Intelligence Commission Annual Report 2016-17’ <https://acic.govcms.gov.au/sites/g/files/net1491/f/acic_2016-17_annual_report.pdf?v=1508387578> accessed 29 July 2019.

Australian Crime Intelligence Commission, ‘Australian Criminal Intelligence Commission Annual Report 2017-18’ <https://acic.govcms.gov.au/sites/g/files/net3726/f/acic_2017-18_ar_digital.pdf?v=1539748074> accessed 29 July 2019.

Australian Crime Intelligence Commission, ‘Money laundering’ (27 February 2019) <https://www.acic.gov.au/about-crime/organised-crime-groups/money-laundering> accessed 23 October 2019.

Australian Digital Commerce Association, ‘About’ <https://adca.asn.au/about/> accessed 19 July 2019.

Australian Digital Commerce Association, ‘Australian Digital Currency Industry Code of Conduct’ <https://adca.asn.au/wp-content/uploads/2019/02/Australian-Digital-Currency-Industry-Code-of-Conduct-Board-Approved-Text-30-Nov-2016.pdf> accessed 19 July 2019.

Australian Federal Police, ‘Criminal Asset Confiscation Taskforce’ <https://www.afp.gov.au/sites/default/files/PDF/criminal-assets-confiscation-taskforce-brochure.pdf> accessed 14 September 2019.

Australian Federal Police, ‘Our Organisation’ <https://www.afp.gov.au/about-us/our-organisation> accessed 14 September 2019.

Australian Tax Office, ‘GST and Digital Currency’ <https://www.ato.gov.au/business/gst/in-detail/your-industry/financial-services-and-insurance/gst-and-digital-currency> accessed 17 September 2019.

Australian Tax Office, ‘Tax Treatment of Crypto-Currencies in Australia – Specifically Bitcoin’ <https://www.ato.gov.au/General/Gen/Tax-treatment-of-crypto-currencies-in-Australia---specifically-bitcoin/> accessed 17 September 2019.

Bambrough B, ‘A Bitcoin Halvening Is Two Years Away - Here's What'll Happen To The Bitcoin Price’ (Forbes, 29 May 2018) <https://www.forbes.com/sites/billybambrough/2018/05/29/a-bitcoin-halvening-is-two-years-away-heres-whatll-happen-to-the-bitcoin-price/#4bffecd05286> accessed 19 March 2019.

Bank of England, ‘What are cryptoassets (cryptocurrencies)?’ <https://www.bankofengland.co.uk/knowledgebank/what-are-cryptocurrencies> accessed 14 October 2019.

Bank of England, ‘What is Money?’ (19 February 2019) <https://www.bankofengland.co.uk/knowledgebank/what-is-money> accessed 07 October 2019.

Barclays, ‘Where’s Britain spending? The Barclaycard Consumer Spending Report Q3 2014’ http://www.barclaycard.com/content/dam/bcardpublic/FinalContent/NewsandViews/2014/q3spendreport/Barclaycard_Spend_Report_Q3_2014.pdf> accessed 17 June 2015.

BBC, ‘The League of Nations and the United Nations’ (17 February 2011) <http://www.bbc.co.uk/history/worldwars/wwone/league_nations_01.shtml> accessed 02 September 2019.

BBC News, ‘Bitcoin Currency Hits New Record High’ <https://www.bbc.co.uk/news/business-42135963> accessed 19 March 2019.

BBC News, ‘Bitcoin explained: How do crypto-currencies work?’ (12 February 2018) <https://www.bbc.co.uk/news/av/technology-43026143/bitcoin-explained-how-do-crypto-currencies-work> accessed 20 July 2018.

BBC News, ‘Bitcoin’ <https://www.bbc.co.uk/news/topics/c734j90em14t/bitcoin> accessed 05 March 2019.

BBC News, ‘Brexit: Boris Johnson's second attempt to trigger election fails’ (10 September 2019) <https://www.bbc.co.uk/news/uk-politics-49630094> accessed 09 October 2019.

BBC News, ‘Business: The Company File: Beenz means business’ <http://news.bbc.co.uk/1/hi/business/297133.stm> accessed 12 June 2015.

BBC News, ‘Criminal's Bitcoin seized in Surrey Police first’ (Surry, 21 July 2018) <https://www.bbc.co.uk/news/uk-england-surrey-44896665> accessed 12 September 2019.

BBC News, ‘Criminals hide 'billions' in crypto-cash – Europol’ (12 February 2018) <https://www.bbc.co.uk/news/technology-43025787> accessed 08 October 2019.

BBC News, ‘Election 2015’ <http://www.bbc.co.uk/news/election/2015/results> accessed 27 September 2019.

BBC News, ‘Election 2017’ <http://www.bbc.co.uk/news/election/2017/results> accessed 27 September 2019.

BBC News, ‘Liberty Reserve digital money service forced offline’ <http://www.bbc.co.uk/news/technology-22680297> accessed 17 June 2015.

BBC News, ‘Liverpool 'dropout' jailed for Silk Road dark web site’ (12 April 2019) <https://www.bbc.co.uk/news/uk-england-merseyside-47913780> accessed 11 September 2019.

BBC News, ‘'Money mules': Rising numbers are in middle age’ (18 June 2019) <https://www.bbc.co.uk/news/uk-48671542> accessed 23 September 2019.

BBC News, ‘MtGox bitcoin exchange files for bankruptcy’ (28 February 2014) <https://www.bbc.co.uk/news/technology-25233230> accessed 07 October 2019.

BBC News, ‘NHS cyber-attack: GPs and hospitals hit by ransomware’ (13 May 2017) <https://www.bbc.co.uk/news/health-39899646> accessed 097 October 2019.

BBC News, ‘One million adults 'do not have a bank account' <http://www.bbc.co.uk/news/10277151> accessed 29 May 2015.

BBC News, ‘Prolific Sheerness hacker ordered to pay back £922k’ (23 August 2019) <https://www.bbc.co.uk/news/uk-england-kent-49450676> accessed 24 September 2019.

BBC News, ‘Rise in teenage money mules prompts warnings’ (16 September 2019) <https://www.bbc.co.uk/news/business-49717288> accessed 23 September 2019.

BBC News, ‘Silk Road drug website founder Ross Ulbricht jailed’ (30 May 2015) <https://www.bbc.co.uk/news/world-us-canada-32941060> accessed 05 September 2019.

BBC News, ‘Theresa May and the DUP deal: What you need to know’ (26 June 2017) <https://www.bbc.co.uk/news/election-2017-40245514> accessed 09 October 2019.

BBC News, ‘Top Bitcoin exchange MtGox goes offline’ <https://www.bbc.co.uk/news/technology-26333661> accessed 02 September 2019.

BBC News, ‘US Election 2016’ <http://www.bbc.co.uk/news/election/us2016/results> accessed 27 September 2019.

BBC News, ‘Video Games Embrace China’s Freemium Model to Beat Piracy’ <http://www.bbc.co.uk/news/technology-20899165> accessed 17 June 2015.

Bitcoin Charts, ‘Markets’ <http://bitcoincharts.com/markets/> accessed 18 June 2015.

Bitcoin, ‘Getting started with Bitcoin’ <https://bitcoin.org/en/getting-started> accessed 14 October 2019.

Bitcoin, ‘How it Works’ <https://bitcoin.org/en/how-it-works> accessed 13 October 2019.

Bitcoin Wiki, ‘Research’ <http://bitcoin.org/bitcoin.pdf> accessed 10 June 2015.

Bitcoin.org, ‘How Does Bitcoin Work?’ <http://bitcoin.org/en/how-it-works> accessed 19 January 2014.

Blizzard, ‘Games and Subscriptions’ <http://eu.battle.net/wow/en/shop/> accessed 11 June 2015.

Blizzard, ‘World of Warcraft: Game Guide’ <http://eu.battle.net/wow/en/game/> accessed 11 June 2015.

Blockchain Australia, ‘Home’ <https://blockchainaustralia.org/> accessed 19 July 2019.

Blockchain Luxembourg, ‘Bitcoin Developer APIs’ <https://www.blockchain.com/api> accessed 26 September 2019.

Blockchain Luxembourg, ‘Block Explorer’ <https://www.blockchain.com/explorer> accessed 30 September 2019.

Blockchain, ‘Block Explorer: Bitcoin Cash’ <https://www.blockchain.com/explorer?currency=BCH> accessed 13 October 2019.

Blockchain, ‘Block Explorer: Bitcoin’ <https://www.blockchain.com/explorer> accessed 13 October 2019

Blockchain, ‘Block Explorer: Ethereum’ <https://www.blockchain.com/explorer?currency=ETH> accessed 13 October 2019

Brett Wilson LLP, ‘Bitcoin seized as ‘realisable assets’ in confiscation proceedings’ (London, 03 September 2019) <https://www.brettwilson.co.uk/blog/bitcoin-seized-as-realisable-assets-in-confiscation-proceedings/> accessed 12 September 2019.

British Bankers Association, ‘Response to Cutting Red Tape Review, The Effectiveness of The UK’s AML Regime’ <https://www.bba.org.uk/download-file/?f=eyJ1cmwiOiJodHRwczpcL1wvd3d3LmJiYS5vcmcudWtcL3dwLWNvbnRlbnRcL3VwbG9hZHNcLzIwMTVcLzExXC9CQkEtcmVzcG9uc2UtdG8tQ3V0dGluZy1SZWQtVGFwZS1SZXZpZXctRWZmZWN0aXZlbmVzcy1vZi10aGUtVUtzLUFNTC1SZWdpbWUucGRmIiwibmVlZGxvZ2luIjpmYWxzZSwidXNlciI6ZmFsc2V9> accessed 28 June 2019.

Business Insider, ‘Second Life Has Devolved into a Post-Apocalyptic Virtual World, And The Weirdest Thing Is How Many People Still Use It’ <http://www.businessinsider.com/second-life-today-2014-7?op=1&IR=T> accessed 11 June 2015.

Cameron F, ‘Sentences for money laundering getting longer: research’ (Pinsent Masons LLP, OUT-LAW, 2 September 2019) <https://www.pinsentmasons.com/out-law/news/sentences-for-money-laundering-getting-longer-research> accessed 12 September 2019.

Carrefour, ‘Carrefour stores worldwide’ <http://www.carrefour.com/content/carrefour-stores-worldwide> accessed 05 March 2019.

CFTC, ‘Bitcoin and Other Virtual Currencies’ https://www.cftc.gov/Bitcoin/index.htm> accessed 04 September 2019.

CFTC, ‘CFTC Issues Order Finding that Korea Exchange, Inc. Made a False and Misleading Certification to the CFTC’ (Washington, United States, 12 July 2019) <https://www.cftc.gov/PressRoom/PressReleases/7971-19> accessed 03 September 2019.

CFTC, ‘CFTC Orders Dean Katzelis and Shahin Maleki d/b/a Essex Futures to Pay a $500,000 Penalty to Settle Charges of Unauthorized Options Trading, Failure to Supervise, and Other Violations’ (Washington, United States, 12 July 2019) <https://www.cftc.gov/PressRoom/PressReleases/7972-19> accessed 03 September 2019.

CFTC, ‘CFTC Orders Vision Financial Markets LLC to Pay a $200,000 Penalty to Settle Charges that It Failed to Supervise Its Employees’ (Washington, United States, 12 July 2019) <https://www.cftc.gov/PressRoom/PressReleases/7973-19> accessed 03 September 2019.

CFTC, ‘Commodity Pool and its President Ordered to Pay $1.2 Million, Banned from Markets for Futures Fraud’ (Washington, United States, 12 July 2019) <https://www.cftc.gov/PressRoom/PressReleases/7948-19> accessed 03 September 2019.

CFTC, ‘Federal Court Permanently Enjoins Defendants and Orders Them to Pay Penalties and Restitution for Bitcoin Solicitation Fraud, Impersonating a CFTC Investigator, and Sending Forged CFTC Documents’ (Washington, United States, 10 July 2019) <https://www.cftc.gov/PressRoom/PressReleases/7965-19> accessed 03 September 2019.

CFTC, ‘Learn and Protect > Bitcoin > Bitcoin and Other Virtual Currencies’ <https://www.cftc.gov/Bitcoin/index.htm> accessed 03 September 2019.

CFTC, ‘Mission and Responsibilities’ <https://www.cftc.gov/About/MissionResponsibilities/index.htm> accessed 03 September 2019.

CNet, ‘E-currency Site Flooz Goes Offline’ <http://news.cnet.com/2100-1017-271385.html> accessed 12 June 2015.

Coin Desk, ‘What is Bitcoin’ <http://www.coindesk.com/information/what-is-bitcoin/> accessed 23 June 2015.

Coin Map ‘World View’ <https://coinmap.org> accessed 05 March 2019.

Coinbase, ‘Coinbase’ <https://www.coinbase.com/> accessed 23 October 2019.

CoinMarketCap list 2310 currencies on its ‘All Cryptocurrencies’ page: CoinMarketCap, ‘All Cryptocurrencies’ < https://coinmarketcap.com/all/views/all/> accessed 08 August 2019.

Commerce Times, ‘Beenz.com Closes Internet Currency Business’ <http://www.ecommercetimes.com/story/12892.html> accessed 12 June 2015.

Consilium, ‘The presidency of the Council of the EU’ <http://www.consilium.europa.eu/en/council-eu/presidency-council-eu/> accessed 30 September 2019.

Council of Europe ‘Council of Europe Committee of Ministers Recommendation No. R (80) 10’ <https://rm.coe.int/16804f6231> accessed 01 September 2019.

Council of Europe, ‘Chart of signatures and ratifications of Treaty 198’ <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/198/signatures?p_auth=7ynMkkvx> accessed 28 September 2019.

Council of Europe, ‘Details of Treaty No.141’ <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/141> accessed 27 September 2019.

Council of Europe, ‘European Committee on Crime Problems’ <http://www.coe.int/en/web/cdpc> accessed 03 September 2019.

Council of Europe, ‘Resolutions and recommendations elaborated under the authority of the CDPC’ <https://www.coe.int/en/web/cdpc/resolutions-recommendations > accessed 25 September 2019.

Crown Prosecution Service, ‘More than £1.2million of Bitcoin seized from drug dealer’ (19 July 2018) <https://www.cps.gov.uk/south-east/news/more-ps12-million-bitcoin-seized-drug-dealer> accessed 11 September 2019.

Crown Prosecution Service, ‘What We Do’ <http://www.cps.gov.uk/about/> accessed 02 March 2016.

Cryptorunner, ‘How to Get Started with Bitcoin’ <https://cryptorunner.com/get-started-with-bitcoin/> accessed 14 October 2019.

CryptoUK, ‘About Us’ <https://cryptouk.io/about/> accessed 23 October 2019.

CryptoUK, ‘Code of Conduct’ <https://cryptouk.io/codeofconduct/> accessed 23 October 2019.

CryptoUK, ‘CryptoUK hosts 5MLD roundtable at the FCA’ (24 July 2019) https://cryptouk.io/2019/07/24/cryptouk-hosts-5mld-roundtable-at-the-fca/> accessed 23 October 2019.

CryptoUK, ‘CryptoUK Members’ <https://cryptouk.io/members/> accessed 23 October 2019.

CryptoUK, ‘Open Letter to Chancellor Sajid Javid from CryptoUK’ (25 July 2019) <https://cryptouk.io/2019/07/25/open-letter-to-chancellor-sajid-javid-from-cryptouk/> accessed 23 October 2019.

Dai W, ‘b-money’ (1998) <http://www.weidai.com/bmoney.txt> accessed 13 October 2019.

Department of Justice, ‘HSBC Holdings Plc. and HSBC Bank USA N.A. Admit to Anti-Money Laundering and Sanctions Violations, Forfeit $1.256 Billion in Deferred Prosecution Agreement’ (11 December 2012) <https://www.justice.gov/opa/pr/hsbc-holdings-plc-and-hsbc-bank-usa-na-admit-anti-money-laundering-and-sanctions-violations> accessed 23 August 2019.

Department of Justice, ‘Justice News’ <https://www.justice.gov/news> accessed 29 August 2019.

Department of Justice, ‘Iranian Businessman Pleads Guilty to Conspiracy to Violate U.S. Sanctions by Exporting Carbon Fiber From the United States to Iran’ (New York, 29 August 2019) <https://www.justice.gov/opa/pr/iranian-businessman-pleads-guilty-conspiracy-violate-us-sanctions-exporting-carbon-fiber> accessed 29 August 2019.

Department of Justice, ‘Search: Query= bitcoin + money + laundering’ <https://search.justice.gov/search?utf8=%E2%9C%93&affiliate=justice&sort_by=&query=bitcoin+money+laundering> accessed 19 October 2019.

Department of Justice, ‘Standard Chartered Bank Admits to Illegally Processing Transactions in Violation of Iranian Sanctions and Agrees to Pay More Than $1 Billion’ (9 April 2019) <https://www.justice.gov/opa/pr/standard-chartered-bank-admits-illegally-processing-transactions-violation-iranian-sanctions> accessed 23 August 2019.

Department of Justice, U.S. Attorney’s Office Central District of California, ‘“Bitcoin Maven” Sentenced to One Year in Federal Prison in Bitcoin Money Laundering Case’ <https://www.justice.gov/usao-cdca/pr/bitcoin-maven-sentenced-one-year-federal-prison-bitcoin-money-laundering-case> accessed 04 September 2019.

Department of Justice, U.S. Attorney’s Office Southern District of New York, ‘Ross Ulbricht, A/K/A “Dread Pirate Roberts,” Sentenced in Manhattan Federal Court To Life In Prison’ (Manhattan, New York, 29 May 2015) <https://www.justice.gov/usao-sdny/pr/ross-ulbricht-aka-dread-pirate-roberts-sentenced-manhattan-federal-court-life-prison> accessed 05 September 2019.

Department of Justice, U.S. Attorney’s Office Western District of Washington, ‘Multi-State International Drug Trafficking Organization Targeted in 18-Month Investigation’ (Washington, United States, 6 December 2018) <https://www.justice.gov/usao-

wdwa/pr/multi-state-international-drug-trafficking-organization-targeted-18-month-investigation> accessed 04 September 2019.

Department of the Treasury, 'Organizational Structure » Offices » Terrorism and Financial Intelligence' <https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Terrorism-and-Financial-Intelligence.aspx> accessed 30 August 2019.

Dogecoin, 'Dogecoin' <https://dogecoin.com/> accessed 13 October 2019.

Egmont Group of Financial Intelligence Units, 'About' <http://www.egmontgroup.org/about> accessed 27 September 2019

Egmont Group, 'Financial Intelligence Units (FIUs)' <http://www.egmontgroup.org/about/financial-intelligence-units-fius> accessed 11 March 2016.

Ethereum, 'Learn about Ethereum' <https://www.ethereum.org/learn/> accessed 13 October 2019.

eToro, 'eToro' <https://www.etoro.com/> accessed 23 October 2019.

EU2017.EE, 'Estonian Presidency of the Council of the European Union' <https://www.eu2017.ee/> accessed 30 September 2019.

EUROPA, 'Countries' <https://europa.eu/european-union/about-eu/countries_en#28members> accessed 03 September 2019.

EUROPA, 'Court of Justice of the European Union (CJEU)' <https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_en> accessed 02 September 2019.

EUROPA, 'Donald Tusk re-elected president of the European Council' <http://www.consilium.europa.eu/en/press/press-releases/2017/03/09-european-council-president-election/> accessed 01 September 2019.

EUROPA, 'European Commission > About the European Union > Organisational Structure > Locations' <https://ec.europa.eu/info/about-european-union/organisational-structure/locations_en#country> accessed 02 September 2019.

EUROPA, 'European Commission > Political Leadership' <https://ec.europa.eu/info/about-european-union/organisational-structure/political-leadership_en#composition-of-the-college> accessed 25 September 2019.

EUROPA, 'European Commission > The Commissioners > President (2014-2019)' <https://ec.europa.eu/commission/commissioners/2014-2019/president_en> accessed 27 September 2019.

EUROPA, 'European Commission' <https://europa.eu/european-union/about-eu/institutions-bodies/european-commission_en> accessed 27 September 2019.

EUROPA, ‘European Council/Council of the European Union: Home > Contact’ <http://www.consilium.europa.eu/en/contact/> accessed 02 September 2019.

EUROPA, ‘European Council: President’ <http://www.consilium.europa.eu/en/european-council/president/> accessed 01 September 2019.

EUROPA, ‘European Parliament: The President’ <http://www.europarl.europa.eu/the-president/en/> accessed 29 September 2019.

EUROPA, ‘European Parliament’ <https://europa.eu/european-union/about-eu/institutions-bodies/european-parliament_en> accessed 02 September 2019.

EUROPA, ‘Regulations, Directives and Other Acts’ <https://europa.eu/european-union/eu-law/legal-acts_en> accessed 08 September 2019.

EUROPA, ‘Revision of the Anti-Money Laundering Directive (AML). Countering Terrorist Financing’ <http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-revision-of-the-anti-money-laundering-directive-(aml)> accessed 01 September 2019.

EUROPA, ‘Revision of the Fourth Anti-Money-Laundering Directive’ <http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/607260/EPRS_BRI%282017%29607260_EN.pdf> accessed 10 September 2019.

EUROPA, ‘The Institution > Contact Us’ <https://curia.europa.eu/jcms/jcms/Jo2_7022/en/> accessed 02 September 2019.
Europa, https://europa.eu/european-union/about-eu/institutions-bodies/council-eu_en> accessed 29 September 2019.

European Commission, ‘Strengthened EU rules to prevent money laundering and terrorism financing’ <http://ec.europa.eu/newsroom/just/document.cfm?action=display&doc_id=48935> accessed 05 September 2018

European Commission, ‘The euro as legal tender’ <https://ec.europa.eu/info/business-economy-euro/euro-area/euro/use-euro/euro-legal-tender_en> accessed 10 October 2019.

European Commission, ‘Questions and Answers: Anti-money Laundering Directive’ <http://europa.eu/rapid/press-release_MEMO-16-2381_en.htm> accessed 16 September 2019.

European Parliament, ‘Supranational decision-making procedures’ <http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuId=FTU_1.4.1.html> accessed 05 September 2019.

Exchanging, or Using Virtual Currencies' <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf> accessed 04 September 2019.

Facebook, 'Facebook Game Payments' <https://www.facebook.com/help/354773291362154> accessed 02 June 2015.

FBI, 'Ross Ulbricht, aka Dread Pirate Roberts, Sentenced in Manhattan Federal Court to Life in Prison' <https://www.fbi.gov/newyork/press-releases/2015/ross-ulbricht-aka-dread-pirate-roberts-sentenced-in-manhattan-federal-court-to-life-in-prison> accessed 11 March 2016.

FCA, '2019 Fines' (11 October 2019) <https://www.fca.org.uk/news/news-stories/2019-fines> accessed 23 October 2019.

Federal Court of Australia, The Court's Jurisdiction' <http://www.fedcourt.gov.au/about/jurisdiction> accessed 12 August 2015.

Federation of American Scientists, 'Congress Research Service: Money Laundering: An Overview of 18 USC 1956 and Related Federal Criminal Law' <https://www.fas.org/sgp/crs/misc/RL33315.pdf> accessed 11 December 2015.

Financial Action Task Force 'Who We Are' <http://www.fatf-gafi.org/about/> accessed 02 September 2019.

Financial Action Task Force, 'Virtual Currencies – Key Definitions and Potential AML/CFT Risks' <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 27th November 2014.

Financial Action Task Force, 'About Us' <http://www.fatf-gafi.org/pages/aboutus/whatwedo> accessed 09 June 2015.

Financial Action Task Force, 'Annual Report 1995-1996' <http://www.fatf-gafi.org/media/fatf/documents/reports/1995%201996%20ENG.pdf> accessed 03 September 2019.

Financial Action Task Force, 'Anti-money laundering and counter-terrorist financing measures - Australia, Fourth Round Mutual Evaluation Report' <https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Report-Australia-2015.pdf> accessed 23 July 2019.

Financial Action Task Force, 'Anti-money laundering and counter-terrorist financing measures – United Kingdom, Fourth Round Mutual Evaluation Report' (Paris, December 2018) <fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-Kingdom-2018.pdf> accessed 11 September 2019.

Financial Action Task Force, 'Australia – Mutual Evaluation Report – April 2015' <http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Report-Australia-2015.pdf> accessed 05 September 2019.

Financial Action Task Force, ‘FATF IX Special Recommendations’ <http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Standards%20-%20IX%20Special%20Recommendations%20and%20IN%20rc.pdf> accessed 02 September 2019.

Financial Action Task Force, ‘FATF Recommendations – 2003’ <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202003.pdf> accessed 28 September 2019.

Financial Action Task Force, ‘Financial Action Task Force on Money Laundering: Report’ <http://www.fatf-gafi.org/media/fatf/documents/reports/1990%20ENG.pdf> accessed 27 September 2019.

Financial Action Task Force, ‘Guidance for a Risk-Based Approach – Virtual Currencies’ <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf> accessed 04 March 2016.

Financial Action Task Force, ‘Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers’ <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 07 October 2019.

Financial Action Task Force, ‘High-risk and non-cooperative jurisdictions’ <http://www.fatf-gafi.org/countries/#high-risk> accessed 03 September 2019.

Financial Action Task Force, ‘History of the FATF’ <https://www.fatf-gafi.org/about/historyofthefatf/> accessed 14 October 2019.

Financial Action Task Force, ‘Improving Global AML/CFT Compliance: On-going Process - 23 June 2017’ <http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/documents/fatf-compliance-june-2017.html> accessed 04 September 2019.

Financial Action Task Force, ‘IX Special Recommendations’ <http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Standards%20-%20IX%20Special%20Recommendations%20and%20IN%20rc.pdf> accessed 28 September 2019.

Financial action Task Force, ‘Ministers renew the mandate of the Financial Action Task Force until 2020’ <http://www.fatf-gafi.org/publications/fatfgeneral/documents/ministersrenewthemandateofthefinancialactiontaskforceuntil2020.html> accessed 04 September 2019.

Financial Action Task Force, ‘Mutual evaluation of United Kingdom of Great Britain and Northern Ireland’ <http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20UK%20FULL.pdf> accessed 02 March 2016.

Financial Action Task Force, ‘Public Statement - 23 June 2017’ <http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/documents/public-statement-june-2017.html> accessed 03 September 2019.

Financial Action Task Force, ‘Publication Search: Virtual Currencies’ <https://www.fatf-gafi.org/publications/?hf=10&b=0&q=virtual+currencies&s=desc(fatf_releasedate)> accessed 25 June 2019.

Financial Action Task Force, ‘The FATF Recommendations’ <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> accessed 24 September 2019.

Financial Action Task Force, ‘The Forty Recommendations of the Financial Action Task Force on Money Laundering 1990’ <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%201990.pdf> accessed 01 September 2019.

Financial Action Task Force, ‘Third Mutual Evaluation Report on Anti-Money Laundering and Combatting the Financing of Terrorism: United States of America’ <http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20US%20full.pdf> accessed 03 September 2019.

Financial Action Task Force, ‘Topic: Mutual Evaluations’ <http://www.fatf-gafi.org/publications/mutualevaluations/?hf=10&b=0&s=desc(fatf_releasedate)> accessed 04 September 2019.

Financial Action Task Force, ‘United Kingdom’ <https://www.fatf-gafi.org/countries/#United%20Kingdom> accessed 11 September 2019.

Financial Action Task Force, ‘Virtual Currencies – Key Definitions and Potential AML/CFT Risks’ <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 27th November 2014.

Financial Action Taskforce, ‘FATF Report to the G20 Finance Ministers and Central Bank Governors’ <http://www.fatf-gafi.org/media/fatf/documents/reports/FATF-Report-G20-FM-CBG-July-2018.pdf> accessed 23 July 2018.

Financial Conduct Authority, ‘About the FCA’ (24 April 2016) <https://www.fca.org.uk/about/the-fca> accessed 17 September 2019.
Financial Conduct Authority, ‘Anti-Money Laundering Annual Report 2012/13’ <http://www.fca.org.uk/static/documents/anti-money-laundering-report.pdf> accessed 15 June 2015.

Financial Conduct Authority, ‘Anti-money laundering Annual report 2018/19’ (09 July 2019) <https://www.fca.org.uk/publication/corporate/annual-report-2018-19-anti-money-laundering.pdf> accessed 18 September 2018.

Financial Conduct Authority, ‘Cryptoassets: Our Work’ (23 January 2019) https://www.fca.org.uk/firms/cryptoassets> accessed 20 September 2019.

Financial Conduct Authority, ‘Cryptoassets’ (07 March 2019) <https://www.fca.org.uk/consumers/cryptoassets> accessed 23 September 2019.

Financial Conduct Authority, ‘Enforcement’ (22 April 2016) <https://www.fca.org.uk/about/enforcement> accessed 18 September 2019.

Financial Conduct Authority, ‘FCA fines Deutsche Bank £163 million for serious anti-money laundering controls failings’ (31 January 2017) <https://www.fca.org.uk/news/press-releases/fca-fines-deutsche-bank-163-million-anti-money-laundering-controls-failure> accessed 18 September 2019.

Financial Conduct Authority, ‘FCA fines Standard Chartered Bank £102.2 million for poor AML controls’ 09 April 2019) <https://www.fca.org.uk/news/press-releases/fca-fines-standard-chartered-bank-102-2-million-poor-aml-controls> accessed 18 September 2019.

Financial Conduct Authority, ‘FCA publishes Feedback Statement on Distributed Ledger Technology’ (15 December 2017) <https://www.fca.org.uk/news/press-releases/fca-publishes-feedback-statement-distributed-ledger-technology> accessed 13 October 2019.

Financial Conduct Authority, ‘Guidance on Cryptoassets – Consultation Paper’ <https://www.fca.org.uk/publication/consultation/cp19-03.pdf> accessed 19 March 2019.

Financial Conduct Authority, ‘Guidance on Cryptoassets: Feedback and Final Guidance to CP 19/3’ (London, July 2019) <https://www.fca.org.uk/publication/policy/ps19-22.pdf> accessed 23 September 2019.

Financial Conduct Authority, ‘How and why consumers buy cryptoassets: A report for the FCA’ (07 March 2019) <https://www.fca.org.uk/publication/research/how-and-why-consumers-buy-cryptoassets.pdf> accessed 23 September 2019.

Financial Conduct Authority, ‘Money laundering and terrorist financing’ (03 August 2015) <https://www.fca.org.uk/firms/financial-crime/money-laundering-terrorist-financing> accessed 17 September 2019.

Financial Times, ‘Length of UK prison terms for money launderers hits record high’ (1 September 2019) <https://www.ft.com/content/846c0e5c-c9a4-11e9-af46-b09e8bfe60c0> accessed 12 September 2019.

Financial Times, ‘Lexicon: Definition of a Currency Swap’ <http://lexicon.ft.com/Term?term=currency-swap> accessed 17 June 2015.

Financial Times, ‘Lexicon: Definition of Disposable Income’ <http://markets.ft.com/research/Lexicon/Term?term=disposable-income> accessed 18 June 2015.

FinCEN, ‘Annual Report 2010’ <https://www.fincen.gov/news_room/rp/files/annual_report_fy2010.pdf> accessed 22 September 2019.

FinCEN, ‘Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies’ (9 May 2019) <https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf> accessed 04 September 2019.

FinCEN, ‘A Quick Reference Guide for Money Services Businesses’ (Washington, United States, September 2007) <https://www.fincen.gov/sites/default/files/shared/bsa_quickrefguide.pdf> accessed 04 September 2019.

FinCEN, ‘Enforcement Actions’ (18 April 2019) <https://www.fincen.gov/news-room/enforcement-actions> accessed 23 October 2019.

FinCEN, ‘FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger’ (Washington, 5 May 2015) <https://www.fincen.gov/sites/default/files/enforcement_action/2016-08-02/20150505.pdf> accessed 02 September 2019.

FinCEN, ‘FinCEN’s Strategic Plan’ <https://www.fincen.gov/about/fincens-strategic-plan> accessed 02 September 2019.

FinCEN, ‘Guidance - FIN-2013-G001 - Issued: March 18, 2013 - Subject: Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies’ <https://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf> accessed 06 August 2019.

FinCEN, ‘In the Matter of BTC-E a/k/a Canton Business Corporation and Alexander Vinnik’ (Vienna, United States, 07 June) <2017https://www.fincen.gov/sites/default/files/enforcement_action/2017-07-27/Assessment%20for%20BTCeVinnik%20FINAL2.pdf> accessed 02 September 2019.

FinCEN, ‘In the Matter of Eric Powers’ (Vienna, United States, 18 April 2019) https://www.fincen.gov/sites/default/files/enforcement_action/2019-04-18/Assessment%20Eric%20Powers%20Final%20for%20Posting%2004.18.19_1.pdf > accessed 02 September 2019.

FinCEN, ‘Law Enforcement Overview’ <https://www.fincen.gov/resources/law-enforcement-overview> accessed 30 August 2019.

FinCEN, ‘Mission’ <https://www.fincen.gov/about_fincen/wwd/mission.html> accessed 03 September 2019.

FinCEN, ‘Reporting Suspicious Activity – A Quick Reference Guide for Money Services Businesses’ <https://www.fincen.gov/statutes_regs/guidance/pdf/msbsar_quickrefguide.pdf> accessed 14 December 2015.

FinCEN, ‘Suspicious Activity Report Statistics (SAR Stats)’ <https://www.fincen.gov/reports/sar-stats> accessed 21 August 2019.
FinCEN, ‘What We Do’ <https://www.fincen.gov/about_fincen/wwd/index.html> accessed 03 December 2015.

Forbes, <http://www.forbes.com/sites/erikkain/2014/11/19/world-of-warcraft-tops-10-million-subscribers-following-warlords-of-draenor-expansion/> accessed 11 June 2015.

Gemini, ‘What is Gemini?’ <https://gemini24.zendesk.com/hc/en-us/articles/204732945-What-is-Gemini-> accessed 18 December 2015.

GOV.UK, ‘Cryptoassets Taskforce: final report’ (30 July 2018) <https://www.gov.uk/government/publications/cryptoassets-taskforce> accessed 20 September 2019.

GOV.UK, ‘Digital currencies: call for information’ <https://www.gov.uk/government/consultations/digital-currencies-call-for-information/digital-currencies-call-for-information> accessed 11 March 2016.

GOV.UK, ‘Digital currencies: response to the call for information’ <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf> accessed 11 March 2016.

GOV.UK, ‘Digital currencies: response to the call for information’ <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf> accessed 24 September 2019.

GOV.UK, ‘The National Crime Agency A plan for the creation of a national crime-fighting capability’ https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97826/nca-creation-plan.pdf> accessed 02 March 2016.

Hannah Murphy, ‘Europol meets cryptocurrency exchanges to thwart criminals’ Financial Time (London, 19 June 2018) <https://www.ft.com/content/9430a3b0-73d4-11e8-b6ad-3823e4384287> accessed 14 October 2019.

Henderson H, ‘application programming interface (API)’ in Harry Henderson (ed) Encyclopedia of Computer Science and Technology (3rd ed, Facts On File, 2017) <https://search-credoreference-

com.ezproxy.uwe.ac.uk/content/entry/fofcomputer/application_programming_interface_api/0> accessed 20 October 2019.

IGN, ‘IGN Presents the History of World of Warcraft’ <http://uk.ign.com/articles/2009/08/18/ign-presents-the-history-of-warcraft> accessed 11 June 2015.

International Monetary Fund, ‘Money Laundering: the Importance of International Countermeasures’ <http://www.imf.org/external/np/speeches/1998/021098.htm> accessed 15 June 2015.

Inland Revenue Service, ‘IRS/FinCen Form 8300’ <https://www.irs.gov/pub/irs-pdf/f8300.pdf> accessed 15 December 2015.

Inland Revenue Service, ‘Notice 2014-21’ <https://www.irs.gov/pub/irs-drop/n-14-21.pdf> accessed 17 December 2015.

Joint Money Laundering Steering Group, ‘Prevention of money laundering/combating terrorist financing: Part I, 2017 REVISED VERSION’ (13 December 2017) <http://www.jmlsg.org.uk/download/10005> accessed 21 October 2019.

Korte K, ‘Postal Annex Owner Sentenced for Structuring Currency Transactions’ (DEA, 11 September 2018) <https://www.dea.gov/press-releases/2018/09/11/postal-annex-owner-sentenced-structuring-currency-transactions> accessed 06 August 2019.

Legisaltion.Gov, ‘Your search for UK Public General Acts has returned more than 200 results’ < https://www.legislation.gov.uk/ukpga> accessed 20 September 2019.

Linden Labs, ‘Become a Second Life Premium Member’ <https://secondlife.com/my/account/membership.php> accessed 11 June 2015.

Linden Labs, ‘LindeX™ Exchange’ <https://secondlife.com/my/lindex/#> accessed 28 August 2018.

Linden Labs, ‘Second Life Market Place’ <https://marketplace.secondlife.com/?lang=en-US> accessed 11 June 2015.

Linden Labs, ‘What is Second Life’ <http://secondlife.com/whatis/> accessed 11 June 2015.

LiteCoin, ‘LiteCoin’ <https://litecoin.org/> accessed 13 October 2019.

Makuck E, Gamespot (3 November 2015) <https://www.gamespot.com/articles/blizzard-will-no-longer-report-world-of-warcraft-s/1100-6431943/> accessed 29 March 2019.

Maltego, ‘Visualising the Bitcoin Blockchain in Maltego’ (12 April 2016) <http://maltego.blogspot.com/2016/04/visualization-bitcoin-blockchain-in.html> accessed 07 October 2019.

'Money Laundering, n.' (OED Online, OUP June 2016) <http://www.oed.com/view/Entry/121171?redirectedFrom=money+laundering+#eid36244231> accessed 06 September 2019.

Mori SAK, ‘Leader of International Drug Money Laundering Organization Sentenced to 30 Years in Prison’ (DEA, 14 August 2018) <https://www.dea.gov/press-releases/2018/08/14/leader-international-drug-money-laundering-organization-sentenced-30> accessed 06 August 2019.

National Crime Agency, ‘RAF sergeant and pensioner jailed for involvement in £1m drug dealing ring’ <https://www.nationalcrimeagency.gov.uk/news/raf-sergeant-and-pensioner-jailed-for-involvement-in-1m-drug-dealing-ring?highlight=WyJtb25leSIsImxhdW5kZXJpbmciLCJsYXVuZGVyIiwibGF1bmRlcmVkIiwibGF1bmRlcmVycyIsImxhdW5kZXJlciIsImxhdW5kZXJlcidzIiwibGF1bmRlcnMiLCJtb25leSBsYXVuZGVyaW5nIl0=> accessed 19 September 2019.

National Crime Agency, ‘Cyber Crime’ <https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime?highlight=WyJiaXRjb2luIiwiYml0Y29pbnMiXQ==> accessed 20 September 2019.

National Crime Agency, ‘Economic Crime Command’ <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime> accessed 02 March 2016.

National Crime Agency, ‘Economic Crime Command’ <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime> accessed September 2019.

National Crime Agency, ‘Ex-Goldman Sachs investment banker ordered to pay back £7.3 million’ (06 September 2019) <https://www.nationalcrimeagency.gov.uk/news/ex-goldman-sachs-investment-banker-ordered-to-pay-back-7-3-million> accessed 19 September 2019.

National Crime Agency, ‘Governance and transparency’ <https://www.nationalcrimeagency.gov.uk/who-we-are/governance-and-transparency> accessed 17 September 2019.

National Crime Agency, ‘High End Money Laundering: Strategy and Action Plan’ <http://www.nationalcrimeagency.gov.uk/publications/625-high-end-money-laundering-strategy/file> accessed 02 March 2016.

National Crime Agency, ‘National Crime Agency Annual Report and Accounts 2015–16’ (London, 21 July 2016) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attach

ment_data/file/583545/NCA_Annual_Report_and_Accounts_2015-16__web_.pdf> accessed 15 September 2019.

National Crime Agency, 'National Crime Agency Annual Report and Accounts 2016–17' (London, 20 July 2017) <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/25-nca-annual-report-2016-17/file> accessed 15 September 2019.

National Crime Agency, 'National Crime Agency Annual Report and Accounts 2017–18' (London, 19 July 2018) <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/177-nca-annual-report-accounts-2017-18/file> accessed 15 September 2019.

National Crime Agency, 'National Economic Crime Centre' <https://www.nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-centre> accessed 19 September 2019.

National Crime Agency, 'National Strategic Assessment of Serious and Organised Crime 2017' <http://www.nationalcrimeagency.gov.uk/publications/807-national-strategic-assessment-of-serious-and-organised-crime-2017/file> accessed 05 September 2018.

National Crime Agency, 'Our Mission' <https://www.nationalcrimeagency.gov.uk/who-we-are/our-mission> accessed 19 September 2019.

National Crime Agency, 'Seventy years for multi-million pound drugs and money laundering group' (26 July 2019) <https://www.nationalcrimeagency.gov.uk/news/seventy-years-for-multi-million-pound-drugs-and-money-laundering-group> accessed 19 September 2019.

National Crime Agency, 'Student behind $100m dark web site jailed for 5 years 4 months' (12 April 2019) <https://www.nationalcrimeagency.gov.uk/news/student-behind-100m-dark-web-site-jailed-for-5-years-4-months?highlight=WyJiaXRjb2luIiwiYml0Y29pbnMiXQ==> accessed 11 September 2019.

National Crime Agency, 'Suspicious Activity Reports (SARs) Annual Report 2014' (London, 24 March 2015) <http://www.octf.gov.uk/OCTF/media/OCTF/images/publications/SARS-Annual-Report-2014.pdf?ext=.pdf> accessed 15 September 2019.

National Crime Agency, 'Suspicious Activity Reports (SARs) Annual Report 2015' (London, 18 May 2017) <https://nationalcrimeagency.gov.uk/who-we-are/publications/2-sars-annual-report-2015/file> accessed 15 September 2019.

National Crime Agency, 'Suspicious Activity Reports (SARs) Annual Report 2018' (London, 15 March 2019) <https://nationalcrimeagency.gov.uk/who-we-are/publications/256-2018-sars-annual-report/file> accessed 15 September 2019.

National Crime Agency, ‘The cyber threat to UK business 2017/18’ (10 April 2018) <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/178-the-cyber-threat-to-uk-business-2017-18/file> accessed 20 September 2019.

National Crime Agency, ‘UK Financial Intelligence Unit’ <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/ukfiu> accessed 04 March 2016.

National Crime Agency, ‘What We Do’ <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do> accessed 02 March 2016.

Northern Territory Government: Department of Attorney General and Justice, ‘Penalty Units’ <https://nt.gov.au/employ/money-and-taxes/taxes,-royalties-and-grants/territory-revenue-office/penalty-units> accessed 22 July 2019.

Organization for Economic Co-operation and Development, ‘Gross Domestic Product’ <http://stats.oecd.org/glossary/detail.asp?ID=1163> accessed 15 June 2015.

Organization for Economic Co-operation and Development, ‘Harmful Tax Competition; An Emerging Global Issue’ <http://www.OECD.org/tax/transparency/44430243.pdf> accesse17 June 2015.

Oxford English Dictionary, ‘Analysis’ <https://en.oxforddictionaries.com/definition/analysis> accessed 10th September 2019.

Oxford English Dictionary, ‘pacta sunt servanda’ <http://www.oed.com/view/Entry/135875?redirectedFrom=pacta+sunt+servanda#eid> accessed 08 September 2019.

Parks S, ‘Houston Man Sentenced for Federal Drug Trafficking and Money Laundering Violations’ (DEA, 17 May 2019)<https://www.dea.gov/press-releases/2019/05/17/houston-man-sentenced-federal-drug-trafficking-and-money-laundering> accessed 06 August 2019.

Parliament of Australia, ‘Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2017’ <https://parlinfo.aph.gov.au/parlInfo/download/legislation/billsdgs/5592699/upload_binary/5592699.pdf;fileType=application/pdf> accessed 16 July 2019.

PayPal, ‘About Paypal’ <https://www.paypal.com/uk/webapps/mpp/about> accessed 17 June 2015.

Sentencing Council, ‘Fraud, bribery and money laundering offences: Definitive guideline’ <https://www.sentencingcouncil.org.uk/wp-content/uploads/Fraud-bribery-and-money-laundering-offences-Definitive-guideline2.pdf> accessed 15 September 2019.

Serious Organised Crime Agency, ‘Suspicious Activity Reports Regime: Annual Report 2010’ (London, 26 November 2010) <https://www.octf.gov.uk/OCTF/media/OCTF/images/publications/SARS%20Annual%20Report/SARs-Annual-Report-2010.pdf?ext=.pdf> accessed 15 September 2019.

The European Union, ‘The EU in Brief’ <https://europa.eu/european-union/about-eu/eu-in-brief_en> accessed 26 August 2016.

Thompson Reuters, ‘Liberty Reserve founder must face $6 bln laundering case in U.S.’ <http://www.reuters.com/article/usa-cybersecurity-liberty-reserve-idUSL1N11T2G420150923> accessed 11 March 2016.

Transparency International-Bond Anti-Corruption Group, ‘Report on the UK’s Compliance with the UN Convention Against Corruption’ <https://www.transparency.org.uk/wp-content/plugins/download-attachments/includes/download.php?id=901> accessed 10 June 2019.

Treasury and Finance, ‘Indexation of Fees and Penalties’ <https://www.dtf.vic.gov.au/financial-management-government/indexation-fees-and-penalties> accessed 22 July 2019.

United Nations Development Programme, ‘Human Development Reports: 2018 Statistical Update’ (14 December 2018) <http://hdr.undp.org/en/2018-update> accessed 14 October 2019.

United Nations Office of Drug Control, ‘Basic Manual on the Detection and Investigation of the Laundering of Crime Proceeds Using Virtual Currencies’ <https://www.imolin.org/pdf/imolin/FULL10-UNODCVirtualCurrencies_final.pdf> accessed 10 June 2019.

United Nations Office on Drugs and Crime, ‘About the UNODC’ <https://www.unodc.org/unodc/en/about-unodc/index.html?ref=menutop> accessed 02 September 2019.

United Nations Office on Drugs and Crime, ‘Basic Manual on the Detection and Investigation of the Laundering of Crime Proceeds Using Virtual Currencies’ <http://www.imolin.org/pdf/UNODC_VirtualCurrencies_final_EN_Print.pdf> accessed 01 September 2019.

United Nations Office on Drugs and Crime, ‘Illicit Money: How Much is Out There?’ <http://www.unodc.org/unodc/en/frontpage/2011/October/illicit-money_-how-much-is-out-there.html> accessed 15 June 2015.

United Nations Office on Drugs and Crime, ‘Political Declaration and Plan of Action on International Cooperation towards an Integrated and Balanced Strategy to Counter the World Drug Problem’ <https://www.unodc.org/documents/ungass2016/V0984963-English.pdf> accessed 05 September 2019.

United Nations Office on Drugs and Crime, ‘UNODC on Money Laundering and Countering the Financing of Terrorism’ <https://www.unodc.org/unodc/en/money-laundering/index.html?ref=menuside> accessed 03 September 2019.

United Nations Office on Drugs Crime, ‘Signature and Ratification Status’ <https://www.unodc.org/unodc/en/corruption/ratification-status.html> accessed 10 June 2019.

United Nations Security Council, ‘Resolution 1617 (2005)’ <http://unscr.com/en/resolutions/doc/1617> accessed 10 June 2019.

United Nations, ‘About Us’ <https://www.un.org/ecosoc/en/about-us> accessed 02 September 2019.

United Nations, ‘Fifty First General Assembly Session: Agenda item 168, Renewing the United Nations: A Programme for Reform’ <https://www.un.org/ga/search/view_doc.asp?symbol=A/51/950> accessed 07 June 2019.

United Nations, ‘Functions and powers of the General Assembly’ <http://www.un.org/en/ga/about/background.shtml> accessed 01 September 2019.

United Nations, ‘History of the United Nations’ <http://www.un.org/en/sections/history/history-united-nations/index.html> accessed 01 September 2019.

United Nations, ‘International Court of Justice’ <http://www.icj-cij.org/court/index.php?p1=1> accessed 01 September 2019.

United Nations, ‘Secretariat’ <http://www.un.org/en/sections/about-un/secretariat/index.html> accessed 02 September 2019.

United Nations, ‘Trusteeship Council’ <http://www.un.org/en/sections/about-un/trusteeship-council/index.html> accessed 02 September 2019.

United Nations, ‘What is the Security Council’ <http://www.un.org/en/sc/about/> accessed 02 September 2019.

United Nations, Overview’ <http://www.un.org/en/sections/about-un/overview/index.html> accessed 01 September 2019.

United States Department of Justice, ‘Standard Chartered Bank Admits to Illegally Processing Transactions in Violation of Iranian Sanctions and Agrees to Pay More Than $1 Billion’ <https://www.justice.gov/opa/pr/standard-chartered-bank-admits-illegally-processing-transactions-violation-iranian-sanctions> accessed 05 August 2019.

United States Government Accountability Office, ‘Virtual Currencies: Emerging Regulatory, Enforcement, and Consumer Protection Challenges’ <http://gao.gov/assets/670/663678.pdf> accessed 04 September 2019.

United States Treasury, ‘National Money Laundering Risk Assessment’ <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf> accessed 5 September 2019.

US Department of State, ‘2015 INCSR: Money Laundering/Financial Crimes Countries’ <https://2009-2017.state.gov/j/inl/rls/nrcrpt/2014/vol2/222471.htm> accessed 23 October 2019.

US Department of State, ‘Duties of the Secretary of State’ <http://www.state.gov/secretary/115194.htm> accessed 18 October 2019.

US Department of the Treasury, ‘About>Terrorism and Financial Intelligence’ <http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Terrorism-and-Financial-Intelligence.aspx> accessed 16 October 2019

US Department of the Treasury, ‘Duties & Functions of the U.S. Department of the Treasury’ <https://home.treasury.gov/about/general-information/role-of-the-treasury> accessed 20 October 2019.

US Department of the Treasury, ‘National Money Laundering Risk Assessment 2015’ <http://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf> accessed 20 November 2015.

US Department of the Treasury, ‘Resource Centre – Money Laundering’ <http://www.treasury.gov/resource-center/terrorist-illicit-finance/Pages/Money-Laundering.aspx> accessed 16 November 2015.

US Securities Exchange Commission, ‘About the SEC’ <http://www.sec.gov/about/whatwedo.shtml> accessed 04 December 2015.

US Securities Exchange Commission, ‘Investor Alert: Beware of Fantasy Stock Trading Websites Offering Real Returns’ <https://www.investor.gov/news-alerts/investor-alerts/investor-alert-beware-fantasy-stock-trading-websites> accessed 18 December 2015.

US Securities Exchange Commission, ‘Investor Alert: Bitcoin and Other Virtual Currency-Related Investments’ <http://www.investor.gov/news-alerts/investor-alerts/investor-alert-bitcoin-other-virtual-currency-related-investments> accessed 18 December 2015.

US Securities Exchange Commission, ‘Investor Alert: Ponzi Schemes Using Virtual Currencies’ <https://www.investor.gov/news-alerts/investor-alerts/investor-alert-ponzi-schemes-using-virtual-currencies> accessed 18 December 2015

US Securities Exchange Commission, ‘SEC Halts $32 Million Scheme That Promised Riches from Amber Mining’ <https://www.investor.gov/news-alerts/press-

releases/sec-halts-32-million-scheme-promised-riches-amber-mining> accessed 18 December 2015.

US Securities Exchange Commission, ‘SPEECH - Anti-Money Laundering: An Often-Overlooked Cornerstone of Effective Compliance’ <http://www.sec.gov/news/speech/anti-money-laundering-an-often-overlooked-cornerstone.html> accessed 04 December 2015.

US Securities Exchange Commission, ‘Spotlight on Anti-Money laundering Rulemaking’ <https://www.sec.gov/spotlight/moneylaundering.htm> accessed 04 December 2015.

US Senate, ‘HSBC Exposed U.S. Financial System to Money Laundering, Drug, Terrorist Financing Risks’ <https://www.hsgac.senate.gov/subcommittees/investigations/media/hsbc-exposed-us-finacial-system-to-money-laundering-drug-terrorist-financing-risks> accessed 05 August 2016.

US Department of Justice, ‘2007 National Money Laundering Strategy’ <http://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/nmls.pdf> accessed 20 November 2015.

US Department of Justice, ‘Agencies’ <http://www.justice.gov/agencies/chart#OAG> accessed 03 December 2015.

White & Chase, ‘New UK AML Action Plan – The Increased Role of the Private Sector’ (London, April 2016) <https://www.whitecase.com/sites/whitecase/files/files/download/publications/new-uk-aml-action-plan-the-increased-role-of-the-private-sector.pdf> accessed 15 September 2019.

Wilsons Auctions, ‘£500k of bitcoin seized from UK criminal to be auctioned, with no reserve!’ (19 September 2019) <https://www.wilsonsauctions.com/news/500k-of-bitcoin-seized-from-uk-criminal-to-be-auctioned-with-no-reserve/> accessed 30 September 2019.

Wolfsberg Group, ‘Mission’ <https://www.wolfsberg-principles.com/about/mission> accessed 14 October 2019.

XE, ‘1 AUD to EUR = 0.628131 Euros’ <https://www.xe.com/currencyconverter/convert/?Amount=1&From=EUR&To=AUD> accessed 23 July 2019.

XE, ‘1 AUD to USD = 0.700376 US Dollars’ <https://www.xe.com/currencyconverter/convert/?Amount=1&From=AUD&To=USD> accessed 23 July 2019.

XE, ‘500,000 USD to AUD = 709,773.06 Australian Dollars’ <https://www.xe.com/currencyconverter/convert/?Amount=500%2C000&From=USD&To=AUD> accessed 22 July 2019.

XE, ‘EUR to USD Chart’ <http://www.xe.com/currencycharts/?from=EUR&to=USD&view=5Y> accessed 24 September 2019.

XE, ‘USD per 1 GBP’ <http://www.xe.com/currencycharts/?from=GBP&to=USD&view=5Y> accessed 23 September 2019.

XE, ‘USD per 1 XBT’ <https://www.xe.com/currencycharts/?from=XBT&to=USD&view=2Y> accessed 07 August 2019.

XE, ‘XE Currency Charts: XBT to GBP’ <https://www.xe.com/currencycharts/?from=XBT&to=GBP&view=5Y> accessed 12 September 2019.

XE, ‘XE Currency Charts: XBT to USD’ <https://www.xe.com/currencycharts/?from=XBT&to=USD&view=10Y> accessed 07 October 2019.

XE, ‘XE Currency Table: XBT - Bitcoin’ <https://www.xe.com/currencytables/?from=XBT&date=2019-01-01> accessed 07 August 2019.