Anti-Money Laundering: The legal and enforcement response to Cryptoassets in the United Kingdom

Amy Yu-Tsu Chen
Doctor of Philosophy (PhD) Thesis
City, University of London
The City Law School
September 2021

Table of Contents

To my family

Acknowledgment

Sincere gratitude goes to Professor Jason Chuah, my thesis supervisor at The City Law School, who triggered my interest in money laundering the niche to which this thesis belongs. Above all I wholeheartedly thank my parents, who provided all kinds of support and have ensured by personal sacrifices that I receive the best possible education. This thesis is dedicated to them.

Abbreviations

5th Anti-Money Laundering Directive ("AMLD5")
Anti-Money Laundering ("AML")
Counter Terrorist Financing ("CTF")
Decentralised Applications ("DApps")
Distributed Ledger Technology ("DLT")
Electronic Money Regulation 2017 (SI 2017/99) ("EMRs")
Enhanced Due Diligence ("EDD").
European Banking Authority ("EBA")
European Economic Area ("EEA")
European Securities Markets Authority ("ESMA")
European Union ("EU")
Financial Action Task Force ("FATF")
Financial Conduct Authority ("FCA")
Financial Services and Markets Act 2000 ("FSMA 2000")
Her Majesty's Treasury ("HM Treasury")
Initial Coin Offering ("ICO")
Initial Public Offering ("IPO")
International Swaps and Derivatives Association ("ISDA")
Joint Money Laundering Steering Group ("JMLSG")
Know Your Customer ("KYC")
Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulation 2017 ("MLRs")
National Crime Agency ("NCA")
Norwich Pharmacal order ("NPO")
Payment Services Regulations 2017 (SI 2017/752) ("PSRs 2017")
Peer-to-Peer ("P2P")
Proceeds of Crime Act 2002 ("POCA")
Sanctions and Anti-Money Laundering Act 2018 ("SAMLA")
Securities and Exchange Commission ("SEC")
Serious Organised Crime and Police Act 2005 (the "SOCPA 2005")
Simplified Due Diligence ("SDD")
Temporary Registration Regime ("TRR")
United Kingdom ("UK")
United States ("US")
Virtual Private Network ("VPN")

Legislation

Civil Jurisdiction and Judgments Act 1982
Civil Procedure Rules
Companies Act 2006
Contempt of Court Act 1981
Criminal Finances Act 2017
Directive 2014/65/ Markets in Financial Instruments (MiFID II)
Directive 2018/843 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending directives 2009/13/EC and 2013/36/EC.
EC 1206/2001: Regulation on co-operation between the courts of the member states in the taking of evidence in civil or commercial matters.
EC 1215/2012: Recast regulation on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.
EC 2015/848: Wire Transfer Regulation
EC 2018/1673: Sixth Money Laundering Directive
Electronic Money Regulation 2011
EU 1215/2012 Regulations on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters ('Recast Brussels Regulation')
Fees (Cryptoasset Business) Instrument 2020
Financial Conduct Authority Handbook
Financial Services and Markets Act 2000
Fourth Money Laundering Directive (EU 2015/848)
Fraud Act 2006
Hague Convention
Human Rights Act 1998
Market in Financial Instruments Regulation (600/2014)
Patents Act 1977
Payment Services Regulations 2017/752
Practice Direction
Proceeds of Crime Act 2002
Sanctions and Anti-Money Laundering Act 2018
Senior Courts Act 1981
Serious Crime Act 2015
Serious Organised Crime and Police Act 2005
The Criminal Finances Act 2017
The Fifth Money Laundering Directive
The Money Laundering and Terrorist Financing (Amendment) Regulations 2019
The Money Laundering Regulations 2017
The Law of Property Act 1925
The Serious Organised Crime and Police Act 2005
Theft Act 1968

Case Law

AA v Persons Unknown [2019] EWHC 3556 (Comm).
AB Bank Ltd v Abu Commercial Bank PJSC [2016] EWHC 2082.
Agip (Africa) Ltd v Jackson [1990] Ch 265.
Air India v Wiggins [1980] 2 All ER 593; Cox v Army Council [1963] AC 48.
American Cyanamid Co (No 1) v Ethicon Ltd [1975] UKHL 1.
Arab Monetary Fund v Hashim (No 8) [1989] WLR 565.
Arcadia Petroleum Ltd and others v Bosworth and others [2015] EWHC 3700.
Armstrong DLW GmbH v Winnington Networks Ltd [2012] EWHC 10 (Ch).
B2C2 Limited v Quoine PTE Limited [2019] SGHC (I) 3.
Bacon v Automattic Inc [2011] EWHC 1072 (QB).
Bank of Ireland v Pexxnett Ltd and others [2010[EWHC 1872.
Bank St Petersburg PJSC and another v Arkhangelsky and another [2020] EWCA Civ 408.
Banque Belge Pour I'Etranger v Hambrouck [1921] 1 KB 321.
BDW Trading Ltd v Fitzpatrick and another [1989] WLR 656.
Borden (UK) Ltd v Scottish Timber Products Ltd [1981] Ch 25.
Burns v The Financial Conduct Authority [2017] EWCA Civ 2140.
Cayne v Global Natural Resources Plc [1984] 1 All ER 225.
Colonial Bank v Whinney [1885] 30 Ch.D 261.
Commerzbank v IMB Morgan plc [2004] EWHC 2771 (Ch).
Commissioners of Police of the Metropolis v Ebanks [2012] EWHC 2368 (Admin).
Cpod SA v de Holanda Jr [2020] EWHC 1247 (Ch).
Dadourian Group v Simms [2006] EWCA Civ 399.
Derby & Co v Weldon [1990] 1 WLR 1139.
Director of the Assets Recovery Agency v Green [2005] EWHC 3168 (admin).
DW Trading Ltd v Fitzpatrick and another [1989] WLR 656.
EI Ajou v Dollar Land Holdings plc [1993] EWCA Civ 4.
Euroil Ltd v Cameroon Offshore Petroleum SARL [2014] EWHC 52.
Foskett v McKeown [2001] 1 AC 102.
Glencore International AG v Metro Trading Inc (No 2) [2001] 1 Lloyd's Rep 284.
HM Commissioners of Customs and Excise v Barclays Bank plc [2006] UKHL 28.
Hogan v Directors of Public Prosecutions [2007] EWHC 978.
Ion Science Ltd v Persons Unknown (unreported), 21 December 2020 (Commercial Court).
Joint Stock Company Aeroflot-Russian Airlines v Berezovsky and Glushkov [2014] EWCA Civ 20.
Joseph Constantine Steamship Line Ltd v Imperial Smelting Corporation Ltd [1942] AC 154.
JSC BTA Bank v Ablyazov and another [2016] EWHC 230 (Comm).
JSC BTA Bank v Ablyazov and others [2013] EWHC 510 (Comm).
Kensington International Ltd v Republic of Congo [2007] EWCA Civ 1128.
Lipkin Gorman v Karpnale Ltd [1988] UKHL 12.
LJY v Persons Unknown [2017] EWHC 3230 (QB).
Lockton Companies International v Persons Unknown [2009] EWHC 3423.
MacKinnon v Danaldson Lufkin & Jenrette Securities [1986] Ch 482.
Mahme Trust Reg and others v Lloyds TSB Bank Plc [2004] EWHC 1931 (Ch).
McGreevy v DPP [1973] 1 WLR 276.
McKinnon v Donaldson Lufkin and Jenrette Securities Corp [1986] Ch 484.
Miler v Minister of Pension [1947] 2 All ER 372.
Murphy v Murphy [1999] 1 WLR 282.

N v The Royal Bank of Scotland Plc [2019] EWHC 1770 (Comm)
National Crime Agency v Azam [2014] EWHC 4742 (QB).
National Crime Agency v Zamira Hajiyeva [2018] EWHC 2534
National Provincial Bank Ltd v Ainsworth [1965] AC 1175.
National Provincial Bank v Ainsworth [1965] 1 AC 1175.
National Provincial Bank v Ainsworth [1965] UKHL 1.
Norwich Pharmacal v Commissioner of Customs & Excise [1974] UKHL 6.
OBG v Allan [2007] UKHL 21.
OJSC Oil Company Yugraneft v Abramovich [2008] EWHC 2613 (Comm).
Pace and Anor v R [2014] EWCA Crim 186.
Paysera LT (UAB "EVP International" v Lieuvos bankas (Case C-389/17)
PML v Persons Unknown [2018] EWHC 838 (QB).
Poly Peck International PLC v Nadir (No. 2) [1992] 4 All ER 769.
R v Akhtar (Urfan) [2011] EWCA Crim 146.
R v Anwar [2013] EWCA Crim 1865.
R v Anwoir and others [2008] EWCA Crim 1354.
R v Benjafield and others [2002] UKHL 2
R v Da Silva [2006] EWCA Crim 1654
R v Fazal [2009] EWCA Crim 1697.
R v Gabriel (Janis) [2006] EWCA Crim 229, [2007] 1.W.L.R. 2272.
R v GH [2015] UKSC 24.
R v Gillard (Simon Paul) (1988) Cr. App R 189.
R v Greenfield [1973] 1 WLR 1151.
R v Grossman [1981] 73 Cr App R 302.
R v Haque [2019] EWCA Crim 1028.
R v Loizou (Lisa) [2005] EWCA Crim 1579
R v Otegbola [2017] EWCA Crim 1147.
R v Rizvi [2002] UKHL 1.
R v Rogers (Bradley David) [2014] EWCA Crim 1680.
R v Rollins [2010] WLR 1922.
R v Saik (Abdulrahman) [2006] UKHL 18.
R v Smith (Wallace Duncan) (No 4) [2004] 3 WLR 229.
R v Smith (Wallace Duncan) (No 4) [2004] Cr App R 17.
R v Thompson [2010] EWCA Crim 1216.
R v Waya [2012] UK SC 51.
Re Diplock [1948] Ch 465.
Re Doherty [2008] UKHL 33.
Re H (Minors) (Sexual Abuse: Standard of Proof) [1996] AC 563.
Re S-B (Children) [2008] UKHL 33.
Reading v Attorney General [1949] 2 KB 232.
Robertson v Persons Unknown [2019] unreported.
Ruscoe v Cryptopia Ltd (in Liquidation) [2020] NZHC 783.
Sabados v Facebook Ireland [2018] EWHC 2369.
Series 5 Software Ltd v Clarke [1996] 1 ALL ER 853.
Serious Organised Crime Agency v Perry [2012] UKSC 350.
Skatteverket v Hedqvist (Case C-264/14) [2015] BVC 34.
SRA v Olayemi Daniel [2015] 11343-2015.
SRA v Tidd [2013] 11178-2013.

The Satanita [1897] AC 59.
Vitol SA v Capri Marine Ltd [2010] EWHC 458.
Vorotyntseva v Money-4 Limited [2018] EWHC 2596.
VTB Capital plc v Nutritek International Corp and others [2013] UKSC 5.
Wakelin v London & South Western Railway Co [1886] 12 App CAS.
Westdeutsche Landesbank Girozentrale v Islington LBC [1996] AC 669.
Westdeutsche Landesbank Girozentrale v Islington LBC [1996] UKHL 12.
Williams v Central Bank of Nigeria [2014] UK SC 10.
Woolmington v DPP [1935] UKHL 1.
Your Response v Datastream Business Media [2014] EWCA Civ 281.
YS GM Marfin II LLC & Ors v Muhammad Ali Lakhani & Ors [2020] EWHC 2629.

Abstract

There is a virtual battle incubating at the moment concerning the future of cryptoassets and the stability of the global financial system. Accordingly, crypto money laundering is one of the most significant economic problems of the 21st century, with substantial social and geopolitical implications. It enables criminals to take advantage of this global technology. This poses a huge threat to national sovereignty since there is a potential for massive movements of illicit assets, which could shift national currencies and overthrow the global financial system. It is submitted that crypto money laundering is not a "victimless crime". The individual or the innocent third parties or the country from which the cryptoasset is stolen are, by definition, the victims, whilst the cryptoasset is used in the host country to support the criminal's lifestyle or other illicit activities such as drug importation, human trafficking, child sexual exploitation, prostitution, terrorism, tax evasion and fraud.

The purpose of this research is to provide a comprehensive theoretical framework that can be applied to the implementation of the United Kingdom's ("UK") Anti-Money Laundering ("AML") rules within the crypto sector. This research concludes that imposing conventional AML rules and assuming that the crypto community is an arm of law enforcement is counterproductive and could provoke programmers to develop new crypto protocols that are more autonomous, and as a result, are harder to detect and enforce. This thesis examines the crypto money laundering problem both generally and in the UK in particular. More specifically, this research sets out the primary forms and types of crypto money laundering schemes and the devices used; and the crypto AML framework that can be applied to the enforcement of the AML regulations in the UK. Nonetheless, at the start of this research, it is important to note that the crypto sector in the UK as well as abroad was essentially unregulated. For that reason, this research extends beyond existing works that have offered insight into the broad workings of the crypto sector and its legal implications. In short, this thesis offers originality in providing a thorough overview of the crypto laws, regulations, and the relevant case law pertaining to cryptoassets in the UK.

Chapter 1: Introduction

"*Technology itself has no agency: it is the choices people make about it that shape the world*"
– The Economist.[1]

Cryptoassets' extremely rapid growth, and then fall, both in terms of the number of tokens and prices and their challenge to the current financial infrastructure, are forcing international regulators as well as market participants to monitor and understand this new trend closely. Cryptoassets are virtual assets or commodities that are created, stored, and governed electronically by an open or closed system, on a decentralised or centralised DLT. There are over 5,005 cryptoassets with a market cap of $213 billion, with Bitcoin being the largest, representing 69% of the market according to CoinMarketCap.[2] Bitcoin, the first cryptoasset, launched in early 2009, has overtaken many competing cryptoassets, many of which still fall back to Bitcoin as the support currency. Overall, cryptoassets could be applicable in areas where current payments systems are slow, such as across jurisdictions and borders, as payment, access or reward tokens or used to fund other blockchain projects, as well as parts of the criminal underworld.

Cryptoassets are unlikely to disappear and will survive in various forms and shapes among different market participants, from those who desire greater decentralisation, peer-to-peer networks and anonymity, to central bankers who desire centralisation, close networks and know your customer ("KYC") as well as enhanced due diligence ("EDD"). However, in a world of heightened scrutiny over money laundering and terrorism funding, it is hard to imagine any government allowing anonymous transactions to take place given domestic as well as international law commitments.[3] Here, anonymous transactions will test civil and criminal laws

[1] The Economist, 'Pessimism v progress' (The Economist, 21 December 2019). <https://www.economist.com/leaders/2019/12/18/pessimism-v-progress> accessed 28 August 2021.

[2] CoinMarketCap, 'All Cryptocurrencies' (CoinMarketCap, January 2020) <https://coinmarketcap.com/all/views/all/> accessed 28 August 2021.

[3] HM Treasury, 'National risk assessment of money laundering and terrorist financing 2017' (HM Treasury, October 2017) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/655198/National_risk_assessment_of_money_laundering_and_terrorist_financing_2017_pdf_web.pdf> accessed 28 August 2021.

that require firms to establish the identities of those involved in a transaction, as well as the end use of the underlying commodity or service being transacted.

Sir Geoffrey, Chancellor of the High Court, gave a speech to the Joint Northern Chancery Bar Association. His key message was that the tech community should have faith in the English legal system to understand the technology; and more importantly, reinforced the notion that their rights and obligation will be upheld and enforced in English courts.[4] Accordingly, the debate has moved on from "whether Bitcoin is money" to the UK recognising cryptoassets as property[5] and smart contracts as enforceable under the laws of England and Wales.[6] Traditionally, following *National Provincial Bank Ltd v Ainsworth*,[7] property must be definable, identifiable by third parties, capable of assumption by third parties and have some degree of permanence or stability. It is found that, cryptoassets are identifiable by third parties, and thus, are capable of assumption by third parties. Moreover, cryptoassets can be held as well as transferred, and in turn, the degree of permanence or stability are established because all transactions are recorded in the blockchain which cannot be altered.

A crypto network is considered to be an electronic database that consists of structured information; here, the physical medium and the rights are treated as property, whilst the information itself is not property.[8] However, the distinction between the crypto network (database information) and cryptoassets. The UK Jurisdictional Taskforce concluded that while a cryptoasset may not be considered a chose in action, under the traditional definition,[9] this does not preclude cryptoassets from being property.[10] Here, the cryptoasset itself and the private key are divided into two distinct elements; the former is held to be property, whilst the latter is

---

4 Sir Geoffrey Vos, "Cryptoassets as property: how can English law boost the confidence of would-be parties to smart legal contracts?' (UK Courts and Tribunals Judiciary, May 2019) < https://www.judiciary.uk/announcements/speech-by-sir-geoffrey-vos-chancellor-of-the-high-court-cryptoassets-as-property/> accessed 28 August 2021.

5 Robertson v Persons Unknown [2019] unreported, CL-2019-000444.

6 UK Jurisdictional Taskforce, 'Legal statement on cryptoassets and smart contracts' (Tech Nation, November 2019) <https://technation.io/news/uk-takes-significant-step-in-legal-certainty-for-smart-contracts-and-cryptocurrencies/> accessed 28 August 2021.

7 [1965] AC 1175.

88 Your Response v Datastream Business Media [2014] EWCA Civ 281.

9 OBG v Allan [2007] UKHL 21.

10 Supra (n 6) Jurisdictional Taskforce.

regarded as information, thus not capable of being property.[11] In other words, cryptoassets do have some degree of permanence, which are definable, identifiable and capable of enforcement by third parties.[12] It is important to note, the case law pertaining to cryptoassets are still developing. Nonetheless, decisions, such as *AA v Persons Unknown*[13] and *Ion Science Ltd v Persons Unknown*,[14] are critical *interim* decisions transforming the law within the crypto space. *Ion Science Ltd v Persons Unknown Others,*[15] is an important decision concerning the emerging case law in relation to Initial Coin Offerings ("ICO"). The applicants submitted that they had been victims of ICO fraud. The first applicant is a company registered in England and Wales and a second applicant is a natural person domiciled in the UK. The Commercial Court at the Royal Courts of Justice granted a proprietary injunction and a worldwide freezing order over the relevant digital property. The judgement follows *AA v Persons Unknown*,[16] an earlier decision finding that a cryptoasset such as Bitcoin was a form of property capable of being the subject of a proprietary injunction, accepting the analysis by the UK Jurisdictional Taskforce's Legal Statement on cryptoassets and smart contracts.[17]

Generally, there is a natural delay between the emergence of new technologies, broad adoption then ultimately, mass regulation and enforcement. For instance, the US Securities and Exchange Commission announced it filed an emergency action and obtained a restraining order against the Telegram Group concerning its alleged illegal offering of securities called "Grams" tokens, which already raised more than $1.7 billion USD.[18] Historically, the privilege of acting as the issuer of a 'private' asset generally comes with obligations to safeguard the financial system from market abuse and fraud; namely, AML concerns. This is not a small ask. Each

[11] ibid.

[12] [2019] EWHC 3556 (Comm).

[13] ibid.

[14] (unreported), 21 December 2020 (Commercial Court).

[15] ibid

[16] Supra (n 12).

[17] The same conclusion was also reached in New Zealand in the case of Ruscoe v Cryptopia Ltd (in Liquidation) [2020] NZHC 783.

[18] The US Securities Exchange Commission, 'SEC Halts Alleged $1.7 Billion Unregistered Digital Token Offering' (SEC, 11 October 2019) <https://www.sec.gov/news/press-release/2019-212> accessed 28 August 2021.

year, European banks spend approximately $20 billion on AML compliance.[19] Whilst North American firms spend more than $31.5 billion annually on AML compliance.[20] Therefore, applying similar regulation to crypto businesses, particularly those designed to facilitate cross-border transactions, such as Libra (rebranded as "Diem"),[21] remains a key area of focus for international regulators.

The European Banking Authority ("EBA") advocates for consistency in the accounting treatment of cryptoassets, i.e. holding of cryptoassets should be treated as an intangible asset.[22] The Chairman of the United States ("US") Commodity Futures Trading Commission confirmed that Bitcoin[23] and Ether[24] is a commodity under the US Commodity Exchange Act. Subsequently, both the HM Revenue and Customs[25] and the Internal Revenue Service[26] issued new tax guidance with regards to activities involving cryptoassets and money laundering.[27] It is submitted that, money laundering is a critical enabler of serious and organised crime, which costs the UK more than GBP 37 billion every year.[28] More importantly, crypto money laundering is not a "victimless crime', since it enables criminals as well as the most powerful

[19] Pawel Kuskowski, 'The Step that would save European Banks Twenty Billion Dollars' (Forbes, 10 September 2018) <https://www.forbes.com/sites/pawelkuskowski/2018/09/10/the-step-that-would-save-european-banks-twenty-billion-dollars/> accessed 28 August 2021.

[20] Lexis Nexis, 'North American Financial Services Firms Spend More than $31.5 Billion a Year on Anti-Money Laundering Compliance According to LexisNexis Risk Solution Study' (LexisNexis, 23 July 2019) <https://risk.lexisnexis.com/about-us/press-room/press-release/20190723-true-cost-aml> accessed 28 August 2021.

[21] Nikhilesh De, "Libra Rebrands to 'Diem' in Anticipating of 2021 Launch" (Coindesk, 1 December 2020) <https://www.coindesk.com/libra-diem-rebrand> accessed 28 August 2021.

[22] European Banking Authority, 'Report with advice for the European Commission' (EBA, 9 January 2019) <https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf> accessed 28 August 2021.

[23] The US Commodity Futures Trading Commission, 'Bitcoin Basics' (CFTC, December 2019) <https://www.cftc.gov/sites/default/files/2019-12/oceo_bitcoinbasics0218.pdf> accessed 28 August 2021.

[24] The US Commodity Futures Trading Commission, 'IN CASE YOU MISSED IT: Chairman Tarbert Comments on Cryptocurrency Regulation at Yahoo! Finance All Markets Summit' (CFTC, 10 October 2019) <https://www.cftc.gov/PressRoom/PressReleases/8051-19> accessed 28 August 2021.

[25] HMRC, 'Policy paper Cryptoassets for individuals' (HMRC, 19 December 2018) <https://www.gov.uk/government/publications/tax-on-cryptoassets/cryptoassets-for-individuals> accessed 28 August 2021.

[26] IRS, 'Virtual currency: IRS issues additional guidance on tax treatment and reminds taxpayers of reporting obligations' (IRS, 9 October 2019) <https://www.irs.gov/newsroom/virtual-currency-irs-issues-additional-guidance-on-tax-treatment-and-reminds-taxpayers-of-reporting-obligations> accessed 28 August 2021.

[27] Skatteverket v Hedqvist (Case C-264/14) [2015] BVC 34.

[28] HM Treasury, Money Laundering and Terrorist Financing (Amendment) Regulations 2019 (Explanatory Memorandum, No. 1511, December 2019) <http://www.legislation.gov.uk/uksi/2019/1511/memorandum/contents> accessed 28 August 2021.

in society to take advantage of the fragmented approach to crypto regulation around the world. In order words, crypto money laundering is one of the most significant economic problems of the 21st century, with huge social and geopolitical implications.[29] Cryptoassets, regardless of size, have implications ranging from AML efforts across different jurisdictions to operational resilience (i.e. cybersecurity and hacking), to consumer and investor data protection concerns to crypto tax avoidance. Against this backdrop of issues, there is an international battle commencing at the moment in relation to future of the global financial system. In one corner, the US, which has been the leader of the global monetary system, in another corner, the Chinese government, launched the Digital Yuan, a cryptoasset 'with Chinese characteristics' which could be used to reinforce the government's surveillance and censorship capabilities at both micro and macroeconomic levels.[30] In the third corner, the challenge of a private cryptoasset created by Facebook, which could pose a real threat to national sovereignty and the international monetary system.[31] Finally, in the fourth corner are the Cypherpunks, who want to overthrow the global financial system by "*using cryptographic technology to build communities invisible to the state and multinational corporations*".[32] As a result, the geopolitical risk associated with cryptoassets are creating tensions around the world, with many countries concerned that the underlying technology could undermine the global financial system, and more importantly, proliferate money laundering.

Parliament launched the UK Jurisdictional Taskforce to investigate and address the impact of the crypto sector.[33] Accordingly, the UK Jurisdictional Taskforce have asked the Law

[29] Geopolitical risk is defined as the risk associated with cryptoassets that proliferates tensions between international states. In the context of crypto money laundering, the individual or the country from which the cryptoasset is stolen are, by definition, the victims, whilst the cryptoasset is used in the host country to support the criminal's lifestyle or confiscated by the local government. In short, geopolitical risks emerge when the international system is undergoing a disruption or transformation.

[30] Alice Ekman, *China's Blockchain and Cryptocurrency Ambitions* (Brief, European Union Institute for Security Studies, 2021)

[31] Jahja Rrustemi and Nils Tuchschmid, "Facebook's Digital currency venture "Diem": the new Frontier…or a Galaxy far, far away?" (*Technology Innovation Management Review*, December 2020) <https://timreview.ca/article/1407> accessed 28 August 2021.

[32] Brady Dale, "Cypherpunk, Crypto Anarchy and How Bitcoin Lost the Narrative" (*CoinDesk*, 24 November 2020) <https://www.coindesk.com/tech/2020/11/24/cypherpunk-crypto-anarchy-and-how-bitcoin-lost-the-narrative/> accessed 28 August 2021.

[33] HM Treasury, "UK regulatory approach to cryptoassets and stablecoins: Consultation and call for evidence" (HM Treasury, January 2021) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950206/HM_Treasury_Cryptoasset_and_Stablecoin_consultation.pdf> accessed 28 August 2021.

Commission to make recommendations to ensure that the UK is capable of accommodating cryptoassets as well as other emerging technology (such as smart contracts and DeFi).[34] During the span of this research, the crypto landscape changed rapidly from an entirely unregulated market to a somewhat regulated sector. This chapter will unfold in two parts. Firstly, this chapter will examine how the current AML framework will apply to the cryptoassets, and thereafter, how the new regulations will apply to crypto businesses in the UK. As mentioned in the previous paragraphs, the relevant period, as outlined in this research, describes a period where cryptoassets were unregulated (2018) to a somewhat regulated crypto sector (2021). In short, this chapter aims to provide an overview of the underlying technology and provides a framework as to how they will be categorised and regulated in the UK. For research purposes, the doctrinal method will be used to examine a combination of legislative as well as non-legislative rules surrounding cryptoassets.

As the crypto market continues to mature, the legal as well as compliance challenges remain high, and whilst the technology led to a surge in alternative tokens (i.e. Dogecoin) many cryptoassets as well as crypto businesses have questionable structures that enables crypto money laundering which supports the criminal underworld. As a result, the UK government have imposed specific requirements in relation to each relevant cryptoasset and/or crypto business implemented through a case-by-case approach.[35] As indicated in the previous chapter, the debate has moved on from 'whether Bitcoin is money' to the UK recognising cryptoasset as property. As a result, the UK is at a critical juncture in developing an internationally recognised regulatory standard for cryptoassets and in turn develop an FCA approved smart contract protocol. (This concept will be further developed in Chapters 5 and 6).

It is submitted that, the world is ready for private money, as most of the money in the world derive from private issuers (private banks). However, crypto businesses will face many regulatory hurdles, coupled with significant regulatory oversight due to costly AML/KYC/CTF compliance obligations. For instance, in April 2020, the Diem Association published a White

[34] Law Commission, 'Adapting English Law for the digital revolution' (Law Commission, 21 September 2020) <https://www.lawcom.gov.uk/adapting-english-law-for-the-digital-revolution/> accessed 28 August 2021.

[35] Bank of England, 'Discussion Paper: Central Bank Digital Currency' (Bank of England, March 2020) <https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf> accessed 28 August 2021.

Paper, which made several amendments to its initial business model, namely: [1] enhancing the safety of the Diem payment platform with a sophisticated compliance framework focusing on AML, KYC, CTF and sanctions obligations; [2] forgoing the notion of a permissionless and anonymous blockchain system; and [3] implementing strong protections in relation to the design of the Diem reserve (as per above).[36] Following these assertions, Diem will likely qualify as a 'virtual currency' under European Union's 5th Anti-Money Laundering Directive ("AMLD5"),[37] and subsequently, are in scope as a 'crypto-asset exchange provider' under the MLR.[38] In order words, Facebook's Diem ecosystem (the custodial wallet providers as well as the fiat-to-crypto and vice versa)[39] must follow the EU as well as the UK's AML framework, if it plans to offer its services to EU costumers. Nonetheless, the EU has warned Facebook against operating in the EU, unless it receives prior approval from the EU commission.[40]

Here, the MLR and the FATF's recommendations in relation to cryptoassets are essentially a baseline framework, aimed at harmonising the international approach to cryptoassets. Here, the UK has gone beyond the FATF's recommendations,[41] however, it is submitted that, Parliament must adopt an evidence-based approach when creating its crypto AML framework. More importantly, the UK should recognise the transformative potential of cryptoassets. However, the UK crypto sector is relatively small.[42] Here, the UK's combined trade volume represents less than 1% of the daily global trade in cryptoassets.[43] Thus given the size of the crypto sector in the UK, the overall money laundering risks are still relatively low, when compared to the global crypto market. Notwithstanding this assertion, crypto money laundering risks increases at the point of exchange, for instance, businesses that provides fiat-

[36] Libra, 'Welcome to the official Libra White Paper' (Libra, 2020) <https://libra.org/en-US/white-paper/> 10 June 2020.

[37] The Fifth Money Laundering Directive ("AMLD5"), Article 1(2)(d)

[38] MLRs 2017, Regulation 14A(1).

[39] AMLD5, Article 3(18)-(19)

[40] Finextra, 'European Union unsure how to regulate Facebook's Libra' (Finextra, 20 February 2020) <https://www.finextra.com/newsarticle/35318/european-union-unsure-how-to-regulate-facebooks-libra> accessed 28 August 2021.

[41] HM Treasury "Transposition of the Fifth Money Laundering: consultation" (HM Treasury, April 2019) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/795670/20190415_Consultation_on_the_Transposition_of_5MLD__web.pdf>

[42] FCA, 'Guidance on Cryptoassets: Consultation Paper: CP19/3' (FCA, January 2019) <https://www.fca.org.uk/publication/consultation/cp19-03.pdf> accessed 28 August 2021.

[43] ibid.

to-crypto, or crypto-to-fiat, or crypto-to-crypto conversion, are more vulnerable to money laundering than other crypto businesses. As a result, firms engaged in crypto exchange or fiat conversion services are more susceptible money laundering. Nonetheless, it is also important to underline the global nature of crypto transactions. For instance, a crypto firm registered in another jurisdiction could circumvent the regulatory standards established in the UK, and as a result, non-UK firms would not be compelled to implement the required AML/KYC checks.

At the start of this research, there was no single definition, nor any commonly agreed taxonomy concerning the classification of cryptoassets that distinguishes each type of cryptoasset by feature or use. Nonetheless, the UK recognised that clarity and legal certainty for market participants concerning the rules surrounding cryptoassets are essential to encourage and support innovations. The lack of legal certainty is often identified as the primary obstacle for the crypto sector in the UK.[44] What makes a cryptoasset so special? Here, the underlying technology enables the transfer of assets in a secure and traceable way that is practically immutable through cryptograph. [45] As a result, the academic debate is twofold. On the one hand, cryptoassets are considered to be an asset recorded in a digital form, which does not represent a financial claim on, nor a financial liability of, any natural or legal person, which do not embody a proprietary right against an entity.[46] On the other hand, cryptoasset are held to represent any asset (including claims and other rights of traditional assets) that is created, stored or transferred on the blockchain, which interchangeably also assert certain proprietary right against the cryptoasset.[47] This assertion will be further explored in Chapter 4.

Chiara Zilioli, the Deputy General Counsel of the European Central Bank, examined the complex nature of cryptoassets.[48] In her article titled, 'Cryptoassets: legal characterisation and challenges under private law', she argues that, 'given the global nature of the crypto-asset

[44] ibid.

[45] Economist, 'The Promise of the blockchain: The trust machine" (Economist, 31 October 2015) <https://www.economist.com/leaders/2015/10/31/the-trust-machine> accessed 28 August 2021.

[46] ECB Crypto-Asset Trask Force, *Cryptoassets: Implications for financial stability, monetary policy, and payments and markets infrastructures* (Occasional Paper Series No. 223, May 2019) <https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf> accessed 28 August 2021.

[47] Liechtenstein Government, 'Blockchain Act Liechtenstein' (*Liechtenstein Government*, October 2019) <https://impuls-liechtenstein.li/en/blockchain-act-liechtenstein/> accessed 28 August 2021.

[48] Chiara Zilioli, 'Crypto-assets: legal challenges under private law' (2020) 45 European Law Review 2, 251-266.

phenomenon, only an international agreement, or at least the adoption of international standards, will be able to tackle this challenge'.[49] Here, it is submitted that, the novelty of cryptoassets will undermine the conventional AML framework in a number of ways: [1] Firstly, cryptoassets are created and transferred via the blockchain. [2] Secondly, a cryptoasset created on a blockchain platform, will do not automatically give rise to a proprietary right against another entity. [3] Thirdly, most cryptoassets are not traditional assets, which do not represent a financial claim nor a financial liability. [4] Fourthly, most cryptoassets derives its own intrinsic value. [5] Finally, given the non-materiality and the anonymity of cryptoassets, the rights of individuals may not be effectively recognised nor enforced. Following this assumption, it is therefore impossible for regulators to step in, as there is no clear answer.

As of March 2020, crypto businesses will be governed by the MLR, which adopts the AMLD5,[50] as a means to ensure the UK meets global AML standards.[51] In addition, Part II of Joint Money Laundering Steering Group ("JMLSG") report provides guidance in relation to the governance of crypto exchanges and custodian wallet providers.[52] As a result, crypto exchanges and custodian wallet providers must meet the required standards under the MLR and register with the FCA.[53] However, Her Majesty's Treasury ("HM Treasury") opened a new consultation due to the community's slow registration rate,[54] since a high number of crypto firms have not met the required FCA standards under MLR.[55] As a result, the HM Treasury announced an extension, from the 9th of July 2021 to the 31st of March 2022, to register with the FCA for

[49] ibid at 2.

[50] Directive 2018/843 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending directives 2009/13/EC and 2013/36/EC.

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

[52] Joint Money Laundering Steering Group, 'Further amendments to JMLSG Guidance' (JMLSG, 10 January 2020) <http://www.jmlsg.org.uk/industry-guidance/article/jmlsg-guidance-current> accessed 28 August 2021.

[53] Financial Conduct Authority, "Cryptoassets: Find out about the regulation of cryptoassets (including "cryptocurrencies" such as Bitcoin and Litcoin) and the risks of investing and making payments using cryptoassets" (FCA, 7 March 2019) <https://www.fca.org.uk/consumers/cryptoassets> accessed 28 August 2021.

[54] HM Treasury, "Call for Evidence: Review if the UK's AML/CFT regulatory and supervisory regime" (HM Treasury, 22 July 2021) <https://www.gov.uk/government/consultations/call-for-evidence-review-of-the-uks-amlctf-regulatory-and-supervisory-regime> accessed 28 August 2021.

[55] HM Treasury, "Amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (information on the Payer) regulation 2017 Statutory Instrument 2022" (HM Treasury, 22 July 2021) <https://www.gov.uk/government/consultations/amendments-to-the-money-laundering-terrorist-financing-and-transfer-of-funds-information-on-the-payer-regulations-2017-statutory-instrument-2022> accessed 28 August 2021.

AML compliance. Here, the HM Treasury hopes to receive feedback from the crypto community in order to provide further clarity on how the AML, CTF and KYC framework should operate in the UK.[56] HM Treasury are of the view that crypto businesses should implement and enforce the FATF's Travel Rule, as per Recommendation 16,[57] which requires crypto firms to send and record information in relation to the originator and beneficiary of each crypto transaction.[58] The question posed here is, how can a crypt firm facilitate its main client business whilst simultaneously overseeing the implementation of national as well as international AML efforts?[59]

This thesis sets out to investigate the role of AML regulations in dealing with crypto money laundering. As a result, the overarching research question is: *How will the AMLD5 and amendments to the MLR influence the crypto sector in the UK*. More specifically, the research questions are as follows: [1] How can cryptoassets facilitate money laundering? [2] How do issuers and users of crypto exploit cryptoassets to bypass the MLR? [3] Can the MLR help manage the risks associated with cryptoassets? Accordingly, this research seeks to investigate, now can the law incentivise the implementation the MLR and the Proceed of Crimes Act ("POCA") within the crypto sector, an agency perspective. This research seeks to examine the agency tension and relationships, in order to enhance the study of crypto money laundering. This research aspires to trace the structural themes in relation to how the MLR and the POCA will shape the crypto sector and look beyond the regulatory measures. It is viewed that, the regulatory reforms suggested by Parliament can be characterised as short-sighted. In short, the current AML framework does not (and will not) address the structural pathology of cryptoassets. As a potential solution, Parliament can mandate the use of a FCA approved smart contract for every crypto transaction transacted in the UK. In this instance, the agency relationship between the FCA and the crypto firm will be neutral since the AML enforcement will be administered by the FCA through an automated AML system governed by the state.

[56] ibid.

[57] Financial Action Trask Force, *International Standards on combating money laundering and the financing of terrorism and proliferation* (FATF Recommendations, June 2021) < https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/fatf%20recommendations%202012.pdf> accessed 28 August 2021.

[58] ibid.

[59] ibid.

Thus, from the perspective of this research, the UK will be the primary jurisdiction of interest. However, given the international reach of cryptoassets, this research also takes inspiration from other tech-forward jurisdictions. The purpose of this research is to provide a comprehensive crypto AML framework that can be applied to the enforcement of the AML regulation in the UK.[60] As a result, this research extends beyond existing work that has offered insight into the crypto sector. In short, this thesis offers originality in providing a thorough overview of the crypto laws, regulations, and the relevant case law in relation to cryptoassets in the UK.

International cooperation is critical due to the global nature of the underlying technology, making cryptoassets well suited for carrying out money laundering and facilitating crimes at an international scale. The FCA must work closely with the crypto community as well as with foreign partners to conduct investigations, makes arrests and seize criminal assets in cases concerning cryptoassets. Thus, this research aspires to trace these structural themes in relation to how the MLR and the POCA will shape the crypto sector in the UK and look beyond the regulatory implementation. As a consequence, the regulatory reforms suggested by the FCA can be characterised as short-sighted. It is submitted that the current AML framework does not (and will not) address the structural pathology of cryptoassets. By 'structural pathology', it is defined as the inability of the law to produce high and sustainable compliance within the crypto sector. This research concludes that imposing conventional AML rules and assuming that the crypto community is an arm of law enforcement is counterproductive and could provoke programmers to develop new crypto protocols that are more autonomous, and as a result, are harder to detect and enforce. Moreover, this research must investigate the current AML framework, as a starting point, in order to pinpoint the obstacle(s) that will emerge between the FCA and the crypto sector.

Overall, the debate over the merits and the dangers of Bitcoin have surfaced in the news with varying degrees of urgency. As interest concerning Bitcoin began to spread, additional cryptoassets were created. The reactions from regulators have also differed widely, as have the use and development of cryptoassets. In particular, some of the divergence in public reactions stem from the lack of distinction drawn between cryptoassets in general and Bitcoin.

[60] This research commenced in 2018, when the crypto sector was essentially unregulated.

Cryptoassets includes Bitcoin; however, not all cryptoassets are Bitcoin. For instance, Bitcoin transactions are anonymous, whilst the more FinTech related cryptoassets, such as Diem coin,[61] JPM coin,[62] and the Cuatrecasas token,[63] are not anonymous. As a result, given that cryptoassets can *potentially* be more efficient and secure, most regulators have in principle, accepted and may have encouraged the development of cryptoassets. However, the anonymous and pseudonymous nature of some cryptoassets, such as Bitcoin and Monero,[64] continues to trouble many regulators, especially in relation to crypto money laundering.

The combination of rapidly growing volumes of cryptoassets with different functions and change in how the DLT is used, stored and processed, opens up a wide range of opportunities for stakeholders. Whilst cryptoassets may have promising features, in the unregulated form, this technology is prone to illicit applications, more specifically, in relation to financial crime, money laundering, terrorist financing and tax evasion. As a result, crypto exchanges and custodian wallet providers must meet the required standards under the MLR and register with the FCA.[65] However, only five crypto firms have received the appropriate AML designation from the FCA to operate in the UK,[66] In order words, most crypto firms currently operating in the UK, are not authorised by the FCA and do not meet the required AML standards under MLR.[67] For instance, Binance advertised as the "*best and cheapest crypto exchange in*

[61] Camilla Hodgson, Hannah Murphy and Martin Coulter, 'Cryptocurrency enthusiasts hate, and love, Libra coin' (Financial Times, 19 June 2019) <https://www.ft.com/content/5cbc38e0-91d8-11e9-b7ea-60e35ef678d2> accessed 28 August 2021.

[62] Mary Ann Russon, 'JP Morgan creates first US bank-backed crypto-currency' (BBC News, 14 February 2019) <https://www.bbc.co.uk/news/business-47240760> accessed 28 August 2021.

[63] Iberian Lawyer, 'Cuatrecasas issues blockchain tokens for legal services' (Iberian Lawyer, 18 February 2019) <http://www.iberianlawyer.com/news/news/8382-cuatrecasas-issues-blockchain-tokens-for-legal-services> accessed 28 August 2021.

[64] Tom Wilson, 'Explainer: 'Privacy coin' Monero offers near total anonymity' (Reuters, 15 May 2019) <https://www.reuters.com/article/us-crypto-currencies-altcoins-explainer/explainer-privacy-coin-monero-offers-near-total-anonymity-idUSKCN1SL0F0> accessed 28 August 2021.

[65] Financial Conduct Authority, "Cryptoassets: Find out about the regulation of cryptoassets (including "cryptocurrencies" such as Bitcoin and Litcoin) and the risks of investing and making payments using cryptoassets" (FCA, 7 March 2019) <https://www.fca.org.uk/consumers/cryptoassets> accessed 28 August 2021.

[66] Joshua Oliver, "Barclays stops UK clients from sending funds to Binance" (Financial Times, 5 July 2021) <https://www.ft.com/content/abc04cc0-ea53-4ecb-8c1e-49c85014fa3f> accessed 28 August 2021.

[67] Mary-Ann Russon, "Binance: Watchdog clamps down on cryptocurrency exchange" (BBC News, 28 June 2021) <https://www.bbc.co.uk/news/business-57632831> accessed 28 August 2021.

the UK",[68] was banned by FCA from undertaking any regulated activities in the UK.[69] Subsequently, Binance stopped its UK customers from withdrawing from their crypto accounts.[70] The move extends a regulatory crackdown on the crypto sector over concerns about Binance's potential involvement in money laundering and fraud.[71]

In the 2018 "National Strategic Assessment of Serious and Organised Crime" report, the National Crime Agency ("NCA") found that "*a small but growing number of criminals are laundering money using crypto[assets] and anticipates that criminals will increasing use crypto[assets] to move illicit funds across borders*". In 2020, the NCA report established that crypto-investment fraud is also an emerging area of concern and "*UK-based criminals continue to identify new ways of using virtual assets, such as crypto[assets] to launder their profits, although more traditional methods are still favoured*". This Chapter underlines the different types of cryptoassets and how money laundering can be committed whilst simultaneously identifying the challenges for law enforcement. This thesis sets out to identify and analyse factors that give rise to crypto money laundering and introduce the relevant laws and statutory instruments. For instance, the FCA have indicated that the UK will apply the same AML rules to cryptoassets as traditional financial instruments. However, conventional AML rules are normally implemented by intermediaries, such as banks, clearing houses, etc., but cryptoassets have no intermediaries. It is important to note the negative externalities posed by crypto money laundering, namely, it causes economic, political, social as well as compliance loss to both the crypto firm and the FCA.

As a result, the value of this technology for the economy and society will depend on its use. For instance, a cryptoasset used as a vehicle of crime may proliferate AML challenges; and could subsequently, pose an increased risk to market abuse, financial crime and, in the extreme,

---

[68] Wilfred Michael, "13 Best Crypto Exchanges in the UK" (Bitcourier, 2021) <https://bitcourier.co.uk/blog/crypto-exchanges-uk> accessed 28 August 2021.

[69] Financial Conduct Authority, "Consumer warning on Binance Markets Limited and the Binance Group" (FCA, 26 June 2021) <https://www.fca.org.uk/news/news-stories/consumer-warning-binance-markets-limited-and-binance-group> accessed 31 August 2021.

[70] Adam Samson, "Binance customers face extensive sterling withdrawal outage" (Financial Times, 29 June 2021) <https://www.ft.com/content/2d427ed7-f9e4-46cf-a4c4-46429b19df5d> accessed 28 August 2021.

[71] Priscila Azevedo Rocha and Joanna Ossinger, "UK Financial Regulator bars Exchange Binance Market" (Bloomberg, 27 June 2021) <https://www.bloomberg.com/news/articles/2021-06-27/u-k-financial-regulator-bars-crypto-exchange-binance> accessed 31 August 2021.

financial instability. Based on these assumptions, it is not difficult to see the parallel between this scenario and geopolitical risks deriving from the rise of cryptoassets. For instance, cryptoassets can be used to circumvent international sanctions and cross-border transactions. As a result, law enforcement must work closely with foreign partners to conduct investigations, make arrests, and seize criminal assets when the relevant cryptoasset are transferred abroad. In short, whether an English order or judgment can be enforced abroad will depend on the law of that particular country. Unfortunately, the law in relation to the process and enforcement of crypto money laundering is still unclear. Nonetheless, there has been a great deal of research and debate devoted to the potential use of cryptoassets and whether cryptoassets can be categorised as money or a legal tender, capable of function as a medium of exchange, store of value and unit of account.[72] However, there is a notable gap in the academic research that seeks to understand how the law can intervene through the existing case law, the MLR and the Proceeds of Crime Act 2002 ("POCA"), to enforce AML objectives in the crypto sector. Due to this legal uncertainty, the legal community must engage and understand the crypto sector since there is a noticeable gap in the academic disclosure in relation to crypto money laundering and the enforcement of AML rules. As a result, a focus on the crypto money laundering is *prima facie* justified since the unmanaged consequence will enable criminals to take advantage of this global technology. More importantly, crypto money laundering is not a "victimless crime". The individuals or the country from which the cryptoasset is stolen are, by definition, the victims, whilst the cryptoasset is used in the host country to support the criminal's lifestyle or other illicit activities such as drug importation, human trafficking, child sexual exploitation, prostitution, terrorism, tax evasion and fraud.

Methodology and theory

The purpose of this research is to provide a comprehensive theoretical framework that can be applied to the application of AML rules within the crypto sector. As a summary, this research finds that imposing traditional AML regulation and assuming that the crypto sector is an arm of law enforcement is counterproductive and could provoke the crypto community to develop protocols that are more autonomous, and as a result, harder to detect and enforce. This

[72] Sarah Green, "It's virtually money" in David Fox and Sarah Green (eds), Cryptocurrencies in Public and Private Law (Oxford University Press, 2019).

thesis will examine the new crypto laws through a distinctly doctrinal approach. However, this research will also examine the crypto sector and its consumers through online sources, such as specialist crypto websites, social media platforms and crypto blogs. Here, for example, Reddit,[73] Cointelegraph,[74] CoinDesk,[75] the Bitcoin Magazine,[76] and Vitalik Buterin's blog (Co-founder of Ethereum),[77] are all secondary sources used to understand the community, perceptions, and the future of cryptoassets. In addition to this, this research approaches crypto money laundering from more than one viewpoint: whilst Chapter 1 examines crypto money laundering from a general and technical perspective, Chapter 2 analyses it from the viewpoint of the UK regulator's legal response to cryptoassets. This research, therefore, commits to a view of crypto money laundering that is holistic and interdisciplinary. Thus, this research implements a classical school of thought found in the social sciences called the agency approach.[78] Within this school of thought there is a cohort of academic papers on money laundering, and more importantly, the agency dilemma in AML regulation, which has developed into a sperate school of thought drawing on insights from law, economics, sociology, business and management. The current research aspires to be part of this niche, and as a result, it is important to identify how the crypto phenomenon relates to the literature that has been produced within this school of thought.

In light of the above, this research explores the agency problem between crypto businesses and the FCA. As per the MLR, crypto firms must monitor transactions and reports suspicious transactions to the FCA, and as a result, undertake costly monitoring, compliance and reporting measures. To incentivise the crypto community, the FCA threatens to adopt a punitive approach, enforced through unlimited fines and bans, when a regulated business fails to report a suspicious transaction. However, scholars such as, Előd Takáts uncovered an underlying issue concerning this agency model. Here, Előd Takáts argues that harmful

[73] Reddit, "Reddit: Home" (Reddit, 2021) <https://www.reddit.com/> accessed 28 August 2021.

[74] Cointelegraph, "Cointelegraph: The future of money" (Cointelegraph. 2021) <https://cointelegraph.com/> accessed 28 August 2021.

[75] Coindesk, "Coindesk" (Coindesk 2021) <https://www.coindesk.com/> accessed 28 August 2021.

[76] Bitcoin Magazine, "The Bitcoin Magazine" (Bitcoin Magazine, 2021) <https://bitcoinmagazine.com/> accessed 28 August 2021.

[77] Vitalik Buterin, "Vitalik Buterin's website" (Vitalik Buterin, 2021) <https://vitalik.ca/> accessed 28 August 2021.

[78] The Agency theory will be explored in further detail in Chapter 3.

excessive reporting, dubbed as "crying wolf", can arise because of this agency set-up.[79] Thus, if, for instance, a crypto firm identifies all transactions as suspicious, then it fails to identify any one of them as suspicious. In order words, over-reporting can eliminate the information value of EDD reports. As a result, excessive reporting tends to arise in connection with excessively high fines which forces uncertain employees to excessively flag transactions on the side of caution, diluting the information value of EDD reports. Notwithstanding this assertion, AML regulation is nonetheless a key part of the reporting and compliance requirement for crypto firms within the UK. However, the administrative implications of AML compliance have been increasing, which is seen to be a burden on crypto businesses and its clients due to the time delays as well as an increase in transaction costs. This thesis aims to explore the role and influence of AML regulations through an agency perspective. The model will focus on the dual agency role that a crypto business must develop between supporting the needs of the client (Principal 1) and implementing FCA's AML mandate (Principal 2), whereby the firm must act as the agent. The conflicting structure of this dual agency relationship is important to understand when examining whether the current AML framework can, in fact, manage the risks associated with cryptoassets.

The current research does not adopt the 'law and finance' approach, since it attempts to quantify crypto laws,[80] through the collection of data currently available. Given the novelty of this research, no crypto laws existed at the start of this research, for the AML framework to be tested and assessed through a 'law and finance' approach. As a result, any effort to do a comparative law by implementing a numerical and statistical methods, such as an index, would be impossible. Nonetheless, implementing an established theory enables scholars to test common assertations as well as entrenched legal principles through the crypto lens. In an ideal world, the law is proactive, but in reality, the law is reactive as it is unlikely that the law will capture all iterations of this emerging technology. Here, an agency theory perspective will be employed in terms of methods, as a wide range of materials, as mentioned above, such as Reddit threads, crypto blogs, discussion papers as well as other community news, will be examined, which extends beyond the black-letter law. Thus, in addition to the doctrinal method, the agency

[79] Előd Takáts, "Laundering Enforcement" (2011) 27 Journal of Law Economics and Organisation 1, 34.

[80] Rafael La Porta, Florencio Lopez-de-Silanes, Andrei Shleifer and Robert Vishny, "Law and Finance" (1998) 106 Journal of Political Economy 6.

theory approach sets out to examine factors that incentivise AML compliance in order to test the legitimacy of the MLR within the crypto community. Studies suggest that behaviours are motivated by rewards and punishments, coupled with flexible governance mechanisms.[81] However, the need to adapt to new innovations and enforcing AML compliance remains the primary impetus for regulators.

This thesis investigates the law concerning the emergence of cryptoassets, and more specifically, how can the law incentivise the implementation of the MLR within the crypto sector. The overarching theme in this thesis sets out to examine the tension between technology-specific and technology-neutral laws employed to facilitate the implementation of the MLR within the UK and beyond. The difference between technology-specific and technology-neutral is that the law is drawn either narrowly to specific technologies, or broadly to general characteristics.[82] Thus, a technology-specific "…regime is described as technology specific to the extent that its scope of application is limited to a particular technological context".[83] In the absence of definitive judicial authority, crypto businesses could capitalise on regulatory gaps and employ low AML standards. To address this issue, regulators must understand the underlying technology and design laws to achieve interoperability between market participants in order to address "…harms associated with particular technological artefacts and practices".[84]

However, crypto developers, on the other hand, argue that technology-specific laws will threaten innovation. Following this assumption, crypto developers concern relates to the notion that 'any' potential liability may hinder technological developments. In short, regulation can kill technology. As a result, crypto rules must leave gaps in the law and remain 'tech neutral', whilst deliberately give discretion to industry leaders. Henceforth, the doctrine of tech-neutrality underlines the notion that the regulatory perimeter should be adjustable and is to be applied to assess whether changes should be made, either to tighten the regulatory net in some areas or in others to remove unnecessary restrictions to encourage innovation. Nonetheless, "*most commentators agree that the timing of regulatory responses to new technologies is*

[81] Tom Tyler, Why people obey the law (Yale University Press, 1990) 19.

[82] Brad Greenberg, 'Rethinking Technology Neutrality' (2016) 4 Minnesota Law Review 100, 1495.

[83] Roger Brownsword, Eloise Scotford and Karen Yeung, *The Oxford Handbook of Law, Regulation and Technology* (1st edn, Oxford University Press 2017).

[84] ibid.

generally poor, coming to too late".[85] As a result, the question in relation to the appropriate level of tech neutrality must be evaluated, by reference to known regulatory goals, through a doctrinal approach. Henceforth, the purpose of this thesis is to examine ways in which the FCA can facilitate this process and create incentives for AML compliance within the crypto sector.

Following the above, this section begins with a brief history of cryptoassets and the underlying technology. After setting the context, the subsequent chapters will underline the AML requirements for crypto businesses in the UK, then this chapter will expand on the illicit activities, and introduce the primary money laundering offences[86] as well as the enforcement procedures in the UK. Finally, to achieve the aims of the research question, this section is structured as follows:

I. **Section 2** outlines in more detail the underlying technology, who uses cryptoassets and what for, the trends and developments in support of ICOs and the potential path to mass adoption will be examined.
II. **Section 3** introduces the money laundering regime in the UK and how it relates cryptoassets and the implementation of the MLR.
III. **Section 4** sets out potential scenarios in which money launderers may use cryptoassets to launder illicit funds.

Cryptoassets and the underlying technology

Bitcoin and its derivatives known as "cryptoassets", was created as a medium of decentralised exchange using cryptography to facilitate transactions. At the present, society as a whole are at the beginning of a 'deep digital transformation', which will fundamentally change the way humans live, work and relate to one another.[87] It is submitted that cryptoassets are the symbol of the fourth industrial revolution – after steam, electricity, and computing.[88]

[85] Roger Brownsword, Eloise Scotford and Karen Yeung, *The Oxford Handbook of Law, Regulation and Technology* (1st edn, Oxford University Press 2017).

[86] Namely, the three primary offences: [1] the concealing offence: section 327, the POCA, [2] the arranging offence: section 328, the POCA, and [3] the acquisition, use and possession offence: section 329, the POCA.

[87] Klaus Schwab, *The Fourth Industrial Revolution* (1st edn, Penguin Random House 2017) 7.

[88] The World Economic Forum, 'The Fourth Industrial Revolution, by Klaus Schwab' (Word Economic Forum, 2019) <https://www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab> accessed 28 August 2021.

The development of cryptoassets is a relatively new concept - gathering momentum from 'proof of concept' to 'real-world' deployments. The story of cryptoassets began in 2008 when *Satoshi Nakamoto* created the first open-source payment system for cryptoassets (centred upon cryptographic proof),[89] which allowed any two parties to transact directly without the need for a trusted third party.[90] As a result, each transaction is verified and based on group consensus rather than through a single intermediary serving as the trusted third party.[91] Thus, unlike traditional assets, cryptoassets is derived from a decentralised system of ledgers known as the blockchain. This decentralised system can be used to record physical assets as well as intangibles assets such as cryptoassets.

Blockchain technology forms the underling infrastructure behind cryptoassets. The underlying technology is a secured ledger database accessible and shared by all participants in a designated network, which records and stores every transaction that occurs in the network, creating an irrevocable and auditable transaction history.[92] Here, the blockchain has a built-in redundancy and can survive the loss of one computer on the network, known as nodes, because the transaction is shared within a network of nodes, each with an identical copy of the transaction. At the present, banks and financial institutions are required to update their internal records every time a customer transfers an asset. By contrast, on a crypto network, transactions are sent to the nodes for validation, and once the nodes reach a consensus, the network validates the transaction.[93] This process of validation involves solving a complex mathematical equation, but once the transaction is verified, a record of the transaction is added to the blockchain. All users on the network receive an identical copy of the transaction. In essence, this verification

[89] The Economist, 'How to put Bitcoin into Perspective' (The Economist, 30 August 2018) <https://www.economist.com/technology-quarterly/2018/08/30/how-to-put-bitcoin-into-perspective> accessed 28 August 2021.

[90] Satoshi Nakamoto "Bitcoin: A Peer-to-Peer Electronic Cash System" (Bitcoin Blog, October 2008) <https://bitcoin.org/bitcoin.pdf> accessed 28 August 2021.

[91] The Economist, 'Telecommunications: The shape of Phones to come' (The Economist, 22 March 2001) <https://www.economist.com/taxonomy/term/23/0?page=15> accessed 28 August 2021.

[92] Sloane Brakeville and Bhargav Perepa, 'Blockchain basics: Introduction to distributed ledgers' (IBM Developers, 18 March 2018) < https://developer.ibm.com/tutorials/cl-blockchain-basics-intro-bluemix-trs/> accessed 28 August 2021.

[93] Antony Lewis, 'A Gentle Introduction to Bitcoin' (Bits on Blocks, 1 September 2015) <https://bitsonblocks.net/2015/09/01/gentle-introduction-bitcoin/> accessed 28 August 2021.

process requires a community consensus; and as a result, the likelihood of fraud is significantly reduced.[94]

In order to transfer the cryptoasset out of a crypto wallet, the owner must hold a unique private key. The cryptographic key is mathematically linked to the cryptoasset, and it is relatively anonymous when compared to traditional assets. However, it is essential to note that, cryptoassets are not entirely anonymous because all transactions are, in fact, transparent and recorded on the blockchain.[95] There are many ways to describe and crave up the crypto market. There is no agreed taxonomy within the crypto community and so terms like cyber-currencies, virtual currencies, digital assets, coins and tokens are used interchangeably to describe very different things. As a result, cryptoassets cover traditional cryptocurrencies, such as Bitcoin, as well as other cryptoassets, such as Diem (previously known as Libra).

The first generation of cryptoassets are digital assets that use cryptography to secure transactions, as well as to control, create and verify transfers. This first wave of cryptoassets was intended to be used as currencies (hence the name) although the consensus tends to be that they are not actually currencies.[96] The second wave of cryptoassets are tokens, which are digital assets associated with the phenomenon of ICOs. ICOs are a method of raising capital by issuing tokens for payment. The holder of the token has certain rights promised by the issuer of the token. These rights are granted in return for fiat currency or the transfer of other cryptoassets. There are many different types of tokens (e.g. payment tokens, utility tokens, security tokens). For instance, securities tokens may confer rights to dividends or voting rights (similar to traditional equities) or interest payments (similar to traditional bonds).

Bitcoin and its derivatives are categorised as non-regulated "cryptoassets", which are created as a medium of decentralised and/or centralised exchange using cryptography to facilitate transactions between two participants. Nonetheless, the second wave of cryptoassets

[94] Kevin Kelleher, 'The gold rush days of bitcoin mining are over, and not because of the price' (Ideas, 22 December 2014) <https://qz.com/316898/the-gold-rush-days-of-bitcoin-mining-are-over-and-not-because-of-the-price/> accessed 28 August 2021.

[95] Andy Greenberg, 'Prosecutors Trace $13.4M in Bitcoins from the Silk Road to Ulbricht's Laptop' (The Wired, 29 January 2015) <https://www.wired.com/2015/01/prosecutors-trace-13-4-million-bitcoins-silk-road-ulbrichts-laptop/> accessed 28 August 2021.

[96] David Fox, Cyber-Currencies in Private Law (1st edn, Oxford University Press 2018).

are viewed to be very similar to regulated assets, such as securities, bonds and derivatives. As a result, the challenge for the FCA is to understand the underlying technology and functionalities of each cryptoasset, where do they fit in the existing regulatory framework. This will be further explored and examined in Chapter 2.

In order for a crypto ecosystem to thrive, a cryptoasset must be created, stored, exchanged and processed. As a consequence:

I. **The miners must create the cryptoasset**. Similar to gold, cryptoassets must be mined by individual computers in order to process the transaction, the miners earn a cryptoasset as a reward. Here, mining is the act of recording the transaction on to the blockchain to unlock a reward. Unfortunately, this process is very resource-intensive, which requires substantial computing power to satisfy the security protocols embedded in cryptography, in order to ensure all nodes withing the network agree the transaction is accurate.[97] The original chain grows more complex as more list of transactions, known as blocks, are added to the chain, increasing the computing power required to sustain the network.[98]

II. **Digital wallet:** Effectively, the wallet stores cryptoassets and it can come in many forms, for instance, through digital online wallets (hot) accessible through an app or browser, and/or through offline hardware options known as cold storage. Examples of crypto wallets include: Coinbase,[99] BitPay,[100] Blockchain.com,[101] Electrum[102] and Exodus.[103]

[97] Peter Loshin and Michael Cobb, "Encryption" (TechTarget, 2021) <https://searchsecurity.techtarget.com/definition/encryption> accessed 28 August 2021.

[98] Anatol Antonovici, "Dogecoin Mining 2021: Everything you need to know" (Coindesk, 28 June 2021) <https://www.coindesk.com/dogecoin-mining-2021-everything-you-need-to-know> accessed 28 August 2021.

[99] Coinbase, "Wallet" (Coinbase, 2021) <https://wallet.coinbase.com/> accessed 28 August 2021.

[100] Bitpay, "Take control of your crypto" (Bitpay, 2021) <https://bitpay.com/wallet/> accessed 28 August 2021.

[101] Blockchain.com, "The world's most popular crypto wallet" (Blockchain.com, 2021) <https://www.blockchain.com/wallet> accessed 28 August 2021.

[102] Electrum, "Electrum Bitcoin Wallet" (Electrum, 2021) <https://electrum.org/#home> accessed 28 August 2021.

[103] Exodus, "Exodus Bitcoin & Crypto Wallet" (Exodus, 2021) <https://www.exodus.com/> accessed 28 August 2021.

III. **Crypto Exchanges**: A platform to trade cryptoassets for other cryptoassets or fiat currencies; thus, cryptoassets can be bought or sold on exchanges. Examples of Crypto Exchanges include: Coinbase,[104] Kraken,[105] Binance,[106] and Coinmama.[107]

IV. **Processors**: Crypto processors provide services and tools for merchants to accept cryptoassets as a form of payment. Examples of crypto processors include Braintree,[108] Shopify[109] and PayPal.[110]

First Generation: Cryptocurrenies

On a DLT, a cryptoasset is recorded on the digital ledger and, all proofs are sent to computers on the network, known as nodes, for validation before it is recorded on to the blockchain.[111] This process of validation involves solving a complex mathematical algorithm that verifies the chain of transactions operated by the users within the system, known as miners. The user's entitlement is proved ("the proof") if the holder has not already spent or transferred the cryptoasset. Effectively, this ensures the user is not double-spending or transferring assets which do not belong to the user. The miner who solves the mathematical algorithm and publishes the results on the network ('Proof of Work'), the system rewards the miner for their efforts with a token.[112] Thereafter, once the transaction is verified, a copy of the cryptoasset is added to the blockchain and all participant on the network receives an updated local record. Effectively, this verification process requires network consensus; and as a result, the likelihood

[104] Coinbase, "Get direct access to Coinbase Exchange" (Coinbase, 2021) <https://www.coinbase.com/exchange> accessed 28 August 2021.

[105] Kraken, "Buy Bitcoin and Crypto" (Kraken, 2021) <https://www.kraken.com/en-gb/> accessed 28 August 2021.

[106] Binance, "Buy and sell crypto in minutes" (Binance, 2021) <https://www.binance.com/en> accessed 28 August 2021.

[107] Coinmama, "The easiest way to buy and sell cryptocurrency" (Coinmama, 2021) <https://www.coinmama.com/?locale=en> accessed 3 August 2021.

[108] Braintree, "Braintree a PayPal Service: Boost Revenue with Global payments partner" (Braintree, 2021) <https://www.braintreepayments.com/gb> accessed 28 August 2021.

[109] Shopify, "Alternative Payments: Cryptocurrency" (Shopify, 2021) <https://help.shopify.com/en/manual/payments/alternative-payments/cryptocurrency> accessed 28 August 2021.

[110] PayPal, "Crypto for the people: Now you can discover crypto in the PayPal app" (PayPal, 2021) <https://www.paypal.com/us/webapps/mpp/crypto> accessed 28 August 2021.

[111] Supra (n 93) Lewis.

[112] Supra (n 90) Nakamoto.

of fraud is significantly reduced.[113] In order to transfer the asset out of the crypto address, the owner must possess a unique private key. The private key is a mathematical algorithm linked to the crypto-asset, and it is relatively anonymous when compared to the transferal of a traditional asset. A private cryptographic key is a 256-bit number, for instance: [114]

E9873D79C6D87DC0FB6A5778633389F4453213303DA61F20BD67FC233AA33262

The user activates each transaction by using their cryptographic key. This private key stays private, and it is not published to other users on the network. As each cryptoasset passes from user to user, the transactional history is recorded on the blockchain. As its name implies, the chain grows longer and longer, whilst the network is entirely anonymous in its operation. The private key is used as a pseudonym for the user's real identity. As a result, the real identity of the person who has control over the private key is not recorded on the blockchain. The history of transactions is therefore recorded on the blockchain but not the identity of the person behind it.[115]

Nonetheless, cryptoassets are not completely anonymous because all transactions are, in fact, transparent and recorded on the blockchain.[116] Cryptoassets are held in a variety of different forms, from cold storage to digital wallets and smart repository. On the one hand, cold storage is the simplest and safest way to store private keys, i.e. printing out the 256-bit codes and crypto addresses and store it in a physical vault.[117] It is nonetheless, vulnerable to fire and theft. On the other hand, users can download a digital wallet directly held on the user's hard drive. Alternatively, the user can use online wallets apps or digital vault services. For instance, Infinitus is a blockchain based DApp which allows users to store encrypted digital data on a decentralised network.[118] Infinitus app is designed for longer-term storage of cryptoassets. The

[113] Supra (n 94) Kelleher.

[114] Bitcoin Wiki, 'Private Key' (Bitcoin, 1 March 2019) <https://en.bitcoin.it/wiki/Private_key> accessed 28 August 2021.

[115] Supra (n 90) Nakamoto.

[116] Supra (n 94) Kelleher.

[117] CryptoNews, 'How to store cryptocurrencies safely in 2020' (CryptoNews, 2020) <https://cryptonews.com/guides/how-to-store-cryptocurrency-safely.htm> accessed 28 August 2021.

[118] Infinitus, 'About' (Infinitus, May 2019) <https://inftech.io/> accessed 28 August 2021.

assets are remotely held from the user's own software, but they can access the wallet to issue instructions.[119] However, the online environment is vulnerable to hacking.[120]

Second Generation: Cryptoassets

ICOs has been described as "donation events", "software pre-sales", "token sales" or "network token sales", possibly to avoid comparisons with Initial Public Offerings (IPO).[121] Nevertheless, ICOs have been increasing in popularity, with more than $3.3billion funnelled through ICOs in 2017, as compared with $70m in the same period in 2016.[122] This surge is one reason for the boom in bitcoin, up more than 750% during the period of 2017-2018.[123] In a typical ICO, if the issuer has developed a cryptoasset, the token issued would be a unit of that cryptoasset.[124] In most cases, the token will not carry any rights or entitlements (for instance, Bitcoin or Ether). In contrast, a token may represent value to be spent on the issuer's product or platform. For instance, 'Storjcoins' can be used to purchase cloud storage on Storj.io.[125] Thus, users who purchased tokens[126] will be able to spend those tokens on their service.[127] In other cases, a secondary market has developed, and tokens are tradeable on Exchanges, such as Poloniex[128] and Kraken.[129] The value of the token may rise if the company is successful, thus

[119] Infinitus Tech, 'What You Need to Know About Infinitus' (Infinitus, 21 August 2018) <https://medium.com/infinitustoken/what-you-need-to-know-about-infinitus-b026190af597> accessed 28 August 2021.

[120] CoinSutra, 'What is cold storge in cryptocurrency' (CoinSutra, 12 August 2019) <https://coinsutra.com/cold-storage-cryptocurrency/> accessed 28 August 2021.

[121] John Biggs, 'How to run a Token sale' (*Tech Crunch*, 22 September 2017) <https://techcrunch.com/2017/09/22/how-to-run-a-token-sale/> accessed 28 August 2021.

[122] The Economist, 'Token Resistance: Regulators begin to tackle the craze for initial coin offering' (*Economist*, 11 November 2017) <https://www.economist.com/news/finance-and-economics/21731157-they-raise-difficult-legal-questions-regulators-begin-tackle-craze> accessed 28 August 2021.

[123] Nasdaq, 'Gold – Latest Price & Chart for CBOT Gold' (*Nasdaq*, 22 November 2011) <http://www.nasdaq.com/markets/gold.aspx> accessed 28 August 2021.

[124] Ethereum, 'Create your own Crypto-Currency with Ethereum' (*Ethereum*, 2017) <https://www.ethereum.org/token> accessed 28 August 2021.

[125] Storj, 'Storj Tocken Update' (Storj, 2017) < https://storj.io/tokensale.html> accessed 28 August 2021.

[126] Bitcoin Exchange Guide, 'Initial Coin Offering – Alternative ICO Cryptocurrency Token Guide' (Bitcoin Exchange Guide, 2017) < https://bitcoinexchangeguide.com/initial-coin-offering/> accessed 28 August 2021.

[127]Coinmarketcap, 'Storjcoin X' (Cryptocurrency Market Capitalizations, 21 November 2017) <https://coinmarketcap.com/currencies/storjcoin-x/#charts> accessed 28 August 2021.

[128] Polobiex, 'Welcome to Poloniex – Trade securely on the world's most active digital asset exchange' (Polobiex, 2017) <https://poloniex.com/> accessed 28 August 2021.

[129] Kraken, 'About' (Kraken, 2017) < https://www.kraken.com/en-gb/about> accessed 28 August 2021.

similar to speculative investments.[130] As a result, start-ups are considering ICOs as a means to target a small community of early adopters, rather than investors from the general public. It is reasoned that by requiring payment in a cryptoasset, the investor-base is arguably limited to early adopters who are familiar with this type of technology.

Tokens can be distributed like that of an IPO of shares. However, there are notable differences between ICOs and IPOs. On the one hand, a formalised legal and regulatory framework governs the IPO process. Thus, shares issued in IPOs are subject to financial market regulations. On the other hand, the legal status of crypto tokens remains unclear. Overall, ICOs are more susceptible to fraud than IPOs due to weak regulatory oversight and AML compliance.[131] In addition, ICOs tend to occur at the beginning of a company's business cycle, whilst IPOs tend to happen when the company becomes more mature.[132] Notable ICO governance shortcomings: [1] lack of managerial transparency; [2] no voting rights; [3] no binding contractual commitments; and [4] no reporting or audit mechanisms. This means ICOs are inherently riskier than IPOs, particularly in circumstances where tokens are found to be securities, and as a result, a speculative market may develop based on fraudulent claims.[133]

In short, for all the innovativeness that cryptoassets can offer, a clear and concise governance structure is conducive to the long-term success of a crypto firm. More importantly, the digital world would benefit from best practices and structures that align the programmers as well as the token holder's incentives. Nevertheless, it is difficult to generalise cryptoassets, since some tokens are sold as crypto equity which makes them akin to securities, whereas other tokens simply represent the value to be spent on the issuer's platform more akin to Kickstarter campaigns. Thus, it is difficult to make a sweeping statement on the legality of ICOs. Therefore, a sound legal framework in the UK and in particular, legal clarity on the nature of claims against

[130] Laura Shin, 'How to Speculate in ICOs: 10 Practical Financial Tips' *Forbes Magazine* (London 17 July 2017) <https://www.forbes.com/sites/laurashin/2017/07/17/how-to-speculate-in-icos-10-practical-financial-tips/#55a5b12c5378> accessed 28 August 2021.

[131] Economist Jobs, 'The future of Initial Coin Offerings' (*Economist Jobs*, 4 October 2017) <https://economistjobs.com/future-initial-coin-offerings/> accessed 28 August 2021.

[132] ibid.

[133] Olga Kharif, 'One of the most High-Profile Initial Coin Offerings had crashed 50%' *Bloomberg Markets* (London, 1 November 2017) < https://www.bloomberg.com/news/articles/2017-11-01/shining-star-of-initial-coin-offerings-crashing-back-to-earth> accessed 28 August 2021.

an issuer and the token holder, is a prerequisite in which this research seeks to uncover. Following this assumption, this research aims examine whether a cryptoasset can be used and recognised on a global scale? In this vein, this section will consider the following questions: [1] is the world ready for private money? Furthermore, [2] is the underlying technology ready for global implementation?

The crypto market lost 85% in value from its 2018 peak;[134] and mainstream institutional acceptance remains challenged, with small tech start-ups as well as retail investors as the most logical near-term adopters. **[1]** Accordingly, a common critique of cryptoassets is that central banks and regulators are protective of their right to control the issuance of currency, interest rates, and in general, the supply of money. Traditionally, money is defined as 'public money' which consists of central bank liabilities in relation to the local currency in circulation (paper and coins) as well as bank reserves. The former is primarily for consumers and companies making everyday payments in person, whilst the latter forms the foundation of the overall payment system on which the economy operates. At the present, corporations rarely use cash and consumers only rely on it for a small and declining fraction of their payments.[135]

In reality, the world is flooded in 'private money', which accounts for more than three-quarters of the total economy.[136] The term 'private money' is defined as commercial bank deposits, which are liabilities of private companies but are nonetheless universally accepted as a store of value and a medium of exchange. As a result, most non-cash payment transactions are essentially a transformation of these private liabilities, i.e. a novation of the creditor and/or obligor. Thereafter, payment transactions are generally batched and netted throughout the day; and as a result, there is very little exchange of public money.[137] Private money derives its value from the fact that, it is functionally exchangeable on demand for public money at par.[138] In

[134] Nick Chong, 'Crypto Industry Execs: This Bitcoin Bear Market is The Best Yet' (News BTC, 26 March 2019) <https://www.newsbtc.com/2019/03/26/crypto-industry-execs-this-bitcoin-bear-market-is-the-best-yet/> accessed 28 August 2021.

[135] Kevin Peachey, 'Pay by cash? Not for long, report warns' (BBC News, 6 March 2019) <https://www.bbc.co.uk/news/business-47456698> accessed 28 August 2021.

[136] JP Morgan, 'Can stablecoin achieve global scale?' (JP Morgan Markets, 3 December 2019).

[137] ibid.

[138] Bank for International Settlements, 'The role of central bank money in payment systems' (BIS, August 2003) <https://www.bis.org/cpmi/publ/d55.pdf> accessed 28 August 2021.

practice, these exchanges, i.e. converting private to public monies, are small relative to the aggregate payment volumes for the reasons mentioned previously. In other words, private money is a form of leverage in the payment system and is thus a money multiplier.[139]

Commercial banks are entrusted to serve this critical function, i.e. converting private for public money. In exchange, commercial banks must maintain their credit worthiness and regulatory compliance measures, such as insurance for deposits. In other words, regulators control commercial banks through a combination of compliance obligations and statutory reserve requirements, which limits the overall size of the banking system.[140] Effectively, commercial banks are subjecting themselves to the above web of regulations as a means to obtain government and central bank backing. As a result, the privilege of acting as the issuer of 'private' money generally comes with obligations to safeguard the financial system from market abuse, fraud, and AML concerns. This is not a small ask; for instance, each year, European banks spent approximately $20 billion on AML compliance.[141] Whist North American firms annually spend more than $31.5 billion on AML compliance.[142] Therefore, ***applying similar regulation to cryptoasset issuers, particularly those designed to facilitate cross-border transactions, such as Facebook's Diem (a stablecoin), remains a key area of focus for international regulators***.[143]

An issuer of a stablecoin can, in principle, act as a **de facto** bank. Henceforth, applying similar banking and compliance measures, a cryptoasset can be designed to facilitate cross-border transactions by implementing AML/CTF/KYC protections that are up to international standards.[144] In that sense, this would likely require some limits on anonymity and the openness of blockchain network.[145] Here, the value of an issuer's liabilities, i.e. the stablecoins, must be

[139] ibid.

[140] ibid.

[141] Supra (n 19) Kuskowski.

[142] Supra (n 20) LexisNexis.

[143] Bank for International Settlements, 'Investigating the impact of global stablecoins' (BIS Committee on Payments, October 2019) <https://www.gouvernement.fr/sites/default/files/locale/piece-jointe/2019/10/1489_-_g7sc_report_on_global_stablecoins_-17_october_2019_final.pdf> accessed 28 August 2021.

[144] David Voreacos, 'Cryptocurrencies U.S., South Korea Bust Giant Child Porn Site by Following a Bitcoin Trail' (Bloomberg News, 19 October 2019) <https://www.bloomberg.com/news/articles/2019-10-16/giant-child-porn-site-is-busted-as-u-s-follows-bitcoin-trail> accessed 28 August 2021.

[145] ibid.

fully backed by a pool of high-quality collateral.[146] It is submitted that, an issuer of stablecoins perform similar functions as a commercial bank, i.e. provide liquidity to its customers, through the settlement of payments. Accordingly, it would not be surprising for a crypto issuer who reaches a certain scale to be subject to some form of international securities and banking requirements. In short, the world is ready for cryptoassets, since fiat money is already privately issued; however, for cryptoassets to be accepted as payment, the issuer must adhere to the same regulatory requirements as financial institutions.

[2] Finally, the second most cited constraint on the potential growth of cryptoassets revolves around the efficiency of the underlying technology; namely, whether the blockchain is ready for global scale and implementation. In practice, the computing power required to validate a crypto transaction varies significantly. This is proliferated through the process of 'mining', in which each 'proof-of-work' generates a complex mathematical problem that is unique for each transaction (thus the speed/the process of mining as well as the computing power required to validate crypto-transactions spans a vast range). This verification process is key to the integrity of the ledger, which acts as the check and balance to confirm the authenticity of each transaction. Nonetheless, this is quite energy-expensive, especially when the difficulty of these math problems increases over time via proof-of-work, as a means to limit the supply of new coins.

Researchers have produced estimates on the power required to process a crypto transaction via the two largest cryptoassets: Bitcoin and Ethereum.[147] It was concluded that, although Ethereum is faster and more efficient, both used more energy than the conventional, centralised, account-based payment systems, such as traditional bank transfers or credit card transactions.[148] In order words, although Ethereum is 20x less demanding than Bitcoin, it is still more power-hungry than the VISA network, which can process more than 1,200 transactions

[146] Ben Regnard-Weinrabe, Heenal Vasu and Hazem Danny Ai Nakib, 'Stablecoins' (7th edn, Hart Publishing 2019) 487.

[147] Christopher Malmo, 'One Bitcoin Transaction Consumes As Much Energy As Your House Uses in a Week' (Vice News, 1 November 2017) <https://www.vice.com/en_us/article/ywbbpm/bitcoin-mining-electricity-consumption-ethereum-energy-climate-change> accessed 28 August 2021.

[148] Shanhong Liu, 'Average energy consumption per transaction for Bitcoin and VISA 2018' (Statista, 2018) <https://www.statista.com/statistics/881541/bitcoin-energy-consumption-transaction-comparison-visa/> accessed 28 August 2021.

for each Ethereum transaction.[149] At this point, the Ethereum 1.0 network uses the same magnitude of power as the country of Bolivia, but it is not nearly as active in terms of transactions per capita. Thus, Bitcoin, as well as Ethereum-like energy consumption, is therefore completely infeasible.[150] In this sense, the fundamental design decisions regarding the protocol that drives a given cryptoasset is a key consideration in its potential to achieve global scale. For instance, one approach is to rely on a semi-private network with a small group of trusted nodes to validate transactions via 'proof-of-stake'. However, a truly open distributed ledgers, such as Bitcoin and Ethereum, are more resilient and transparent, but both platforms are also more computationally intensive than private and/or semi-private networks.[151]

In this sense, private as well as semi-private blockchain networks are more efficient, but there are some operational and cybersecurity risks associated with a centralised system validated by a few trusted nodes. At this point, this research cannot say for certain whether a cryptoasset can or cannot achieve global scale (as technology is ever evolving), but the required improvements on blockchain 2.0 may require a somewhat centralised network. Nonetheless, the energy requirement remains a significant limitation for the crypto sector.

The legal framework

The crypto space is, by its nature, volatile and incapable of discriminating between criminals and early adopters. For instance, the MIT Technology Review examined 1,450 ICOs and its white papers and found that more than 19% raised serious doubts about their authenticity.[152] In the UK, exchange related scams had more than tripled from 2018 to 2019,

[149] Sean Williams, 'Which Cryptocurrencies have the fastest transaction speeds?' (The Motley Fool, 14 January 2018) <https://www.fool.com/investing/2018/01/14/which-cryptocurrencies-have-the-fastest-transactio.aspx> accessed 28 August 2021.

[150] Colin Schwarz, 'Ethereum 2.0: A Complete Guide' (Medium, 4 July 2019) <https://medium.com/chainsafe-systems/ethereum-2-0-a-complete-guide-d46d8ac914ce> accessed 28 August 2021.

[151] The Economist, 'Why bitcoin uses so much energy' (The Economist, 9 July 2018) <https://www.economist.com/the-economist-explains/2018/07/09/why-bitcoin-uses-so-much-energy> accessed 28 August 2021.

[152] Mike Orcutt, 'Surprise! Hundreds of ICOs are probably scams' (MIT Technology Review, 18 May 2018) <https://www.technologyreview.com/f/611170/surprise-hundreds-of-icos-are-probably-scams/> accessed 28 August 2021.

with more than GBP 27 million reported lost.[153] As a result, the FCA is considering a potential ban on the sale, marketing and distribution of cryptoassets to retail customers (unlikely).[154] Market abuse and financial crimes are prevalent in the crypto space, the issues are twofold: First, because cryptoassets are novel and in many ways, unlike other traditional financial products, i.e. bonds, shares and derivatives. As a result, regulators face interpretative obstacles in determining whether a new cryptoasset falls within its existing legal framework. Second, in light of the cross-border nature of cryptoassets, each governing body needs to manage possible jurisdictional overlaps with other regulators. As a result, the treatment of cryptoassets will depend on the approach as agreed by international regulators.

Notwithstanding the above, progress has been made to move cryptoassets beyond the experimentation stage to vast adoption in the realms of payments, custodial arrangements, derivative agreements, international settlements, asset tokenisation, and ICOs. However, the real developments have largely been confined to decentralised applications ("DApps") and smart contracts. Therefore, barriers for mainstream "crypto" adoption remains significant.[155] A cryptoasset is the representation of a value in relation to a specific address referenced in the blockchain (or distributed ledger technology – "DLT"). However, determining the characteristics and consequent categorisation of a cryptoasset is not straightforward. Cryptoassets can, in principle, fall into two categories, those that [1] do not represent any real-world asset and [2] those that represent a real-world asset. In reality, the world of cryptoassets is fluid with hundreds of new innovations every week, with new tokens combining different features of crypto and blockchain technology. For instance, a cryptoasset may change in nature and functionality during their existence.

However, it is broadly accepted, for example, by the UK Jurisdictional Taskforce, the US Securities and Exchange Commission ("SEC"), the European Securities Markets Authority

[153] Financial Conduct Authority, 'Over £27 million reported lost to crypto and forex investment scams' (FCA, 21 May 2019) <https://www.fca.org.uk/news/press-releases/over-27-million-reported-lost-crypto-and-forex-investment-scams> accessed 28 August 2021.

[154] FCA, 'Prohibiting the sale to retail clients of investment products that reference cryptoassets' (FCA Consultation Paper CP19/22, July 2019) < https://www.fca.org.uk/publication/consultation/cp19-22.pdf> accessed 28 August 2021.

[155] International Finance Corporation, *Blockchain opportunities for private enterprises in emerging markets* (Work Bank Group, January 2019).

("ESMA") and the European Banking Authority ("EBA") (albeit with minor variations in labelling) that there are three main categories of cryptoassets:

I. **Security token**: These tokens confer rights such as ownership or entitlement to a share in future profits of a company or network, such as contractual entitlement to profit share through dividends or ownership. As a result, these tokens will most likely meet the criteria of a 'specified investment' under the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001(SI 2001/544) ("ROA") and should be treated as traditional investments.

II. **Utility token**: These tokens may be redeemed for access to a specific network, product or service. They will likely be outside the regulatory perimeter unless the tokens meet the criteria of 'e-money', as per the UK Electronic Money regulation 2011 (SI 20 2011/99) ("EMRs").

III. **Exchange token**: These tokens are used as a decentralised tool for the buying and selling of goods and services without traditional intermediaries. Here, these tokens will most likely be outside the regulatory perimeter; unless the token are structured in such a way to fall within the jurisdiction of 'e-money' under EMRs.

Accordingly, tokens may also have mixed features that may overlap with the above or change over time. For example, Ether can be used as a means of payment on the platform ("exchange token") then used to run DApps on the Ethereum blockchain ("utility token").

At the present, the FCA implements a case-by-case analysis of each new cryptoasset, and when determining if a particular cryptoasset is regulated or unregulated. Here, the FCA will consider the following questions:

I. Will the cryptoasset be transferable securities or is similar to other types of regulated financial instruments or investments?

II. Might the underlying structure involve the creation of a collective investment scheme?

III. Will the cryptoasset give rise to the issuance of electronic money or the provision of payment services?

IV. Might the cryptoasset be regarded as crowdfunding?

However, there is a clear indication that the FCA will use its high-level powers to, if appropriate, police actions taken by firms in relation to both regulated as well as unregulated

crypto-related activities.[156] For instance, the FCA is considering a ban on the sale, market and distribution of investment products that reference cryptoassets to all retail investors.[157] FCA estimates that a ban could reduce harm by GBP 75 million to GBP 234.3 million a year for retail investors.[158]

In 2018, the FCA divided cryptoassets into three categories: [1] security token; [2] exchange tokens; and [3] utility tokens. However, following the final FCA report published in July 2019, the token categories are as follows:

I. **Securities token (regulated):** largely unchanged from the draft guidance, this covers tokens which qualify as investments like shares, bonds or units in a fund;[159]
II. **E-money tokens (regulated):** cryptoassets that meet the definition of e-money are regulated;[160] and
III. **Unregulated tokens:** any cryptoasset that is not a security, or an e-money token is unregulated e.g. exchange tokens (aka crypoasset) like Bitcoin and Litecoin or utility tokens which allow access to a service or network.

In addition, the buying and selling unregulated tokens do not require FCA authorisation. However, dealing in crypto derivatives is a regulated activity (even if the underlying cryptoassets are unregulated). Financial crime and AML concerns are one of the FCA's cross-sector regulatory priorities; and as such, the regulatory reach in this area will only be increasing. The FCA has been granted further powers following the enactment of the 5AMLD and will, as of March 2020, be monitoring the AML supervision carried out by crypto firms, such as exchange providers and custodian wallet providers.[161]

---

[156] Financial Conduct Authority, *Guidance on Cryptoassets* (FCA Consultation Paper 19/3, 2019).

[157] Financial Conduct Authority, *Prohibiting the sale to retail clients of investment products that reference cryptoassets* (FCA CP19/22, July 2019).

[158] Financial Conduct Authority, 'CP19/22: Restricting the sale to retail clients of investment products that reference cryptoassets' (FCA, 3 July 2019) <https://www.fca.org.uk/publications/consultation-papers/cp19-22-restricting-sale-retail-clients-investment-products-reference-cryptoassets> accessed 28 August 2021.

[159] Linklaters LLP, 'FCA provides further clarity on UK cryptoasset regulation in new draft guidance' (Linklaters LLP, 25 January 2019) <https://www.linklaters.com/en/insights/blogs/fintechlinks/2019/fca-provides-further-clarity-on-uk-cryptoasset-regulation-in-new-draft-guidance> accessed 28 August 2021.

[160] Electronic Money Regulation 2011.

[161] Financial Conduct Authority, 'Cryptoassets: AML/CTF regime' (FCA, 25 October 2019) <https://www.fca.org.uk/firms/financial-crime/cryptoassets-aml-ctf-regime> accessed 28 August 2021.

From March 2022, crypto businesses must register with the FCA, as per the Fees (Cryptoasset Business) Instrument 2020.[162] The fees are:

I. GBP 2,000 for businesses with revenue up to and including GBP 250,000; or

II. GBP 10,000 for businesses with revenue of over GBP 250,000.[163]

The above is the result of 5AMLD[164] which imposed new AML requirements on e-money businesses (i.e. *a firm will be an electronic money issuer when it opens an 'electronic payment account and/or wallet for a customer*)[165] carrying out crypto-related activities and transactions, through crypto-exchanges, and/or platforms supporting the transfer or custody of crypto.[166]

In support of the above, the FATF published an updated version of its international standards in relation to AML/CTF compliance,[167] coupled with its guidance for virtual assets and virtual asset service providers.[168] The FATF recommends a risk-based approach[169] and advises countries to:

[162] The FCA made the instrument under regulation 102 of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulation, as amended by the Money Laundering and Terrorist Financing (Amendment) Regulations 2019.

[163] Fees (Cryptoasset Business) Instrument 2020, App 3.1.4.

[164] HM Treasury, 'Transposition of the Fifth Money Laundering Directive: Consultation' (Her Majesty's Treasury, April 2019) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/795670/20190415_Consultation_on_the_Transposition_of_5MLD__web.pdf> accessed 28 August 2021.

[165] Paysera LT (UAB "EVP International" v Lieuvos bankas (Case C-389/17): The ECJ ruled that Article 5(2) must be interpreted as meaning that services provided by e-money institutions in payment transactions in payment transactions constitute activities linked to the issuance of e-money, within the meaning of that provision, if those services trigger the issuance or redemption of e-money in a single payment transaction.

[166] Clifford Chance, 'HM Treasury considers gold-plating 5MLD requirements for cryptos' (Clifford Chance, 8 May 2019) <https://www.cliffordchance.com/hubs/regulatory-investigations-financial-crime-insights/our-insights/hm-treasury-considers-gold-plating-5mld-requirements-for-cryptos.html> accessed 28 August 2021.

[167] Financial Action Task Force, 'International standards on combating money laundering and the financing of terrorism and proliferation: FATF Recommendations (FATF, June 2019) <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html> accessed 28 August 2021.

[168] Financial Action Task Force, Guidance for a risk-based approach: virtual assets and virtual asset service providers' (FATF, June 2019) <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html> accessed 28 August 2021.

[169] A risk-based approach means countries should have an understanding of the FATF recommendations in relation to AML/CTF/KYC and focus their resources and attention on areas where the risks are deemed higher and ensure the mitigation of those risks.

I. Identify, assess and understand domestic AML risks in relation to crypto activities and the activities or operations of virtual activity service providers ("VASP").[170]

II. Instruct VASPs to identify, assess and understand its AML obligations to mitigate their money laundering and terrorist financing risks.[171]

Require VASPs to be licensed or registered to prevent criminals from controlling, behind beneficial owners of, or holding directorial and/or managerial positions in a VASP.[172] Therefore in addition to ensure that VASPs adheres to AML regulations which must be monitored by a competent authority via risk-based supervision. The competent authority must have adequate powers to supervise and impose a wide range of disciplinary and financial sanctions that are proportionate. Moreover, sanctions should be applied not just to the VASPs, but also to their directors and managers.[173] The UK, must engage with its international counterparts in order to deliver the FCA's AML mandate, in part due to the global reach of this underlying technology.[174]

Money laundering risks are seen as the key impediment to the development of the crypto sector. As a result, regulators must decide whether cryptoassets should be isolated, regulated or integrated in relation to the existing AML frameworks. Different international regulators classify and treat cryptoassets differently. Some regulators classify cryptoassets as a unit of account whilst others reject it as an emerging technology. Other regulators take the view that a case-by-case assessment is necessary. The UK has adopted a proportionate and case-by-case approach. The UK has not ignored cryptoassets, nor have they attempted to ban them. At the present, cryptoassets are treated like any other financial instruments, and proportionally to a cryptoassets market importance, complexity, and associated risks. Given their global, trans-border character, the UK aims to encourage international consistency and harmonisation in crypto regulations through international organisations, such as the 'Global Financial Innovation Network' ("GFIN").[175] The GFIN is a network of 38 international governmental organisation

[170] ibid.

[171] ibid.

[172] ibid.

[173] ibid.

[174] ibid.

[175] Financial Conduct Authority, 'Global Financial Innovation Network (GFIN)' (Financial Conduct Authority, 31 January 2019) <https://www.fca.org.uk/firms/global-financial-innovation-network> accessed 28 August 2021.

committed to support financial innovation and to facilitate a new practical method of regulatory collaboration on cross-border regulatory testing.[176]

However, the European Parliament acknowledged that the existing European legal framework fails to deal with the pseudonymity of cryptoassets.[177] Nonetheless, the latest version of the European AML rules will include to virtual currency exchange services and custodian wallet providers; thus as of March 2022, crypto firms will need to perform customer due diligence and report suspicious transactions to the financial intelligence unit. However, critics have flagged that some key players within the industry, such as miners, pure cryptoasset exchanges, non-custodial wallet providers, trading platforms and coin offerors, are not captured by the AMLD5.[178] Thus, the European Parliament are considering: [1] mandatory KYC registration of crypto clients; [2] implementing the Funds Transfer Regulation rule to crypto transactions; and [3] a ban on aspects of crypto technology designed to make users untraceable.[179] The European Parliament notes that the fight against money laundering should focus on the illicit use of cryptoassets rather than the underlying technology, thus adhering to the principle of tech neutrality.[180] This means "*regulation should not have a negative effect on the development of technology and should not unduly discriminate between technologies*".[181]

As per AMLD5, the FCA must be monitor the internal AML systems and controls carried out by crypto firms. It will do so through its Office for Professional Body Anti-Money Laundering Supervision. In line with its mission, the FCA aims to ensure that crypto businesses have effective systems and controls to minimise the risk of crypto money laundering. Herein,

---

[176] The Global Financial Innovation Network, 'GFiN – One year on – Report 2019' (GFiN, January 2019) <http://dfsa.ae/Documents/Fintech/GFIN-One-year-on-FINAL-20190612.pdf> accessed 28 August 2021.

[177] Robby Houben and Alexander Snyers, 'Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion (European Parliament Special Committee on Financial Crime and Tax Avoidance, July 2018) <http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf> accessed 28 August 2021.

[178] ibid.

[179] The UK Government, 'Information you must send with a transfer of funds to prevent money laundering' (GOV.UK, 25 February 2014) <https://www.gov.uk/guidance/how-to-comply-with-eu-payments-regulation#the-eu-funds-transfer-regulation> accessed 28 August 2021.

[180] ibid.

[181] Chris Hoofnagle, 'Should regulation be 'Technology Neutral' (Berkeley.edu, 2 February 2018) <https://hoofnagle.berkeley.edu/2018/02/02/should-regulation-be-technology-neutral/> accessed 28 August 2021.

reinforces the application of the 'risk-based' approach which aims to strike the right balance between proportionality and efficiency. For instances, crypto firms must maintain adequate safeguards against AML, but also minimise the untended consequence of AML compliance such as excessive delay in providing its services and opening account for low-risk clients. Although this sounds straightforward in the abstract, striking the right balance in practice and meeting the FCA's expectations is often more complicated. The FCA expects crypto businesses to take a curious approach to the origins of a client's finances, whilst being vigilant throughout a client's lifecycle. In other words, the onus is on the business to design as well as review their operational effectiveness on the company's AML systems and controls.

As a general introduction, there are three primary money laundering offences, which are set out in Part 7 of the POCA (this will be further examined in Chapter 4). It is an offence to:

I. Conceal, disguise, convert or transfer the proceed of crime, and/or to remove the proceeds of crime from the UK.[182] This is the basic money laundering offence.
II. Enter into, or become a party in an arrangement, in which the person knows or suspects the retention, use or control of criminal property.[183] This is known as the aiding and abetting offence.
III. Acquire, use or possess the proceeds of crime.[184] This is known as the handing of stolen goods offence.

All money laundering offences require either *knowledge* or *suspicion* of money laundering. To prove knowledge, the FCA has to prove a suspect knew that the relevant property derived from the proceeds of crime. Suspicion, on the other hand, does not have to be clear, or firmly grounded in relation to the specific facts, but must be more than mere 'fanciful'. Following *R v Da Silva*, suspicion meant that "*the defendant thinks there is a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice"*.[185] In order words, if a crypto employee suspects that money laundering is occurring and fails to report it, the business as well as the employee maybe guilty of an offence under POCA. Knowledge or suspicion catches both the criminals as well as those facilitating and/or benefiting from the

[182] POCA 2002, s327.
[183] POCA 2002, s328.
[184] POCA 2002, s329.
[185] R v Da Silva [2006] EWCA Crim 1654.

proceeds of crime. Given the severity of these offences, banks, as well as e-money services, are contractually entitled to close customer accounts without notice in light of knowledge and suspicion of money laundering.[186]

Subsequently, the Criminal Finances Act 2017 introduced a number of new measures to tackle money laundering and other financial crime. In addition to introducing the new corporate criminal offences for failure to prevent the facilitation of tax evasion, the Act introduces new investigative and information sharing tools to enable law enforcement to combat money laundering. For instance:

I. **Unexplained Wealth Orders**: [187] a person or company involved in or associated with serious financial crime to explain the origins of their assets which appear to be disproportionate to their known income;[188]
II. **Regulatory tools/powers**: freezing orders[189] and/or seizure of assets;[190] and
III. **Suspicious Activity Reports AML reforms**:[191] longer moratorium period by up to six months for the FCA and NCA to investigate any suspicious activity, which will have practical implications for any crypto business.

Money laundering has long been a regulatory focus because it is at the heart of a number of criminal activities. It is commonly accepted that crypto money laundering is a critical enabler of serious and organised crime, corporate corruption as well as terrorism. Money laundering activities transacted through the financial markets and laundered within the mainstream economy erodes market integrity and presents risks to the soundness and stability of the global financial system.

As a result the FCA instructs banks to implement a 'reasonable and proportionate measures' to reduce the risk of financial crime and money laundering by crypto clients.[192] The

[186] N v The Royal Bank of Scotland Plc [2019] EWHC 1770 (Comm).

[187] POCA 2002, Part 8 s362A-362R and s396A-396U; Criminal Finances Act 2017.

[188] National Crime Agency v Zamira Hajiyeva [2018] EWHC 2534.

[189] POCA 2002, Part 8 s362D-R.

[190] POCA 2002, Part 5 s289, s294

[191] The Criminal Finances Act 2017

[192] Financial Conduct Authority, 'Dear CEO: Cryptoassets and Financial Crime' (FCA, June 2018). <https://www.fca.org.uk/publication/correspondence/dear-ceo-letter-cryptoassets-financial-crime.pdf> accessed 28 August 2021.

FCA underlined the risk associated with crypto money laundering arising from businesses that provide services to crypto-businesses and clients whose source of wealth is derived from cryptoassets trading and/or ICOs. In this vein, when pseudonymity is built into the structure of some cryptoassets, such as Bitcoin and Ethers, crypto firms must assess the risks posed by clients whose wealth is derived from cryptoassets or other cryptoasset-related activities, using the ***same*** AML criteria that would be applied to traditional assets. Thus, if a crypto firms transactions has a weak evidence trail, this does ***not*** justify applying a different evidential test on a client's source of wealth.[193]

In addition, the AMLD5 will trigger amendments to the JMLSG AML Guidance, for instance Part I paragraphs 5.3.17 and 5.3.67. MLR (6)-(7): "*Firms carrying on business in the UK must not set up an anonymous accoun**t**, an anonymous passbook, or an anonymous safe-deposit box for any new or existing customer. All firms carrying on business in the UK must apply CDD measures to all existing anonymous accounts, passbooks and safe-deposit boxes before such accounts, passbooks or safe-deposit boxes are used in any way*". The JMLSG guidance aims to mitigate risks that are specific and proportionate to the crypto sector. For instance, the risk of crypto money laundering increases at the point of exchange, thus firms engaged in the exchange or conversion services are more susceptible money laundering. Accordingly, the current AML framework was developed and transposed from a number of international reviews and recommendations from supranational organisations. For instance, in 2018, the FATF concluded that *'[t]he United Kingdom has a well-developed and robust regime to effectively combat money laundering and terrorist financing. However, it needs to strengthen its supervision, and increase the resources of its financial intelligence* unit'.[194] As a result of this observation, the FCA was granted new legal powers to fine a crypto firm for its failure to monitor and report suspicious activity,[195] and whether it deployed adequate safeguards to protect its customers from illicit activities.[196]

---

[193] ibid.

[194] Financial Action Task Force, 'The United Kingdom's measures to combat money laundering and terrorist financing' (FATF, December 2017) <https://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-united-kingdom-2018.html> accessed 28 August 2021.

[195] FCA Handbook, PRIN 2.1.1 R.

[196] FCA Handbook, SYSC 6.1.1. R; SYSC 3.2.6 R; MLR 2017, reg 19, reg 28(11), reg 31, reg 33.

As per the FATF's guidance, the FCA adopts a 'risk-based' approach in relation to its supervisory and AML regime, in line with the AMLD5 requirements, the FATF recommendations as well as the JMLSG guidance.[197] Here, a 'risk-based approach' underlines the balance between proportionality and efficiency; this means crypto-businesses must maintain adequate safeguards against money laundering, whilst minimising the unintended consequences of AML compliance, such as excessive delay in opening crypto accounts for low-risk clients. Although this seems quite straightforward, striking the right balance in practice whilst meeting FCA expectations is often a more complicated matter. As a result, a firm's AML obligation goes well beyond identifying their clients via KYC.[198] Here, a crypto firm's internal policies, procedures and compliance controls must also be implemented and documented to the FCA's satisfaction. [199] For instance, a new client must undergo an AML risk matrix (i.e. high, medium and low-risk rating),[200] in order to examine the client and the nature of the transaction through a case-by-case risk approach.[201] Following the AML risk matrix, a crypto firm must consider the following questions:

I. Is it a new or higher risk sector? For instance, is the business cash intensive;
II. Is the client from a higher risk jurisdiction? For instance, Russia or Jersey, etc.;
III. Is the client's corporate structure complex? As an example, shell companies; and
IV. Is the client or corporate subject to potential sanctions risk? For instance, Venezuela, Russia, Iran, etc.

The AML risk matrix aims to assess the objective nature of the business relationship.[202] As a result, a crypto firm must continuously monitor each transaction carried by its client and check the origins of the funds.[203] For instance, a crypto business must check the origin of the funds

[197] Supra (n 25).

[198] MLR 2017, reg 28.

[199] MLR 2017, reg 19.

[200] MLR 2017, reg 28.

[201] MLR 2017, reg 33.

[202] Compliance Tyler, 'Part Two — How to write a compliance monitoring programme' (Medium, 14 September 2019) <https://medium.com/@tyler.woollard/part-two-how-to-write-a-compliance-monitoring-programme-7d054ae4c614> accessed 28 August 2021.

[203] FCA Handbook, SYSC 6.3 / SYSC 3.2.6 A-J.

and whether the transaction is consistent with the client's profile, and any unusual transactions must be documented in a risk assessment report.[204]

In addition, a crypto firm must also implement internal systems and controls that mitigate money laundering risks that are specific and proportionate to the nature and scale of its operations.[205] Here, founders, senior management and front office personals all have a crucial role to play in delivering effective governance and risk management.[206] Partly due to international pressures, the FCA has turned its attention to crypto money laundering. It is well established that the FCA has the power to prosecute substantive money laundering offences under the POCA, as a private prosecutor.[207] Here, the POCA applies to both corporate entities as well as natural persons. Part 7 of the POCA criminalises both the process of money laundering and the failure of a crypto firm to report suspicious transactions. Money laundering is widely defined under section 340(11) of the POCA. As a result, the POCA categorises the offence of failing to notify the relevant personnel or a regulatory body, as distinct offences. For instance, section 330 of the POCA, applies if an employee fails to notify the firm's Money Laundering Reporting Officer in relation to suspicious transactions; whilst section 331 of the POCA, applies if the Money Laundering Reporting Officer fails to notify the FCA or the NCA.

However, in terms of substantive money laundering, the Serious Fraud Office ("SFO") and the FCA have overlapping jurisdiction in relation to AML responsibilities in the UK. Nonetheless, an employee can be found guilty under section 330 of the POCA, if the following elements are met:

I. the employee must know or suspect money laundering;
II. the information must have come to them in the course of business;
III. the employee must be able to identify the person and/or property;
IV. the employee must have failed to make a required disclosure; and

[204] MLR 2017, reg 28(11).

[205] FCA Handbook, SYSC 6.1.R / SYSC 3.2.6 R.

[206] FCA Handbook, PRIN 2.1.1 R.

[207] See R v Rollins [2010] WLR 1922, which involved a question of whether the FSA had the power to prosecute offences of money laundering contrary to section 327 and 328 of the Proceeds of Crime Act 2002 (even through the power to prosecute money laundering offences was not expressly provided for by section 402(1) of the Financial Services and Markets Act 2000).

V. no exception(s) apply to their obligation to notify.

Thus, the exception(s) to the general rule are as follows: [1] the relevant information or evidence is ascertained through privilege;[208] or [2] the requirements for the overseas defence are met.[209] The former relates to information received in privileged circumstances, whilst the latter underlines the defence whereby the relevant conduct is deemed to be lawful in the country where the offence took place. For instance, if tax evasion is illegal in the jurisdiction where the funds originate, this rules out the overseas defence.

Overall, it is presumed that offences as set out in the POCA will only apply to acts that occur in the UK or where the offence has a substantial connection the UK.[210] Here, the only exception to the general rule is that the statute must contain explicit 'wording' that an offence will have an exterritorial effect. It is submitted that, although the POCA mentions unlawful acts committed abroad, the offence as per section 330 *itself does not have an exterritorial effect*. In order words, the POCA offences cannot be committed by entities or natural persons with no presence or connection with the UK. Therefore, if a crypto business does not have a registered office in the UK and it does not serve UK clients, it is unlikely the company would be liable for an offence under the POCA. This concept will be further examined in Chapter 4, entitled "Cryptoassets, Illicit Activities and Criminal Proscription".

Money laundering scenarios

According to the United Nations Office on Drugs and Crime, money laundering represents about 2-5% of global GDP, or USD 2 trillion.[211] Money laundering is the process by which illegal profits are disguised without compromising the criminals who wish to benefit from their criminal income.[212] In general, there are a number of ways to launder money, for instance:

[208] Section 330(6)(b)(i) POCA.

[209] Section 330 (7A) POCA.

[210] R v Smith (Wallace Duncan) (No 4) [2004] 3 WLR 229.

[211] United Nations Office on Drugs and Crime, "Money-Laundering and Globalisation' (UNODC, 2020) <https://www.unodc.org/unodc/en/money-laundering/globalization.html> accessed 28 August 2021.

[212] United Nations Office on Drugs and Crime, "The Money-Laundering Cycle' (UNODC, 2020) <https://www.unodc.org/unodc/en/money-laundering/laundrycycle.html> accessed 28 August 2021.

I. **Casinos**: Proceeds of crime is converted into chips, then cashed out in the form of a cheque.[213]

II. **Real estate**: Property is purchased using proceeds of crime, then the buyer sells the property and pockets the legitimate profits.[214]

III. **Horses**: Proceeds of crime is used to purchase and breed horses, or fix horse races, then the person pockets the legitimate profits and winnings.[215]

IV. **High-end art**: The artwork is purchased using proceeds of crime, then the buyer sells the artwork and pockets the additional value as legitimate profit.[216]

V. **Trade based**: The misrepresentation of the price of the invoiced goods or services in order to pocket the additional value as legitimate profit.[217]

VI. **Cryptoassets**: Proceeds of crime is used to purchase cryptoassets through an unregulated crypto exchange and/or unlicensed money transmitting business, then the token holder withdraws the tokens and converts it to fiat currency.[218]

The anonymous and borderless nature of cryptoassets make this technology attractive to front-line criminals as well as international criminal organisations. As a result, criminals appear to be laundering an increasing amount of dirty money through cryptoassets, as seen through the significant increase in crypto money laundering in 2019, from USD 266 million in 2017, to

[213] Ashifa Kassam, 'How criminals use Canada's casinos to launder millions' (The Guardian, 15 October 2018) <https://www.theguardian.com/world/2018/oct/15/canada-money-laundering-casino-vancouver-model> accessed 28 August 2021.

[214] Palash Ghosh, 'Gabon's Bongo Family: Living in Luxury, Paid for By Corruption and Embezzlement' (International Business Times, 15 February 2013) <https://www.ibtimes.com/gabons-bongo-family-living-luxury-paid-corruption-embezzlement-1088930> accessed 28 August 2021.

[215] Ioan Grillo, 'A True Tale of Drug Cartels, Money Laundering and Horse Racing' (The Ney York Times, 22 September 2017) <https://www.nytimes.com/2017/09/22/books/review/bones-joe-tone-trevino-brothers.html> accessed 28 August 2021.

[216] Peter Hardy, 'Art and Money Laundering' (The National law Review, 20 March 2019) <https://www.natlawreview.com/article/art-and-money-laundering> accessed 28 August 2021.

[217] Jason Chuah, Money Laundering Considerations in Blockchain based International Commerce in Zhao, L. and Jia, S. "*Maritime and Commercial Law in China and Europe" (Informa) (Forthcoming 2022), chapter 14.*

[218] The United States Department of Justice, 'Dark Web Vendors Pleads Guilty to Cryptocurrency Money Laundering Conspiracy' (Department of Justice, 2 October 2019) <https://www.justice.gov/usao-sdca/pr/dark-web-vendors-plead-guilty-cryptocurrency-money-laundering-conspiracy> accessed 28 August 2021.

USD 761 million in 2018,[219] and to USD 2.8 billion in 2019.[220] Money laundering can be very simple or highly sophisticated,[221] but most schemes involve three dynamic stages:

I. **Placement**: the process of getting the illegal funds into the financial system;
II. **Layering**: the process of moving money in the financial system to disguised and distanced from its illegal source through a complex webs of transactions, often through offshore companies based in the Cayman Islands; and
III. **Integration**: the process by which the illicit funds are absorbed and integrated into the main stream economy, for instance purchasing real estate.[222]

Placement

Cryptoassets can be purchased with cash via a Bitcoin ATM[223] or with other types of tokens. Unfortunately, given the international nature of crypto exchanges, online trading platforms have a varying level of AML compliance. Legitimate exchanges, such as Coinbase, Gemini, etc.,[224] are licenced and follows international requirements for KYC verification and are AML compliant. Whilst other unregulated exchanges and/or crypto 'exchangers' are not AML complaint and would accept cash "*with no questions asked*" in exchange for tokens.[225]

[219] Penny Crosman, 'Crypto money laundering up threshold in 2018: report' (American Banker, 3 July 2018) <https://www.americanbanker.com/news/crypto-money-laundering-rose-3x-in-first-half-2018-report> accessed 28 August 2021.

[220] Mike Orcutt, 'Criminals laundered $2.8 billion in 2019 using crypto exchanges, finds a new analysis' (MIT Technology Review, 16 January 2020) <https://www.technologyreview.com/f/615064/cryptocurrency-money-laundering-exchanges/> accessed 28 August 2021.

[221] Bonnie Buchanan, 'Money laundering – a global obstacle' (2004) 18 Research in International Business and Finance 1, 115.

[222] The Crown Prosecution Services, 'Proceeds of Crime Act 2002 Part 7 - Money Laundering Offences' (CPS, 1 March 2018) <https://www.cps.gov.uk/legal-guidance/proceeds-crime-act-2002-part-7-money-laundering-offences> accessed 28 August 2021.

[223] Buy Bitcoin Worldwide, 'How to buy bitcoins with cash or cash deposits' (Buy Bitcoin Worldwide, 2020) <https://www.buybitcoinworldwide.com/en/buy-bitcoins-with-cash/> accessed 28 August 2021.

[224] Craig Adeyanju, 'What Crypto exchanges do to comply with KYC, AML and CFT regulations' (Coin Telegraph, 17 May 2019) <https://cointelegraph.com/news/what-crypto-exchanges-do-to-comply-with-kyc-aml-and-cft-regulations> accessed 28 August 2021.

[225] The United States Department of Justice, 'Bitcoin dealer indicted on money laundering charges; held without bond' (The US Department of Justice, 17 August 2018) <https://www.justice.gov/usao-sdca/pr/bitcoin-dealer-indicted-money-laundering-charges-held-without-bond> accessed 28 August 2021.

Layering

Criminals then use anonymising service providers to protect their identities via privacy tokens like Monero.[226] Data anonymisation aims to conceal the token holder's identity and data by deleting or encrypting personal information from the database,[227] and transactions are thus untraceable as it uses the concept of ring signatures and stealth addresses to hide the identities of the seller and buyer.[228] Effectively, this will obfuscate the origin of the cryptoasset.

Integration

A simple method of legitimising the illicit income is to withdraw the digital asset via a Bitcoin ATM which accepts bitcoins and credits the criminal with cash.[229] A more sophisticated method includes a random gift or airdrop of a cryptoasset.[230] In these cases, the criminal must send the anonymised token from their digital wallet to a regulated exchange then trade the anonymised token for Bitcoin or Ether or any other cryptoasset that can be exchanged for fiat money.[231] Criminals exploit loopholes and weaknesses in countries with little or no AML regulation and end with the clean Bitcoin or Ether, which can be converted into local fiat currency.[232]

As mentioned previously, AML enforcement varies significantly, from relatively strict regulations in much of Europe to practically non-existence in other countries. In response, the

---

[226] Monero, 'Monero: a reasonable private digital currency' (Monero, 2020) <https://www.getmonero.org/> accessed 28 August 2021.

[227] Jake Frankenfield, 'Data Anonymization' (Investopedia, 25 June 2018) <https://www.investopedia.com/terms/d/data-anonymization.asp> accessed 28 August 2021.

[228] Shobhit Seth, 'The five most private cryptocurrencies' (Investopedia, 25 June 2019) <https://www.investopedia.com/tech/five-most-private-cryptocurrencies/> accessed 28 August 2021.

[229] Weusecoins, 'Bitcoin ATM map how to find and use Bitcoin ATMs' (Weusecoins, 2020) <https://www.weusecoins.com/en/bitcoin-atms/> accessed 28 August 2021.

[230] Wikipedia, 'Airdrop (cryptocurrency)' (Wikipedia, 2020) <https://en.wikipedia.org/wiki/Airdrop_(cryptocurrency)> accessed 28 August 2021.

[231] Chris McCoy, 'Overview: convert cryptocurrency to fiat currency' (BlockchainDK, 18 December 2017) <https://www.blockchaindk.com/2017/12/18/convert-cryptocurrency-to-fiat-currency/> accessed 28 August 2021.

[232] Elliptic, 'Bitcoin money laundering: how criminals use crypto (and how MSBs can clean up their act) (Elliptic, 18 September 2020) < https://www.elliptic.co/our-thinking/bitcoin-money-laundering> accessed 28 August 2021.

FATF advised member states to adopt a global mandate for crypto firms to collect and share customer identities for transactions over a certain threshold, known as the *Travel Rule*.[233] Essentially, the Travel Rule requires crypto exchanges to pass information about their customers to one another when transferring funds between exchanges as a means to combat the *layering* and *integration* issue as described above. However, CoinDesk notes: "*people are going to lean towards the countries with either weak implementation or enforcement. It will be interesting to see how this scenario plays out*".[234]

Against the above backdrop, this thesis sets out the AML requirements for the crypto sector in the UK. After setting the context, the subsequent chapters will underline the AML requirements for crypto businesses and examine the UK's risk-based approach in relation to crypto money laundering. Here, this research examines primary forms and types of crypto money laundering schemes and the devices used; and the crypto AML framework that can be applied to the enforcement of the AML regulations in the UK and abroad. It is submitted that, whether an English worldwide freezing order can be enforced abroad will depend on the law of that particular country. As a result, international cooperation is critical due to the global nature of the underlying technology, making cryptoassets well suited for carrying out money laundering at an international scale. In order to investigate this phenomenon, the subsequent chapters are structured as follows:

I. **Chapter 2** investigates the key AML regulations in the UK and provide an overview of the essential obligations applicable to the crypto sector. Here, Chapter 2 aims to introduce factors that give rise to crypto money laundering as well as risks specific to the AML regime in the UK.
II. **Chapter 3** inquiries into MLR framework through an agency perspective, and reviews the relevant compliance obligations, such as KYC and AML, in the context of crypto money laundering. Here, the agency model is the appropriate theoretical framework

[233] Mike Orcutt, 'A new money-laundering rule is forcing crypto exchanges to scramble' (MIT Technology Review, 6 February 2020) <https://www.technologyreview.com/f/615151/crypto-fatf-travel-rule> accessed 28 August 2021.

[234] CoinDesk, 'Inside the standards race for implementing FATF's travel rule' (Coin Desk, 4 February 2020) <https://www.coindesk.com/inside-the-standards-race-for-implementing-fatfs-travel-rule> accessed 28 August 2021.

used to discuss the different types of agency relationships that are affected by the UK's approach to AML regulations.

III. **Chapter 4** sets out potential scenarios in which money launderers may use cryptoassets to launder illicit funds and activities whilst examining the mens rea as well as actus reus requirements for the primary money laundering offences under the POCA in the UK.

IV. **Chapter 5** builds on Chapter 4 by examining the overall risk associated with the convertibility of cryptoassets to fiat. This chapter will examine the enforcement process in relation to the seizure of illicit cryptoassets held in the UK as well as abroad.

V. **Chapter 6** examines the main conclusion arising from this research and sets out a way forward: Namely whether smart contracts are the future for AML compliance? For instance, parliament can mandate the use of all FCA approved smart contract for crypto transactions transacted in the UK, and effectively circumvent the potential jurisdictional disputes that may arise, if and when, the relevant asset is held abroad.

Chapter 2: The UK's legal and AML response to cryptoassets

This chapter investigates the UK's legal and enforcement response to crypto money laundering. Here, this research will explain what is regulated by the FCA and define the regulatory scope in relation to how this framework will impact the crypto sector. In other words, this considers whether certain activities relating to cryptoassets fall within the FCA regulatory parameter, as per, Part 4A of the Financial Services and Markets Act 2000 ("FSMA 2000"), the Electronic Money Regulation 2017 (SI 2017/99) ("EMRs") and the Payment Services Regulations 2017 (SI 2017/752) ("PSRs 2017"). As of January 2020, the FCA's anti-money laundering and counter-terrorist financing regime for the crypto sector, as per the MLR, which came into force. As mentioned, there is currently no internationally accepted definition nor taxonomy concerning the categorisation of cryptoassets. In the absence of an international taxonomy, the UK Jurisdictional Taskforce, thus defines cryptoassets as "cryptographically secured digital representations of value or contractual right that use some type of DLT and can be transferred, stored or traded electronically".[235] Here, the UK adopts the term cryptoassets, rather than virtual currencies or cryptocurrencies, because it was deemed to be more tech neutral, and thus, capturing a wider range of tokens than, for instance, "cryptocurrencies", which is designed merely as a means of exchange. In general, cryptoassets are categorised as follows:

Type of token	Are they regulated?	Regulators view on whether they should be regulated?
Exchange/Payment Token: Provides a means of payment, but holders have no claim on the issuer, nor any rights or access in respect of the issuer.	**Yes**, if they amount to regulated payments services or meet the definition of e-money. **No**, if fiat funds are not involved – they are not regulated as an investment instrument	These tokens pose 'new challenges to traditional forms of financial regulation'. While they are intended for payment/exchange, some are being treated as investments by crypto investors.
Security/Asset Token: Providers rights such as ownership (of issuer or an	**Yes**, if the underlying asset is regulated or if the token has the characterisation of a regulated	The novelty of some tokens may mean that the market participants do not correctly understand the scope of current

[235] Financial Conduct Authority, "Cryptoassets: How we define cryptoassets" (FCA, 2019) <https://www.fca.org.uk/firms/cryptoassets> accessed 28 August 2021.

asset), repayment of a sum of money, or entitlement to share in future profits	investment instrument (e.g. a share, bond, unit, etc)	regulation. However, security tokens are clearly caught by current regulation, further guidance is needed for clarification.
Utility Token: Provides access to a specific application service, but not only accepted by the issuer.	**No**, tokens of this type do not normally have the characteristics of a regulated investment/instrument.	These tokens should not be regulated if they are not transferable. However, if they are transferable, they may have risks similar to regulated investment. Further consideration of whether this warrants regulation is needed.
Hybrid Tokens: Provide any mixture of the above	See above	See above
Stablecoins: Provide any mixture of the above	See above	See above
Non-fungible Tokens (NFTs): Provide a representation of rights to an underlying tokenised digital asset giving security of ownership.	**No**, tokens of this type do not normally have the characteristics of a regulated investment or instrument. Thus, NFTs are not regulated in the UK.	The novelty of NFTs may mean that the market participants do not correctly understand the scope of current regulation. However, certain existing regulations may apply to a particular NFT depending on the underlying structure, features and how it is marketed.

The FCA have suggested that 'labels' are not very helpful because cryptoassets can be structured in so many ways and regulation must be determined on a case-by-case.[236] However, in general, any token that is not a security token or an e-money token, are deemed to be an unregulated token – this includes any [1] utility tokens that do not fit the requirements as prescribe by the e-money regulation or [2] are exchange tokens. Subsequently, unregulated tokens or exchange tokens, such as Bitcoin or other cryptoassets, are only regulated in the UK for money laundering purposes, thus investors will not have access to the Financial Ombudsman

[236] Harry Eddis, Richard Hay and Simon Treacy, 'UK FCA spells out when cryptoassets fall within the scope of regulation' (Linklaters LLP, 1 August 2019) <https://www.linklaters.com/en/insights/blogs/fintechlinks/2019/august/uk-fca-spells-out-when-cryptoassets-fall-within-the-scope-of-regulation> accessed 28 August 2021.

Service or the Financial Services Compensation Scheme for further regulatory protection.[237] However, whether a cryptoasset will fall within the regulatory perimeter will depend on the token's underlying features, it is thus fact specific and, on a case-by-case basis. Interestingly, with the exception to regulated crypto businesses, the FCA does not regulate the sale or transfer of unregulated tokens nor will the FCA intervene on behalf of crypto investors who lose their investments due to price volatility or market manipulation.[238]

E-Money Tokens

The UK's regulatory response to cryptoassets have developed overtime, with many of the initiatives only emerging from 2018. Here, the FCA divided the crypto market into three sectors: [1] security token; [2] exchange tokens; and [3] utility tokens. However, following the final report published July 2019, the FCA reframed cryptoassets as:

> **[1] Securities token (regulated):** largely unchanged from the draft guidance, this covers tokens which qualify as investments like shares, bones or units in a fund;
> **[2] E-money tokens (regulated):** cryptoassets that meet the definition of e-money are regulated; and
> **[3] Unregulated tokens:** any cryptoasset that is not a security token or an e-money token is unregulated, such as Bitcoin and Litecoin or utility tokens.

The FCA reframed the taxonomy to include 'e-money tokens' which falls under the EMRs and requires FCA authorisation. As a result, the buying and selling of unregulated tokens does not require FCA authorisation. However, dealing in crypto derivatives deriving its value from unregulated tokens, for instance Bitcoin, is a regulated activity (even if the underlying cryptoassets are unregulated). According to the final guidance published by the FCA, aimed to

[237] Financial Conduct Authority, "Consumers: Cryptoassets" (FCA, 2021) <https://www.fca.org.uk/consumers/cryptoassets> accessed 28 August 2021.

[238] Steve Browning, 'Briefing Paper: Cryptocurrencies: Bitcoin and other exchange tokens' (House of Commons Number 8780, 19 February 2020) < https://researchbriefings.files.parliament.uk/documents/CBP-8780/CBP-8780.pdf> accessed 28 August 2021.

[1] reframed the taxonomy (as per above) and [2] to provide guidance pertaining to when tokens might constitute e-money. As a result, the FCA expect key participants within the crypto space to take this new guidance into consideration. Therefore, if a company acts in line with the guidance provided by the FCA, then the UK government will treat them as having complied with the relevant laws and AML requirements. The FCA created a dedicated webpage for cryptoassets listing all regulated as well as unregulated tokens (to date) - found **here** https://www.fca.org.uk/firms/cryptoassets.

As a result, the FCA only regulates two types of cryptoassets: [1] security token and [2] e-money tokens. However, when a crypto firm carries on activities that involve payment services, i.e. exchanging fiat to crypto, relating to any type of token, regulated or unregulated, the business will be subject to registration requirements under the Payment Services Regulations 2017/752 ("PSR"). Here, the regulatory guidance echo that of 'tech neutrality' in that the requirement to have the appropriate authorisation or registration applies regardless of the underlying technology. In other words, the FCA's cryptoassets guidance considers both unregulated as well as regulated tokens. Nonetheless, the FCA explains in its final guidance that, whilst it is not binding on the courts,[239] and as mentioned above, if a crypto-business acts in line with the guidance it will treat the business as having complied with the relevant requirement.[240] However, the FCA notes that, whether a new cryptoasset falls within the regulatory regime can only be made on a case-by-case basis. In response to this uncertainty, the FCA launched the 'FCA Innovate' and its purpose is twofold: to provide direct support to crypto-firms and to oversee the FCA's innovation policy.[241] The FCA's Innovate programme aims to provide crypto businesses specific feedback on its regulatory model and AML system.

It is admittable that the FCA's guidance is murky at best, the final policy statement includes several case studies based on various propositions to help individuals to establish whether they are dealing with a regulated or an unregulated cryptoasset. After that, whether a

[239] The guidance only represents the regulator's views; thus, does not bind the courts, but it can be a persuasive factor in judicial outcomes, for instance, enforcing contracts.

[240] Financial Conduct Authority, Guidance on Cryptoassets: Feedback and Final Guidance to CP 19/3 (FCA, Policy Statement PS19/22) <https://www.fca.org.uk/publication/policy/ps19-22.pdf> accessed 28 August 2021.

[241] Financial Conduct Authority, 'FCA innovation – fintech, regtech and innovative businesses' (FCA, 2020) <https://www.fca.org.uk/firms/innovation> accessed 28 August 2021.

crypto firm requires authorisation to carry on that activity in accordance with FSMA or apply to be registered under PSR or EMRs. In order to streamline its regulatory guidance, the FCA provides numerous examples of what it considers regulated versus unregulated. As a result, the former consists of security tokens which are considered as specified investments under the Regulated Activities Order,[242] and falls within the scope of FSMA. Subsequently, e-money tokens are regulated under EMRs. As indicated above, a security token is a cryptoasset that meets the definition of a specified investment under the Regulated Activities Order, due to the fact that it provides rights and obligations similar to specified investments. Here, a security token is similar to traditional financial instruments such as shares or debentures. Nonetheless, a cryptoasset will be considered a regulated token based on its underlying structure and the token's lifecycle. For instance, if a utility token becomes a security token, it is then considered to be a security token from the outset.

In addition, an e-money token is a regulated cryptoasset under EMRs because it has an "…electronically stored monetary value, as represented by a claim on the electronic money issuer, which is issued on receipt of funds for the purpose of making payment transactions; accepted as a means of payment by a person other than the electronic money issuer".[243] In other words, e-money tokens must enable users to make a payment transactions with a third party, therefore, the token must be accepted by various parties (not just the issuer of the e-money token). Here, e-money tokens must transact with fiat balances as well as other various types of online wallets and/or other prepaid cards to the EMRs definition of e-money. In other words, a token that represents a unit of account, rather than representing fiat funds, are unlikely to be considered to be e-money. Accordingly, a token which is pegged to a fiat currency, commonly known as "Stablecoins", could also meet the definition of e-money.

Finally, unregulated tokens are essentially any tokens which do not meet the above requirements. Here, unregulated tokens are thus, not considered security tokens nor an e-money token. In general, unregulated tokens includes (some) utility tokens as well as exchange tokens. Henceforth, unregulated cryptoassets are not within the FCA's regulatory perimeter, thus no

[242] Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (SI 2001/544).

[243] Financial Conduct Authority, 'PERG 3A.3 the definition of electronic money' (FCA, 2013) <https://www.handbook.fca.org.uk/handbook/PERG/3A/3.html> accessed 28 August 2021.

protection is offered to investors who choose to buy them and use them as means of exchange or payment. In other words, the FCA does not regulate the sale or transfers of unregulated tokens, and as a result, customers will not have access to the Financial Ombudsman Service and the Financial Services Compensation Scheme.[244] Accordingly, although exchange token, such as Bitcoin, are used as an alternative to fiat currency, they are nonetheless classified as an unregulated token by the FCA. The FCA considers unregulated tokens as 'other assets' that remain outside the regulatory perimeter, such as fine wine or art, bought speculatively with a view to realising profits.[245] In other words, transactions in relation to the transfer, purchase and sale of exchange tokens, are the unregulated by the FCA. Similarly, utility tokens may grant purchasers access to a current or prospective product or service (akin to pre-payment vouchers), also fall outside the regulatory perimeter and are classified as unregulated tokens by the FCA. Subsequently, stablecoins varies significantly in terms of structure and arrangement; however, all stablecoins share one common purpose in that it attempts to peg and/or stabilise their value using a variety of mechanisms. Most commonly, stablecoins are backed by fiat currencies, whilst others are backed with different types of assets (i.e. crypto-collateralised and/or asset-backed), or algorithmically stabilised tokens via algorithms that control the support of the tokens to influence price. Here, stablecoins may fall within the definition of e-money or a security token, however, it will depend on the underlying structure of the asset, and more importantly, the rights assigned to the tokens.

Crypto Derivatives

As of January 2021, the FCA banned the marketing, distribution and sale in and/or from the UK to all retail investors,[246] of investment products, such as derivatives (i.e. contract for difference, options and futures) and exchange trade notes, that reference certain type of unregulated transferable cryptoassets.[247] The FCA views these financial products are 'ill-suited' for retail investors who cannot understand the value and risk of crypto derivatives or exchange

[244] Financial Conduct Authority, 'Cryptoasset investment scams' (FCA, 2020) <https://www.fca.org.uk/scamsmart/cryptoasset-investment-scams> accessed 28 August 2021.

[245] Supra (n 242) FCA.

[246] Retail investors are defined as all investors that are not institutional investors.

[247] FCA, 'PS20/10: Prohibiting the sale to retail clients of investment products that reference cryptoassets' (FCA, October 2020) <https://www.fca.org.uk/publications/policy-statements/ps20-10-prohibiting-sale-retail-clients-investment-products-reference-cryptoassets> accessed 28 August 2021.

trade notes that reference cryptoassets.[248] In support of this assertion, the FCA published a Technical Annex providing a description of the supporting data alongside the rules banning the sale of crypto-derivatives to retail investors. In the Technical Annex, the FCA finds that, 47% of retail investors bought cryptoassets 'as a gamble that could make or lose money', as evidenced in the 2017 'investment mania'.[249] The FCA concluded that, there is a strong correlation between the price of cryptoassets and the number of Google searches for these cryptoassets, thus the 2018 'crypto-bubble' was the result of retail participation.[250] In addition, the regulator found that there was significant price dislocation across exchanges, coupled with the extreme price fluctuations, the FCA therefore concluded that, crypto-derivatives are 'ill-suited' to retail investors due to lack of reliably available information for investors to assess the value and risks of crypto derivatives and exchange trade notes.[251] Notwithstanding the FCA's conclusion, 97% of the respondents opposed banning retail investors from investing in crypto derivatives.[252]

On 6 October 2020, the FCA published a policy statement (PS20/10), prohibiting the sale of crypto-derivatives and exchange traded notes referencing unregulated transferable cryptoassets to retail investors.[253] Interestingly, the definition of unregulated transferable cryptoassets was amended to exclude crypto-commodities and central bank digital currencies.[254] As a result, from 6 January 2021, crypto firms must cease the marking, distribution or selling of crypto derivatives and exchange traded notes to its retail customers.[255]

[248] Financial Conduct Authority, *Prohibiting the sale to retail clients of investment products that reference cryptoassets* (FCA Policy Statement, October 2020)

[249] Financial Conduct Authority, 'Prohibiting the sale to retail client of investment products that reference cryptoassets: Technical Annex' (FCA, October 2020) <https://www.fca.org.uk/publication/policy/ps20-10-technical-annex.pdf> accessed 28 August 2021.

[250] ibid.

[251] ibid.

[252] Supra (n 242) FCA.

[253] Existing retail investors can still remain invested following the prohibition, until they choose to disinvest. There is no time limit on this and the FCA does not require or expect firms to close out retail investor's positions unless the client ask for this.

[254] Supra (n 242) FCA.

[255] ibid.

Crypto Regulation

The transfer of all regulated as well as unregulated tokens will inevitably fall within the scope of the UK's AML and CFT regime, as governed by the MLR. For the purposes of the MLR, a cryptoasset is defined as a cryptographically secured digital representation of value or contractual right uses a form of DLT and can be transferred, stored, or traded electronically.[256] This board definition aims to capture all tokens. The MLR are applicable to UK businesses identified as most vulnerable to the risk of money laundering and terrorist financing, such as cryptoasset exchange providers and custodian wallet providers.[257] The FCA expects cryptoasset exchange providers and custodian wallet providers to comply with the AML standards as set out in the FATF recommendations and the MLR. This section focuses on the UK's AML/CTF framework for cryptoasset firms under the MLR; and as such, this chapter will not consider the FCA's regulation of cryptoassets under FSMA, PRSs 2017 and EMRs. Here, "crypto firms" means those businesses that fall within the scope of the MLR.

In Peter Yeo's article titled, 'Crypto-assets: Regulators' dilemma', he argues that most advanced economises have reached a consensus to regulate cryptoassets in alignment with the FATF recommendations.[258] Whilst others argues that, the international response have been fragmented, which proliferates uneven playing-fields and induces the risk of forum-shopping.[259] It is submitted that, whilst there is no one-size-fits-all solution, international norms and obligations via FATF standards, enables the smooth application of existing AML/CFT rules and tax laws to cover cryptoassets as well. The MLR form part of the UK's apparatus as well as defence against, crypto money laundering and terrorist financing. Here, the MLR transpose the provisions of the EU's MLD4, MLD5 as well as the revised Wire Transfer Regulation (EU 2015/848) into domestic UK law. The aforementioned pieces of legislation have strengthened the EU as well as the UK's AML and CFT framework, whilst also ensuring the UK is aligned with the FATF's international AML and CTF standards. Consequently, this section will firstly examine the domestic requirements as per the MLR, and thereafter, the FATF, AML standards,

[256] MLRs 2017, Regulation 14A(3)(a).
[257] MLRs 2017, Regulation 8(2) and (3)
[258] Peter Yeo, 'Crypto-assets: Regulators' dilemma' [2020] 4 Journal of Business Law 265.
[259] Supra (n 243) FCA.

then identifying the red flag indicators of crypto money laundering. The latter aims to deduce the variables and detect suspicious transactions by reviewing the potential red flags. Overall, this section will explore MLR as well as the FATF's guidance for a risk-based approach to AML compliance. It is submitted that, the risk-based approach offers regulators as well as businesses the degree of flexibility which in turn is intended to increase efficiency and effectiveness of the AML systems and controls implemented by crypto firms.

In 2020, the Money Laundering and Terrorist Financing (Amendment) Regulations,[260] amended the MLR to implement AMLD5 which clarifies issues pertaining to cryptoassets. The MLR defines "cryptoassets", as a cryptographically secured digital representation of value or contractual rights that uses a form of DLT and can be transferred, stored or traded electronically,[261] which also includes a right to a cryptoasset, or an interest in a cryptoasset.[262] The Taskforce's definition of cryptoassets, confined the scope of this legislation to those using blockchain technology.[263] The definition implemented by the UK government still meets the ultimate aim of the AMLD5, which was to regulate the crypto sector and enforce the compliance of AML and CTF rules in the UK.

Following the implementation of the AMLD5, the HM Treasury provided further guidance in relation to the categories of the following tokens:

[1] **Exchange tokens**: Tokens or cryptoassets, such as Bitcoin, which use a blockchain platform. Not issued or backed by a central bank. Exchange tokens do not provide the type of rights or access rights provided by other cryptoassets, such as security or utility tokens, but are used a means of exchange or investment.

[2] **Security tokens**: Tokens considered to be a specified investment and are regulated by FSMA. Here, securities tokens provide rights such as ownership, repayment, or entitlement to

[260] 2019 (SI 2019/1511)

[261] MLRs 2017, Regulation 14A(3)(a).

[262] MLRs 2017, Regulation 14(3)(c).

[263] HM Treasury, "Transposition of the Fifth Money Laundering Directive: Response to the consultation" (HM Treasury, January 2020) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/860491/5MLD_Consultation_Response.pdf> accessed 28 August 2021.

a share in future profits. In addition, such tokens may also be transferable securities or financial instruments under the MiFID II Directive.[264]

[3] **Utility tokens**: Tokens, such as DogCoin, can be redeemed for access to a specific product or service.[265]

In short, the above tokens are considered digital representation of value, or in some cases, contractual or access rights, thus within the regulatory scope of the MLR. Subsequently, crypto firms identified by the FATF are most vulnerable to money laundering. As a result, according to Regulation 8 of the MLR, vulnerable crypto firms include "cryptoasset exchange providers"[266] and "custodian wallet providers".[267] However, these vulnerable firms are only caught by MLR, if these firms' transactions are considered as "being carried on by way of business" in the UK.[268]

Thus, determining whether a cryptoasset activity is being carried on by way of business is not clear cut. As a result, the FCA sets out the following factors to consider when determining if a crypto activity is "being carried on by way of business" in the UK:

1. Does the individual and/or entity, acts or holds itself out in a way that would suggest it is performing a service and/or business transaction related to cryptoassets?
2. Does the individual and/or entity, receive direct and/or indirect benefit from providing the service. The FCA will also consider how significant the cryptoasset activity is in relation to the other activities carried on within that firm.
3. Finally, the regulator will examine how frequent the cryptoasset activity is being carried on as a business.

On the FCA's crypto-registration webpage, the FCA explains that when determining whether a crypto activity is "being carried on by way of business" in the UK will be assessed on a case-

[264] Markets in Financial Instruments (MiFID II) Directive 2014/65/EU.

[265] HM Treasury, 'Transposition of the Fifth Money Laundering Directive: Consultation' (HM Treasury, April 2019) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/795670/20190415_Consultation_on_the_Transposition_of_5MLD__web.pdf> accessed 28 August 2021.

[266] MLRs 2017, Regulation 8(2).

[267] MLRs 2017, Regulation 8(3).

[268] MLRs 2017, Regulation 8(1).

by-case basis, and as such, assessed based on its own merits. As a result, the FCA will examine the nature of the business being undertaken, and thereafter, will take into account a number of factors, namely, whether the individual or entity have a registered office in the UK, that may indicate that the crypto activity is being carried out in the UK. Conversely, if the crypto firm does not have a registered office in the UK, then the FCA will examine whether the crypto activity is being carried out by an UK entity and whether the presence of that UK entity means that the business is being carried out in the UK. It is important to note, when a crypto firm is registered abroad and the entity does not have a registered office in the UK, it is unlikely to fall within the scope of "being carried on by way of business" in the UK, as per the FCA guidance.[269]

Cryptoasset exchange providers

The taxonomy "cryptoasset exchange provider" is defined in Regulation 14A(1) of the MLR. Following the MLR, an individual and/or entity who, by way of business, provides one or more regulated crypto activities as well as services in scope, such as exchanging or arranging or making arrangement with a view of exchanging, fiat currency to crypto, and vice versa. For instance, exchanging pound or any other central bank backed currency or in any medium of exchange (i.e. recognised commodities, such gold, diamond, old, etc thus not include a cryptoasset) for a cryptoasset.[270] Subsequently, the individual and/or entity may also provide this service with a view to the exchange, one cryptoasset for another. In addition, the individual and/or entity may also operate a machine that uses algorithms or other automated process to exchange cryptoassets for money or money for cryptoassets. In order words, individuals and/or entities based in the UK, providing peer-to-peer ("P2P") services, automated teller machines as well as businesses issuing new cryptoassets via ICOs are all captured by the MLR.[271]

Interestingly, the HM Treasury has provided some additional guidance in relation to the implementation of AMLD5, and more importantly, on how parliament determines the scope and regulation of crypto exchange providers under MLR. In the HM Treasury's Transposition

[269] Financial Conduct Authority, 'Cryptoassets: AML/CFT regime: Register with the FCA' (FCA, 1 October 2020) <https://www.fca.org.uk/cryptoassets-aml-ctf-regime/register> accessed 28 August 2021.

[270] MLRs 2017, Regulation 14A(3)(b).

[271] Supra (n 260) Yeo.

of the Fifth Money Laundering Directive: Response to the Consultation, it was initially submitted that, all businesses involved with the issuance of new cryptoassets should be brought in scope of the MLR.[272] However, responses from the crypto community suggested that due to the crypto market being relatively small, the scale and extent of AML/CTF response would be disproportionate to the relative threat. As a result, the community was divided on whether businesses facilitating P2P exchange services should be brought in scope. Proponents expressed reservations about difficulties of enforcing complex AML regulations when the market is not fully matured (and in turn, hamper innovation).[273] Opponents, on the other hand, suggests that the use of cryptoasset for money laundering and terrorist financing purposes are increasing in the UK.[274] There was, however, some general consensus that where the provider is a centralised UK entity that is completing, matching or authorising a transaction for users, this should be captured by the MLR.[275] Following this assertation, the UK FCA proceeded on this basis, since it is proportionate to the country's money laundering risk.[276]

Moreover, there was a lack of consensus in relation to the definition of 'privacy coins', for instance, Monero or Zcash,[277] a type of cryptoasset that hides data about its users, thus facilitating anonymous transactions.[278] Many commentators suggest that the phrase 'private coins' was ambiguous, due to the notion that the degree of privacy of each token is constantly changing (via advancement in technology, and etc).[279] Here, the FCA agrees with commentators, and stated that it should be the responsibility of the issuer or platform on which such privacy tokens are issued or exchanged to comply with the AML standards as set out in the MLR.[280] In other words, privacy tokens will be regulated at the point at which a UK crypto exchange deals in them.[281]

---

[272] Supra (n 265) FCA.

[273] ibid.

[274] ibid.

[275] ibid.

[276] ibid.

[277] Shobhit Seth, 'The five most private cryptocurrencies' (Investopedia, 24 May 2020) <https://www.investopedia.com/tech/five-most-private-cryptocurrencies/> accessed 28 August 2021.

[278] Supra (n 265) FCA.

[279] ibid.

[280] ibid.

[281] ibid.

As aforementioned, due to the crypto sector in the UK, being relatively small, enhanced AML/CTF laws would be disproportionate to the relative threat; the UK government decided, not to bring publishers of open-source software into scope. In other words, non-custodian wallet providers activities not to be brought into scope of the MLRs on the ground that AML and CFT regulation should be carried out on an activities-basis only.[282] Here, the JMLSG submits that, the definition of a cryptoasset exchange provider in accordance to MLRs is technologically neutral.[283] Here, the definition is broad, as it pertain to 'arranging or making arrangement with a view to the exchange' and as such, the JMLSG suggests that the MLR does not intend to capture firms that only acts as a bulletin board.[284] Nonetheless, JMLSG notes that the FCA will assess the business models on a case-by-case basis.

Custodian Wallet Providers

The taxonomy "custodian wallet provider" is defined in Regulation 14A(2) of the MLR. Following the MLR, an individual and/or entity who, by way of business, provides services to safeguard, or to safeguard and administer, such as: [1] providing cryptoasset services on behalf of its customers; and/or [2] holding, storing and transferring private cryptographic keys on behalf of its consumers.[285] In accordance with the guidance as discussed above, the MLR does not capture decentralised non-custodian wallet providers; however, the regulation does capture centralised custodian wallet providers. In addition to the guidance provided by the JMLSG notes that, the definition in MLR relates 'to the hold, store and transfer of crypto assets' as per Regulation 14A(2), thus excluding non-custodial wallet service providers. As a result, companies who merely hold and store private keys, and do not administer the transferring of cryptoassets will not be captured by the MLR.[286]

[282] ibid.

[283] The Joint Money Laundering Steering Group, 'Prevention of money laundering and combating terrorist financing: Part II Sectoral Guidance' (JMLSG, June 2020) <https://secureservercdn.net/160.153.138.163/a3a.8f7.myftpupload.com/wp-content/uploads/2020/07/JMLSG-Guidance_Part-II_-July-2020.pdf> accessed 28 August 2021.

[284] ibid.

[285] MLRs 2017, Regulation 14A(2).

[286] Supra (n 285).

In accordance with the MLR, crypto firms in scope, must comply with a range of AML obligations. Most of these requirements are the same AML obligations that traditional institutions must follow.[287] Following the implementation of the MLR, the FCA is now required to maintain a register of all crypto firms carrying on activities in the UK, such as "cryptoasset exchange providers"[288] and "custodian wallet providers".[289] Subsequently, the registration of crypto businesses enables the FCA to act as the gatekeeper and supervise the implementation of its AML objectives. In order words, this initial registration process allows the FCA to determine whether each applicant has the necessary AML/CTF systems and controls in place on an ongoing basis. If the FCA is not satisfied with an applicant's internal AML/CTF/KYC systems and controls, it will refuse to register the applicant and the business will not be permitted to undertake any regulated activity in the UK. In other words, the applicant must not carry on its crypto business or be subject to the FCA's criminal and civil enforcement powers.

As a result, "cryptoasset exchange providers" and "custodian wallet providers", must register with the FCA, unless the crypto firm fall within the Temporary Registration Regime.[290] The Temporary Registration Regime, existing crypto firms have until 31 March 2022 to be registered with the FCA[291]. However, crypto firms (whether registered or not) are expected to comply with the required standards under the MLR and are still at risk of FCA enforcement action for breach of AML/CFT rules.[292] Interestingly, non-crypto firms, such as financial firms and services providers, authorised under the FSMA do not have to register under the MLR framework as well (this is to prevent unnecessary duplication in the financial sector). By contrast, crypto firms authorised under the FSMA, must also register under the MLR even if they are already regulated and/or authorised under the FSMA.[293] Here, the FCA underlines that, 'business that are already registered or authorised with the FCA for other activities (e.g. e-money institutions, payment services and FSMA firms) will also have to register with the FCA

[287] MLRs 2017, Regulation 54(1A).

[288] MLRs 2017, Regulation 14A(1).

[289] MLRs 2017, Regulation 14A(2).

[290] MLRs 2017, Regulation 51(1)-(5).

[291] Financial Conduct Authority, "Cryptoassets: AML/CTF regime: Register with the FCA" (FCA 19 March 2021) <https://www.fca.org.uk/cryptoassets-aml-ctf-regime/register> accessed 28 August 2021.

[292] ibid.

[293] ibid.

if they are carrying on relevant cryptoasset activities'.[294] As a result, crypto firms that operate and act 'by way of business' in the UK, as set out in Regulation 14A(1) of the MLR, must register with the FCA. However, the assessment on whether an activity is being carried on 'by way of business' in the UK are assessed on a case-by-case basis; thus an arbitrary assessment.

Furthermore, in terms of the application and enforcement of the AML laws, Regulation 9 of the MLR provides a critical insight as to the meaning of 'carrying on business in the United Kingdom', it is essentially measured by reference to a registered office based in the UK. In addition, Regulation 9 of the MLR, provides that crypto firms will be subject to CDD requirements when the firm has an established 'business relationship' with a customer based in the UK.[295] Thus, in order to manage accounts and book transactions in the UK,[296] the crypto firm,[297] must establish a business relationship with the client and must meet the required AML standards. For instance, Regulations 27 to 32 of the MLR, provides a general framework for CDD, the level of CDD required (simplified, general, or enhanced), however the level of CDD or EDD will depend on the individual and their perceived level of risk.

The FCA's jurisdiction over crypto firms

The FCA has statutory powers under both the MLR and the FSMA to investigate and mandate the disclosure of documents held by a crypto firm based in the UK. Furthermore, if a foreign crypto exchange has an established 'business relationship' with a customer based in the UK, the Courts of England and Wales[298] will have jurisdiction over the issue. Following *R v Grossman*,[299] English courts appear to voluntarily restrict their jurisdiction within territorial limits, expect in exceptional circumstances, and will leave matters outside those territorial limits to courts of the other relevant jurisdiction.[300] In *Grossman*, an application was made against an

[294] ibid.

[295] MLRs 2017, Regulation 4.

[296] For instance, sending out generic marketing materials to a wide audience of potential clients will not be considered as creating a 'business relationship' with a client, as outlined in Regulation 4 of MLRs 2017; thus, do not need to undertake CDD.

[297] For instance, sales and trading (cryptoasset exchange providers) or relationship management (custodian wallet providers).

[298] Here, the "Courts of England and Wales" will now be referred to as "English courts" or "UK courts".

[299] [1981] 73 Cr App R 302.

[300] MacKinnon v Donaldson Lufkin & Jenrette Securities [1986] Ch 482.

international financial institution to provide documents in relation to an account held by its Isle of Man branch. The Court of Appeal refused the application, on the basis that [1] the Isle of Man branch was subject to Manx law, and more importantly, the Isle of Man branch was a separate entity from its London headquarter; and [2] any such order should be made by the Isle of Man Courts of Justice, otherwise this would create jurisdictional conflict. In addition, a foreign crypto exchange may object to the FCA exercising its jurisdiction to regulate their conduct if, in doing do, the regulator would be exceeding the proper territorial limits of the UK's jurisdiction. Accordingly, the FCA will not have the authority to mandate an international crypto exchange to produce documents in relation to an account based outside the territorial limits of the UK.

However, in *Mahme Trust Reg and others v Lloyds TSB Bank Plc*,[301] *Grossman* was distinguished. For instance, as per the above, an international crypto exchange can refuse to provide the FCA information in relation to accounts held abroad. However, in *Mahme*, claimants brought an action against an UK international financial institution and its Geneva branch. As a result, jurisdiction was established on the grounds that, Geneva recognised and enforced the 2007 Lugano convention, Recast Brussels Regulation[302] and the European Convention on the enforcement of English judgments. Whilst in *Grossman,* the branch in question was based in Isle of Man and not a member to the convention on the enforcement of foreign judgments. More importantly, in *Grossman,* the UK financial institution was not a party to the underlying action; whilst in *Mahme,* the claimants brought an action against both entitles. Nonetheless, the decision in *Mahnme* is significant since it widened the FCA's jurisdiction to include related offshore businesses. For instance, on 25 August 202, the FCA issued a supervisory notice to Binance Markets Limited, a UK subsidiary of the wider Binance Group, based in the Cayman Islands.[303] In short, the FCA issued a notice banning Binance Markets Limited from carrying out regulated activities in the UK because it refused to provide

[301] [2004] EWHC 1931 (Ch).

[302] Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

[303] FCA, "First Supervisory notice to Binance Markets Limited" (FCA, 25 June 2021) <https://www.fca.org.uk/publication/supervisory-notices/first-supervisory-notice-binance-markets-limited.pdf> accessed 28 August 2021.

information about the wider Binance Group, [304] thus in breach of section 165(1) of FSMA.[305] It is viewed that the FCA will continue leverage its powers over UK crypto firms to incentivise, and in turn, enforce the disclosure of off-shore related business.

International Level

The FATF and the EU uses the term 'virtual currency' and 'virtual asset' in the AMLD5. Here, the EU's AML framework sets out the main provisions designed to prevent crypto money laundering and terrorist financing. The AMLD5 essentially implements the FATF recommendations in order to mitigate the global risk of crypto money laundering. The AMLD5 amends the AMLD4 to capture virtual currencies. Subsequently, the Sixth Money Laundering Directive ("AMLD6")[306] harmonises the taxonomy as well as the definition of the primary money laundering offences and sanctions in relation to crypto transaction across the EU, through the revised 2021 Eurocrime Directive on the freezing and confiscation of assets deriving from the proceeds of crime.[307] As per the AMLD5, 'virtual currencies' includes all categories of cryptoassets. Similar to the UK Jurisdictional Taskforce, EU groups cryptoassets as: exchanges tokens, security tokens and utility tokens. Conversely, the AMLD5 defines virtual currencies as:

> "*a digital representation of value that is not issued guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency, and does not possess a legal status of currency or money, but is accepted by natural or legal persons, as a means of exchange, and which can be transferred, stored and traded electronically*" (AMLD5, Article 1(2)d).

[304] ibid.

[305] FSMA, s 165(2) requiring the production of information the FCA. In addition, there may be criminal liability in relation to a s165(2) breach, as per s 177 of the FSMA.

[306] EU 2018/1673

[307] HM Treasury advise that EU law would continue to have effect in the UK until the end of the transition period, until the 31st of December 2020. However, this may mean, the UK may not transpose the AMLD6 AML framework. In addition, it is viewed that the UK will not transpose the Eurocrime Directive, since the consultation to revise the Eurocrime Directive on the freezing and confiscation of instrumentalities and proceeds of crime is open until 27 September 2021. From this, it can be inferred that the Eurocrime Directive will not applicable to the UK, post Brexit.

The AMLD5 definition captures a wide range of cryptoassets. Accordingly, the EU observes that cryptoassets can be used for "*for other different purposes and find broader applications such as a means of exchange, investment purposes, store-of-value products or uses in online casinos*".[308] In short, the EU's AML/CFT framework goes beyond the FATF recommendations;[309] as evidence through the creation of the Eurocrime Directive. Here, confiscation requests submitted by other Member States must be given equal priority to domestic request. The revised Eurocrime Directive also contains provisions designed to improve both the investigation of crypto money laundering offences and the co-operation of Member States. Alternatively, the FATF is an international inter-governmental body that sets out the international AML/CFT standards in order to mitigate crypto money laundering. The FATF defines cryptoassets as: "*a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes*".[310] It is viewed, that the FATF sets out to create a tech-neutral definition, whilst not differentiating cryptoassets from virtual currencies.

As a summary, the MLR captures businesses most at risk of crypto money laundering, such as cryptoasset exchanges and custodian wallet providers.[311] Nonetheless, the MLR only captures exchanges and/or custodian wallet providers acting 'in the course of business carried on in the UK'.[312] On one hand, Regulation 9 of the MLR, provides that, it is irrelevant where the customer is located.[313] On the other hand, Regulation 9(3) asserts the importance of 'where' the business is located. As a result, the company's registered address determines the jurisdiction

[308] European Parliament, 'Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion' (TAX3 Committee, July 2018) <https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf> accessed 28 August 2021.

[309] European Commission, 'Communication from the Commission on an Action Plan for a comprehensive Union policy on prevent money laundering and terrorist financing' (Brussels, 7 May 2020) <https://ec.europa.eu/finance/docs/law/200507-anti-money-laundering-terrorism-financing-action-plan_en.pdf> accessed 28 August 2021.

[310] Financial Action Task Force, "Glossary of the FATF Recommendations' (FATF, 2020) <https://www.fatf-gafi.org/glossary/u-z/#:~:text=A%20virtual%20asset%20is%20a,for%20payment%20or%20investment%20purposes> accessed 28 August 2021.

[311] MLRs 2017, Regulation 8(2)-(3)

[312] MLRs 2017, Regulation 8(1).

[313] MLRs 2017, Regulation 9(5)(b).

as well as enforcement rules. In order words, 'carrying on business in the UK' is set on the location of the company's registered office. Nonetheless, Regulation 15 carves out small firms operating in the UK "on an occasional or very limited basis".[314] Here, the crypto firm's annual turnover must not exceed GBP 100,000.[315]

Nonetheless, determining whether an international crypto firm is captured by the MLR, is not straightforward. For instance, if the parent company is an US entity, which buys and sells cryptoassets from established counterparties (henceforth provides liquidity). However, the parent company does not have an office in the UK; and nonetheless, the parent company is "carrying on business in the UK" through its UK subsidiary, acting as an agent on its behalf.[316] In principle, the US parent company would be considered a 'cryptoasset exchange provider' on the premise that it facilitates the exchange of crypto to fiat in the UK. In practice, the MLR, would deem the parent company as a separate foreign entity, based on the premise that its registered office is in the US.[317] Subsequently, since the UK subsidiary is effectively a booking agent, the guidance provides that '…*it is not intended to capture a firm that only provides a forum where buyers and sellers can post their bids and offers, such as a bulletin board where the availability of the assets are merely made known and the parties trade at an outside venue either through individual wallets or other wallets not hosted by the forum or a connected firm*". Following the JMLSG guidance, both the US and UK entities would not be captured by the MLR. As a result, the JMLSG guidance should be revised since it fails to capture international crypto firms.

More importantly, the FATF seems to suggest that a company that facilitates the exchange of crypto to fiat, through buying and selling, should be caught under AML legislation.[318] However, the FCA asserts that a crypto firm must have a place of business in the

[314] MLRs 2017, Regulation 15(2).

[315] MLRs 2017, Regulation 15(2).

[316] For instance, a UK trading desk which books trades for an offshore entity.

[317] Consultation review JMLSG: Part 22 Cryptoasset exchange and custodian wallet providers, 1.11: "The definition is broad, providing for exchanging as well as "arranging or making arrangements with a view to the exchange." This may include activities relating to a dedicated peer-to-peer platform. However, it is not intended to capture a firm that only provides a forum where buyers and sellers can post their bids and offers, such as a bulletin board where the availability of the assets are merely made known and the parties trade at an outside venue either through individual wallets or other wallets not hosted by the forum or a connected firm".

[318] FATF, *Virtual Currencies Key Definitions and Potential AML/CFT Risk* (FATF report, June 2014) <https://www.fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 28 August 2021.

UK; thus, the buying and selling of cryptoassets 'by way of business' to its own entity (it is effectively a liquidity provider to justify the position) is unlikely to be in scope.[319] A broad reading of the JMLSG guidance seems to be counterintuitive, and as a result, may be a regulatory "loop-hole", if and when, an international crypto exchange does not want to go through the hassle of registration. Nonetheless, the UK is at a critical juncture in developing its regulatory approach in relation to cryptoassets and has a valuable opportunity to position the UK at the forefront of innovation. In short, cryptoassets, by their nature and technology, require regulatory coherence with other international jurisdictions to ensure cross-border interoperability, legal clarity as well as certainty.

[319] Consultation review JMLSG: Part 22 Cryptoasset exchange and custodian wallet providers, 1.13: "In determining the perimeter of regulation, the FCA will have regard to the policy objectives of the legislation as well as the definition itself. The following activities may, for example require assessment on a case-by-case basis: The buying or selling of cryptoassets for one's own account by way of business in exchange for money or cryptoassets is unlikely to be in scope".

Chapter 3: Theories and the prevention of crypto money laundering

This chapter sets out the three pillars in relation to how the law can mitigate the risk associated with crypto money laundering, by exploring the following: [1] the validity of the risk-based approach within the context of cryptoassets; [2] the practicalities surrounding AML compliance within the crypto space; and [3] the importance of international cooperation as a means to reduce the risk of crypto money laundering. This chapter investigates the regulatory influences of the UK's AML framework and considered it from an agency theory perspective. It is submitted, that the FCA's assumption that the crypto sector is part of the state, and an arm of law enforcement is counterproductive and could provoke the community to develop new protocols that are more autonomous, and as a result, are harder to detect and enforce. In short, the agency problem is centred upon the crypto sector and the FCA; as such, this theory is used to understand the relationships between agents and principals. Here, the model submitted will focus on the dual agency role that a crypto firm (the Agent) must adhere and develop between supporting the needs of the client (Principal 1) and implementing the regulatory mandate of the FCA (Principal 2). In the ideal world, a crypto firm must represent the interest of the principals in all business transactions and is expected to represent the best interest of the principals without regards for self-interest. The underlining assumption of agency theory rest upon the notion that the principal is always right in its demands, thus the "agency problem" is ensuring that the crypto firm does not jeopardise its relationship with the FCA and/or with the client in its own pursuit for profit. However, in the crypto money laundering context, the traditional agency model discount: [1] the criminal tendencies of principal clients and [2] the inconvenient social policy demands of the government principal, this assertion will be further tested in this chapter.

The key fundamentals in relation to AML:

One of the growing areas of regulation and compliance for crypto firms has been AML and KYC. The increased focus on AML and KYC regulation and compliance reinforces the notion that another principal-agent relationship exists within the crypto money laundering context. Here, the principal is the FCA, and the agent is the crypto firm. It is submitted that the agency roles are in conflict with each other because the FCA is adding more overhead costs by mandating more administrative and compliance steps for each crypto transaction through KYC

checks and reporting suspicious transactions. In response, the MLR hopes to reduce this tension by advocating a risk-based approach that is proportionate and reasonable; and in turn, this provides crypto firms with "some" flexibility when implementing the regulatory mandate of the FCA. As of January 2020, the MLR was amended to transpose the EU's 5th Directive to include AML provisions designed to mitigate risk associated with crypto money laundering. The revised MLR will now capture some FSMA authorised firms as well as crypto exchange providers and custodian wallet providers. As a result of the AML rules as set in the MLR, crypto exchange providers and custodian wallet providers must design onboarding processes and implement KYC as well as compliance protocols.[320] The firm's internal compliance policies and procedures must implement controls to mitigate crypto money laundering risks,[321] coupled with a regular assessment of its internal AML/CTF/KYC protocols.[322] The key guidance for the MLR, is the JMLSG, an industry body that sets out what is expected from crypto firms in relation to the prevention of money laundering in the UK. It is important to note that, the guidance as suggested by the JMLSG is not legally binding and so compliance is not compulsory. However, the JMLSG is approved by the FCA, and as a result, provides an indication of what the FCA expects from crypto firms. The challenge when applying the current framework is that the agency roles are in conflict with each other. Here, the FCA is adding more administrative burdens on crypto firms through additional compliance checks, which can, as a result, cause the firm to lose money through delayed transactions and increased overhead costs.

A mandatory requirement to KYC

As of March 2022, crypto firms must adhere to AML laws; this mandate was implemented as a means to address the growing problem of crypto money laundering and to undermine the system used by criminals, namely placing revenues acquired from illicit activities into crypto accounts held in the UK and abroad, then converting the crypto back to clean fiat money. As a result, a FCA regulated firm must determine and verify the identity of a potential customer before establishing a business relationship (or, as soon as practicable afterwards, if the customer is deemed to be 'low' ML/TF risk). However, if the customer is

[320] SYSC 6.1.1R.
[321] SYSC 6.3.1R.
[322] SYSC 6.3.3r

deemed to be 'high' ML/CFT risk, the business must identify and verify the identity of the customer before establishing a business relationship. Here, enhanced DD must be conducted when the firm doubts the veracity and adequacy of the customer's documents. It is important to note that the extent of verification and customer due diligence will depends on the individual's ML/TF risk. As a result, firms must gather the information to assess whether the transactions are consistent with expectations on the purpose and for the intended nature of its business relationship. In other words, if KYC is incomplete, the firm must not engage in a business relationship with a potential client.

The key requirements for conducting CDD can be found in Regulations 27-28 of MLR and the JMLSG, pt. 1,5.1-5.3. As a summary, the CDD obligations arises when a firm establishes a business relationship or oversee an occasional crypto transaction over EUR15,000 on behalf of any person. It is important to note that, the level of CDD required varies significantly; nonetheless, the crypto firm must assess the purposes and the intended nature of the business relationship and from this point assign the customer a risk rating, for instance, low - "SDD" or high – "EDD". Simplified due diligence ("SDD") measures are essentially less onerous; whilst the EDD measures are more onerous, as further information must be obtained in order to determine the customer's ML/TF risk, as well as to uncover the purpose and intended nature of the customer's business relationship. In short, crypto-firm must implement a risk-based approach whilst taking into account a number of factors including the type of customer, nature of the business relationship and the product or transaction types. According to the MLR and the JMSG's guidance, it is a mandatory requirement to know and confirm the identity of the customer and the beneficial owner. A crypto firm must then decide whether to apply a simplified or enhanced due diligence assessment on the new customer. Here, simplified due diligence can be carried out for low-risk customers (i.e. UK and/or European Economic Area ("EEA") regulated firms), however, this can only be applied when the proposed business relationship or transactions are deemed to be low risk. Following Regulation 33 of the MLR, EDD is required for high-risk consumers, for instance, in circumstances where the customer is a politically exposed person. Whilst the requirements for EDD are set out in Regulation 33 and in the JMLSG, pt 1, and 5.5, here, a firm must conduct EDD when it suspects the customer is potentially 'high' in relation to ML/TF risks. However, in practice, the JMLSG guidance notes

that it will not be appropriate for every business relationship and transaction to know their customers equally well.

A customer's risk ratings

A firm's information demands must be proportionate to a customer's risk profile, and the firm must be able to justify their information request.[323] The requirements for high-risk customers, are listed in the JMLSG, pt 1, 5.5.9 in respect of which EDD measures must be applied. As a result, the checklist for EDD are as follows:

> [1] a high risk of money laundering or terrorist financing;
> [2] any business relation with a person located in a high risk third country (i.e. Venezuela, Russia, etc.);
> [3] a non-EEA credit or financial institution;
> [4] the customer or potential customer is a politically exposed persons, or a connection person is a politically exposed person; and/or
> [5] the customer has provided false or stolen identification or misleading documents.

In addition to the above, the JMLSG outlined circumstances where EDD should be applied, for instance, when the transaction is complex or unusually large. Subsequently, the JMLSG also notes further red flags, for instance when: a) the transaction has no apparent economic or legal purpose or b) there is an unusual pattern of transactions which by its nature pose a higher risk of money laundering and terrorist financing.

Overall, EDD requires additional information requests in relation to the customer, the beneficial owner, in order to determine the intended nature of the business relationship and source of funds. Following the guidance as per the JMLSG, pt 1, 5.5.11, crypto firms must conduct KYC, and obtain information in relation to the reason for the business; then onboarding must be approved. Once the client is onboarded, the compliance team must ensure the firm's ongoing monitoring requirements are met. As a result, the firm must exercise sufficient

[323] JMLSG, pt 1, 5.5.4.

oversight in relation to its compliance process since the firm remains liable for insufficient CDD. KYC/CDD requirements also includes an ongoing duty to monitor the costumer's transactions undertaken during the relationship. Alternatively, if a firm does not conduct CDD, the crypto firm runs the risk of enforcement action by the FCA.[324]

In addition, firms must determine the extent of its CDD measures based on a risk-sensitive basis; in short, the assessment is dependent on the customer profile, and the nature of business relationship.[325] In terms of a customer's risk rating, internal AML/KYC protocols must set out pre-defined "red flags" to assess and identified high-risk customers. For purposes of AML, a customer is deemed to be high-risk, when: [1] the customer is domiciled or engages in business in a country subject to international sanctions, or [2] the customer or connected persons are politically exposed persons, etc.[326] As a result, CDD is based on subjective assessments; thus, it is viewed that the risk-based approach provides wide discretion. In order words, whether a sufficient level of KYC/CDD has been conducted is subjective because the government's KYC guidance is based on subjective assessments. Therefore, the quality of the due diligence conducted is dependent on the employee. For instance, although there is usually guidance in relation to minimum KYC checks, but how an employee processes the information they find and how they use that information to consider what additional searches need to be conducted is hard to regulate. Therefore, the quality of CDD conducted is dependent on the firm's internal AML/KYC policies and training employees.

Ongoing AML/KYC compliance

Under the MLR and JMSLG guidance, once a customer has been verified, there is no obligation to re-verify the identity unless doubts arise as to the veracity of the information previously collated.[327] In practice, crypto firms are required to review its CDD files on an annual basis, with frequency of the review driven by a customer's risk profile. For instance, high risk, medium risk and low risk, corresponding to 1, 2, or 3 year review cycles. In addition, crypto firms cannot, however, simply undertake these periodic checks and ignore developments

[324] MLR 2017, Regulation 27(1).
[325] MRL 2017, Reg 28; JPMSG, pt. 1, 5.1.4 & 5.1.9.
[326] JPMSG, pt. 1, 5.4.
[327] MLRs, regulation 28(11)(b); JMSLG pt.1, 5.3.27.

during the 1, 2, or 3 year review period that may impact its assessment of AML risks. In addition to ongoing monitoring, a range of trigger events might prompt a firm to seek addition CDD, and as a result, must decide whether to report suspicious activity and/or offboard the client. Here, the triggering events:

> [1] an unusually significant transaction;
> [2] material change in the business relationship; or
> [3] significant change in customer documentation standards.[328]

However, given the nature of a permissionless and anonymous nature of some cryptoassets, and the readiness of Virtual Private Network ("VPN") technology, it is questionable whether a crypto firm can implement adequate AML/KYC controls in order to satisfy the FCA's regulatory mandate.[329] The underpinning issue that agency theory warns about is that agents have the tendency to work from a position of self-interest first, and as a result, in order for the crypto community and the FCA to work effectively there needs to be a system of mutual benefit. However, the current framework is based on a threatening relationship of adhering to AML compliance or face fines or revoked licenses. Following this model, the alleged benefit to the crypto firm is to avoid fines or revoked license by complying and losing money, or not complying and not being caught, or move its operations to another "crypto friendly" jurisdiction. In order words, as soon as the cost of regulation to the crypto sector becomes higher than the penalties deriving from non-compliance, regulation stop being a priority. As a result, inefficient and complex AML laws is not the long-term solution to addressing the money laundering problem since a firm can move its operations to another "crypto friendly' jurisdiction or create new crypto protocols that are more autonomous, and as a result, are harder to detect and enforce.

Thus, conventional AML rules may not be substitute for crypto firms since direct client contact may not be possible. For instance, Regulation 28 of the MLR, underlines that crypto firms must ensure a client's transactions are consistent with the firm's knowledge of the client's business, employment and risk profile. In practice, the scope and complexity of AML

[328] JMSLG pt.1, 5.7.10.
[329] MLSG pt 1, 5.7.3.

monitoring will depend on the firm's business activities. As an example, if a crypto firm provides exchange services or takes part in ICOs or offers settlement and custodial services, there will be an expectation that a robust AML/KYC controls are in place.[330]

Money Laundering Theories

The global money laundering risks could be enhanced, as cryptoassets creep into the mainstream. Naheem asserts that, crypto firms should not be used as an enforcement arm since this approach could proliferate the development of more complex money laundering schemes that may be harder to detect. [331] This sector explores the agency problem between crypto firms and the FCA. For instance, crypto firms must monitor transactions and report suspicious transactions to the FCA. As a result, crypto firms must undertake costly CDD, monitoring, compliance reporting because the FCA will enforce punitive measures and fines. However, Takáts notes an underlying issue in relation to this agency model, whereby harmful excessive reporting, dubbed as "crying wolf", can arise in this regulatory set-up.[332] For instance, if a crypto firm identifies all transactions as suspicious, then it fails to identify any one of them as suspicious. Thus, over-reporting can eliminate the information value of CDD/EDD reports. Nonetheless, excessive reporting tends to arise in correlation with excessively high fines which forces uncertain firms to excessively flag transactions as suspicious, on the side of caution, thus diluting the information value of CDD/EDD reports.

Notwithstanding the above, AML regulation is nonetheless a key part of the reporting and compliance requirement for crypto firms in the UK. However, the administrative as well as the resource implications of AML compliance have been consistently increasing, which proves to be a burden on the crypto sector and its clients because of time delays and increased administration costs. This section sets out the role and influence of AML compliance through a business decision-making model known as the agency theory. The agency model is used to understand the relationships between agents and principals. The principal and agent problem occurs when the interests of the principal and the agent come into conflict. Here, the model will

[330] JMLSG pt 1, 5.7.8.

[331] Mohammed Ahmad Naheem, "The Agency Dilemma in Anti-Money Laundering Regulation" (2020) 23 Journal of Money Laundering Control 1, 26

[332] Supra (n 62) Takáts.

focus on the dual agency role that a crypto firm must develop between supporting needs of the client (Principal 1) and implementing the FCA's regulatory mandate (Principal 2). The conflicting structure of this dual agency relationship is important to understand when examining whether the current AML framework can, in fact, manage the risks associated with cryptoassets. Agency theory was first introduced in relation to business management theories as a way to understand the influences that affect businesses and its decision-making model. Kathleen Eisenhardt underlines the notion that the agency model is a useful addition to organisational theory because it aims to deduce the organisational risk associated with regulatory outcomes as well as uncertainties in relation to the incentives contributing to management outcomes.[333] Whilst agency theory may not be appliable to all areas of management, especially in relation to the audit department.[334] Here, the application of the agent and principal model remains a core theory because it underlines the conflicting nature of the business decision-making process, namely, working for the client to achieve its bottom line.

Subsequently, the traditional focus of agency theory primary centred on the agent and the principal, whereby the business is contracted and incentivised to work on behalf of the client to ensure the best value and outcome for the client. According to Jensen and Meckling, an agency relationship is a contract in which the principal engages in a contractual relationship with the agent to manage their crypto portfolio or crypto-transaction on their behalf, thus delegating their decision-making authority to the agent.[335] Hence, the underlining assumption of this theoretical approach rests upon the notion that the client is always right and the agency problem is ensuring that the firm does not jeopardise the client's business in its own pursuit for profit.[336] Nonetheless, the aim of this relationship is to maximise the utility of the principal as well as the agent. Thus, the contention of this doctrine is conceived in the context of a simple relationship between two individuals, one principal and one agent. In this ideal situation, the agency problem is more evident, as the presumption is that the agent will not act in the best

[333] Kathleen Eisenhardt, 'Agency Theory: An Assessment and Review' (1989) 14 The Academy of Management Review 1, 57.

[334] Getie Dessaiegn Mihret, "How can we explain internal auditing? The inadequacy of agency theory and a labour process alternative" (2014) 25 Critical Perspectives on Accounting 8, 771.

[335] Michael Jenson and William Meckling, "Theory of the firm: Managerial behaviour, agency costs and ownership structure" (1976) 3 Journal of Financial Economics 4, 305.

[336] Supra (n 333) Naheem.

interest of the principal. However, the challenge when applying this theoretical framework to a crypto firm's activities is that it does not consider the nature of a client's criminal tendencies.[337] It is submitted that this theory may be too narrow because it discounts a client's criminal tendencies. Here, this restrictive assumption of agency theory disregards the notion that diverse actors in various situation may behave differently. For instance, as crypto laws become stricter and a FCA regulated firm will no longer be able to supply its services as readily, the criminal client will access other services that are more willing to turn a blind eye. One of the options available to criminals looking to avoid AML detection is to move their illicit transactions to DeFi platforms, thus out of formal centralised exchanges completely and into decentralised crypto service providers. The development of DeFi has generally been a known side effect of trying to control the crypto community. It is submitted that as the cost of regulation becomes too high for crypto firms to deal with, programmers will be rewarded more lucratively for developing new protocols that are harder to detect and falls outside the current regulatory framework. DeFi transactions avoids the use of a centralised exchange, thus ensuring the transaction is anonymous and more difficult to trace. For this reason, it is not in the best interest of the FCA, to see crypto transactions being moved to DeFi platforms, since all DeFi products are automated through DApp protocols (no humans involved), and thus avoiding any form of regulatory oversight.

Agency theory can best be understood as maximizing behaviour on the part of all individuals. However, this theoretical approach does not incorporate the other responsibilities that the firm may have, such as the FCA and its AML requirements, which might equally impact on the business and its stakeholders. In order words, corporate profits made at the expense of all other interests is not conductive to AML mandates.[338] Henceforth, the extension of the traditional assumptions may allow for a more balanced assessment of agency relationships, not only between two actors but also in the context of the business and the regulator. Here, an increased focus on AML and CFT regulation has meant that another principal-agent relationship exists. It is submitted that, the system of crypto-transactions involves a number of stakeholders,

[337] John Parkinson, *Corporate power and responsibility: Issues in the theory of company law* (1st edn, Oxford University Press) 41-42.

[338] Peter Wright, Ananda Mukherji and Mark Kroll, "A reexamination of agency theory assumptions: extensions and extrapolations" (2001) 30 Journal of Behavioural and Experimental Economics 5, 413.

such as the crypto-firm, the client and the regulator. In this agency model, the principal is the FCA who oversee AML regulations by enforcing AML rules to make crypto transactions more transparent, and in turn, to control money laundering. In other words, the FCA utilises the services of a crypto-firm's internal compliance measures to perform its function of AML at national as well as international levels. The fundamental assumption here is that all actors within the crypto sector evaluate and assess their decisions rationally whilst considering all available current sources. Here the decision making process breaks down and determines the values and costs of each transaction in accordance with the present value of return through the scope of strategic behaviours. However, the insurmountable flaw in relation to the traditional agency perspective is the notion of bounded rationality, as outlined by Simon.[339] In support of this assumption, David Campbell reiterates the inevitable human flaw of bounded rationality, whereby humans never have the 'prefect' or 'complete' information; and as a result, agency theory contains elements that will never be resolved.[340]

Origins of Agency Theory

During the 1960s, economists and legal scholars explored the risk sharing problem as one that arise when counterparts have different attitudes towards risk.[341] Hence, agency theory was developed as a means to examine the ubiquitous agency relationships, in which the principal delegates work to the agent, who then performs that work.[342] Traditionally, this theory is concerned with resolving two essential paradigms that can occur in agency relationships. Firstly, this theory examines the agency problem that arises when the goals or desires of the agent and principal conflict because it is difficult or expensive for the principal to verify what the agent is actually implementing. The premise rest upon the notion that the principal cannot verify that the agent has in fact implemented the agreed instructions appropriately. Secondly, this theory uncovers the problem of risk sharing that arises when the agent and principal have different attitudes in relation to risk allocation. As a result, the problem here is that the principal and the agent may prefer different actions due to different risk preferences.

[339] James March, "Bounded rationality, ambiguity, and the engineering of choice" (1978) 9 The Bell Journal of Economics 2, 590.

[340] David Campbell, 'The roles of monitoring and morality in company law: A criticism of the direction of present regulation' (1997) 7 Australian Journal of Corporate Law 343.

[341] ibid.

[342] Supra (n 337) Jenson and Meckling.

The unit of analysis pertains to the contract governing the relationship between the agent and the principal. Hence, the focus of this theory rest upon the contract and developing the most efficient provisions governing the agent-principal relationship. Here, agency theory is focused on creating the most efficient contract based on the aforementioned assumptions on people (namely, bonded rationality, self-interest, and risk aversion), and the goal conflict between participants and imperfect information. As a result, agency theory centre upon rigid assumptions, and more specifically, whether behaviour-oriented contracts (for instance, salaries, bonuses, governance structures, etc) are more efficient than outcome-oriented contracts (for instance, stock options, employee shares, etc).[343] In short, the overarching premise of agency theory is to mirror the basic agency structure of an agent and a principal who are engaged in cooperative behaviours, whilst having different goals as well as attitudes towards risk.[344]

Agency theory is essentially a behaviour-oriented research focused on determining the optional contract, namely the behaviour versus outcome between the agent and the principal. As a result, agency theory revolves around the concept of cooperative relations developed through a network of economic exchanges. Here, the principal grants authority to the agent to act on his or her behalf, and the welfare of the principal becomes affected by the decisions of the agent.[345] The ethos of this theory is that the welfare of the principal may not be maximised because the principal as well as the agent tend to have a perceived goal divergence, thus creating a differing predisposition toward risk.[346] In this vein, the principal is viewed to be risk neutral to their preference in relation to an agent's actions, since the principal can diversify their investments across multiple firms.[347] By contrast, agents are perceived to be risk averse since the agent's employment and income are intrinsically tied to the profitability of the firm.[348] Here, agents are assumed to be risk averse in decisions pertaining to the firm in order to lower risk to

[343] Supra (n 337) Jenson and Meckling.

[344] Supra (n 337) Jenson and Meckling.

[345] Supra (n 329).

[346] Peter Wright, Mark Kroll, Bevalee Pray and Augustine Lado, "Strategic orientations, competitive advantage, and business performance" (1995) 33 Journal of Business Research 1, 143.

[347] Robert Wiseman and Luis Gomez-Mehia, "A Behavioural Agency Model of Managerial Risk Taking" (1997) 23 The Academy of Management Review 1, 133.

[348] ibid.

personal wealth. Effectively, the focus of agency theory is to develop a contract that minimises the costs associated with an agency relationship.

In Stephen Ross's work, "The Economic Theory of Agency: The Principal Problem", an agency-based utilitarianism is a normative ideal that prescribe actions that maximise the principal-agent relationship.[349] Here, the classical utilitarianism ideals was coined by John Stuart Mill in his book, "Utilitarianism" to provide support for the connection between justice and utility, and as a result, happiness maximise the overall good of all participants.[350] In support of this assertion, Bentham underlined that humans all, implicitly or explicitly, consent to utilitarianism because the principle of utility is the foundation of all actions.[351] Here, the utilitarian calculation aims to improve the utility of society, by punishing and rewarding according to actions that appears to invoke the greatest happiness for the greatest number of people. Following this assertion, the main purpose of AML regulation is to discourage crime and to promote the overall good of society. However, following Jeremy Bentham's view, regulators should only punish when the principle of utility warrants the punishment.[352] Here, he underlined that we should not invoke punishment via regulation when doing is deemed to be groundless and it does not deter the undesired action; nor where the regulation is ineffective and does not prevent the undesired action; nor where the regulation is deemed to be unprofitable or too expensive to achieve the desired result, in the cheapest manner.[353] In other words, Jeremy Bentham underlined that the value of regulation and punishment should follow the principle of utility, as such "[t]he value of the punishment must not be less in any case than what is sufficient to outweigh that of the profit of the offence".[354]

[349] Stephen Ross, "The Economic Theory of Agency: The Principal Problem" (1973) 63 The American Economic Review 2, 135.

[350] John Stuart Mill, *Utilitarianism and the 1868 Speech on Capital Punishment* (2nd edn, Hackett Publishing Company Inc 2001) 3.

[351] University of California Press, "3 Justifications of Practice: Utilitarian and Retributive" (UC Press E-Books Collection, 2021) <https://publishing.cdlib.org/ucpressebooks/view?docId=ft4q2nb3dn&chunk.id=d0e2447&toc.depth=100&toc.id=d0e2430&brand=ucpress> accessed 28 August 2021.

[352] ibid.

[353] ibid.

[354] ibid.

Following the above assertion, the government should not regulate areas found to be ineffective nor unprofitable nor too expensive. Here, by narrowly focusing on the two-tier principal-agent relationships, coupled with the aforementioned set of assumptions, the contribution of this theory is that it provides logical predictions in relation to how each rational actor will act in each agency relationship. Whilst the agency structure is conceived in the context of a single principal and agent, in order to capture the complexity and demands of a crypto firm, this research submits a two-tier principal-agent model. Here, the main premise of this doctrine revolves around the notion that economic relations should be examined from the deliberate behaviours of individuals. Thus, the agent and the principal can best be understood as utility maximisers. As a result, agency researchers have focused on identifying scenarios in which the agent and the principal are likely to have conflicting goals and then proscribing a provision and/or the governance mechanism that may limit the agent's self-serving behaviour.[355]

Adolf Berle and Gardiner Means, asserts that the agents should not have any responsibility other than to its principal, and more importantly, must produce maximum profits for the principal.[356] In short, the traditional role of agency theory derives from the method in which the supplier of finance assures a return on their investment via shareholder maximisation.[357] The Berle and Mean's model have been particularly influential on the governance of modern corporations, which focused exclusively on the agent-principal relationship between the shareholders and managers of large public corporations. As a result, the agency problems as outlined in the Berle and Mean's model may not be applicable to a crypto firm.

From a theoretical perspective, agency theorists have been most concerned with describing the control mechanisms that solve the agency problem. For instance, Jensen and Meckling studied the ownership structures of companies and endorsed shareholder value maximisation by aligning the agent's interests with the principal.[358] As a result, the traditional

[355] ibid.

[356] Adolf Berle and Gardiner Means, *The Modern Corporation and Private Property* (1st edn, Macmillian 1932) 114.

[357] Supra (n 337) Jenson and Meckling.

[358] Supra (n 337) Jenson and Meckling.

propositions are two-fold: The first proposition, the principal-agent relationship is to be governed by a contract that coaligns the preferences of the agent with those of the principal. Ideally, the rewards for both depends on the same action, and in turn, encourages the agent to behave in the interest of the principal.[359] For instance, increasing the equity ownership of managers decreases the agent's opportunism.[360] The second proposition is the premise of open information. Here, when the principal has open access to information to verify the agent's behaviour, the agent is more likely to behave in the interest of the principal.[361] For instance, Eugene Fama and Michael Jensen underlines that a principal's access to managerial information can also control an agent's behaviour.[362]

However, the traditional agency model has been criticised for being too narrow, thus not reflecting the realities of crypto money laundering. Nonetheless, the focus of the agent-principal literature is derived upon determining the optional contract, behaviour versus outcome, between the agent and the principal.[363]As a result, the third proposition rest upon the notion that the agent and principal have different goals and the principal cannot decipher as to whether the agent has behaved appropriately due to its innate moral hazards.[364] Moral hazards is described as a lack of effort on the part of the agent when dealing on behalf of the principal. The concept here is that when the agent has unobservable behaviours, the principal has two options. One is to discover the agent's moral hazards by investing in information systems such as reporting procedures and surveillance tools. It is argued that such investments will reveal the agent's moral hazards to the principal. Second is to create a contract that promotes desired behaviours and preferred outcomes that seeks to align the agent's preferences with those of the principal, by transferring the risk to the agent. However, as uncertainty increases, it becomes more expensive to shift the risk.

[359] Supra (n 337) Jenson and Meckling.

[360] ibid.

[361] Eugene Fama and Michael Jensen, "Separation of Ownership and Control" (1983) 26 Journal of Law and Economics 2 <https://www.jstor.org/stable/725104?seq=1> accessed 28 August 2021.

[362] ibid.

[363] Supra (n 335) Eisenhardt.

[364] ibid.

As a result, agency theory studies the goal conflict inherently present when counterparts with differing preferences are engaged in a cooperative effort. However, Charles Perrow have denounced agency theory for being too narrow.[365] Nonetheless, these assertions may be extreme, thus it is submitted that agency theory must be expanded to cover more contingencies to address the realities of money laundering within the crypto space. As a result, this thesis submits two recommendations: One is to apply the agency structure within the context of crypto money laundering. Whilst examining the agent-principal relationship, we must understand the scope and complexity of money laundering scheme, namely, criminal actors operate complex money laundering operations at different regions. In addition, crypto money laundering usually involves a chain of transactions and carried out through a sophisticated and complex process. Notwithstanding this fact, agency theory is still relevant and will contribute to an overall framework in which these various forms of self-interest, leading to a better understanding of when such behaviours will be prevalent and when such agency structures will be effective.

The second area is to understand agency relationships beyond the pure behaviour and outcome framework, as described by traditional theorists such Jenson and Meckling.[366] Traditional theorist focused on topics such as goal orientation, obligation and reciprocation, moral hazards, risks and self-interest. As a result, traditional theorists are focused on a single reward, whist neglecting circumstances in which multiple rewards are present. For example, a crypto employee can be compensated through multiple rewards avenues, such as through its transaction income, promotions, and bonuses, when approving or turning a blind eye to suspicious transaction. Aa a result, Kathleen Eisenhardt notes that although agency theory is important, it is also viewed to be controversial.[367] Eisenhardt criticised agency theory for being too narrow because it focused on the contract formation between the principal and agent. As a result, two opposing positions are presented. On the one hand, Jensen and Meckling argues that agency theory provides a powerful foundation to organisational behaviour research.[368] On the other hand, scholars such as Charles Perrow, contend that agency theorists confine the scope too narrowly, coupled with restrictive assumptions which predominately focuses on the contract

[365] Charles Perrow, *Complex Organisations: A critical essay* (3rd edn, Random House 1986).
[366] Supra (n 337) Jenson and Meckling.
[367] Supra (n 335) Eisenhardt.
[368] Supra (n 337) Jenson and Meckling.

between a principal and an agent; and is thus dangerous.[369] It is viewed that a more valid perspective lies in the middle. The intent of this chapter is to show that agency theorists can provide a unique perspective in relation to the study of crypto money laundering by extending this paradigm to allow for a more balanced assessment of agency relationships.

Traditional Agency Perspective

Traditional agency theorists underline a number of explicit assumptions pertaining to the behaviour of the agent. Here, opportunism is perceived as self-interest seeking tendencies, such as to mislead, disguise or cheat. It is viewed that in spite of incentives structure and monitoring, it is anticipated that opportunism will prevail. As a result, traditional agency theorists asserts that the contractual approach can align the behaviours of the agent to the principal.[370] Thus, Jensen and Meckling devoted most of their research studying the employment contracts,[371] as a means to design the most effective contractual provision to incentivise the agent towards desired outcomes,[372] since the sole duty of the agent is to maximise the principal's wealth.[373] The logic follows that, because principals, unlike other stakeholders such as taxpayers, HMRC, FATF, etc., have a right to the firm's profits as they are the "owners" of the firm, they have the greatest incentive to increase the value of the business.[374] Henceforth, the logic presumes that in pursuit of shareholder value maximisation, the crypto-firm's other stakeholders will benefit as well – increasing the firm's "net-wealth". It is argued that shareholder value maximisation allows the firm to expand and hire more employees whilst allocating more resources to other stakeholders; and as a result, everyone is better off. Proponents argue that negative externalities, such as harms to society are not reasons to depart from shareholder wealth maximisation. Here, Ian Lee contends that by considering the negative externalities, the agent would in turn reduce the overall "net-wealth" of the firm, because it requires the agent to balance the interests of stakeholders against the principal's

[369] Supra (n 367) Perrow.

[370] Supra (n 337) Jenson and Meckling.

[371] Supra (n 337) Jenson and Meckling.

[372] ibid.

[373] Milton Friedman, "The social responsibility of business is to increase its profits" (*The New York Times Magazine*, 13 September 1970) <http://www.colorado.edu/studentgroups/libertarians/issues/friedman-soc-resp-business.html> accessed 28 August 2021.

[374] ibid.

interest to maximise corporate profits.[375] It is reasoned that a departure from shareholder value maximisation will increase agency costs, and as a result, diminish the aggregated welfare of society.[376]

Moreover, traditional theorists assume agents are risk averse; and thud expect agents to exhibit risk averse behaviours in its decision-making process. Thus, Jensen and Meckling contend that any deviations from this assumption are abnormalities, and in turn, risky behaviours such as approving suspicious transactions are viewed as special case scenarios.[377] Here, the traditional paradigm outlined a set of negative assumptions in relation to the agent whilst not factoring in the potential illicit behaviours of the principal, such as money laundering and terrorist financing. Thus, when faced with distortion on the maximisation of expected utility, traditional theorists do not account the non-risk averse preferences of the agents nor the potential deviant behaviours of the principal. In short, traditional theorists have outlined a rigid set of negative assumptions in relation to the agent whilst discounting the illicit incentives of the principal.

In summary, the traditional paradigm has a set of assumptions used to design performance criteria on which agents are evaluated and remunerated in accordance to a set of preferred behaviours codified within their employment contract.[378] Eugene Fama and Michael Jensen, argues that contracts outline the internal rules of the game that specify the rights and obligation of the agent, whilst implementing performance as well as remuneration structures used to incentivise the agent towards desired outcomes.[379] It is viewed that the employment contract structure combined with surveillance technology and external legal constraints can drive the maximisation of utility within agent-principal relationships. However, as mentioned above, any deviations from normative expectations, such as risk seeking and money laundering, are viewed as abnormalities, which are discounted in the traditional agency paradigm.

[375] Ian Lee, "Efficiency and ethics in the debate about shareholder primacy" (2006) 2 Delaware Journal of Corporate Law 31, 538.

[376] ibid.

[377] ibid.

[378] Supra (n 363) Fama and Jensen

[379] ibid.

The Management Agency Perspective

Both the agency traditional and management perspectives, the underlining assumption is that agents will inevitably use the firm's resources to enrich themselves at the cost of the principal. As mentioned previously, the traditional agency paradigm underlines the agent's autonomy as well as freedoms which invariably dampers the utility between the agent and principal. Here, the management perspective underlines the notion that the conduct of actors in society should be viewed through the lens of societal outcomes, through the key influence attributed to social and psychological determinants of individual actors.[380] In support of this premise, Anthony Giddens, argues in his book "*Central Problems in Social Theory*", that noneconomic predispositions of individual actors must be considered within the agency analysis, namely elements that drive the utility, in conjunction with the social and psychological attributes of individual actors.[381] Giddens gives considerable exploration in relation to the power of reflexivity and control to the agent.[382] It is viewed that the agent is able to monitor, rationalise and motivate their own actions in relation to unacknowledged conditions of an action and the unintended consequences of their actions.[383] As a consequence, in the management agency perspective, the agent's autonomy in relation to their decision making process is not viewed negativity.

Subsequently, in the management paradigm, theorists adopts concepts from the stakeholder theory of the firm,[384] whereby the obligations as well as the interests of the agent are, in law and in fact, aligned with the rights and interests of its shareholders.[385] Thus, Parkinson, contends that even if the principal's interests were the most efficient means to increase aggregate social welfare, "unconstrained profit maximisation" is nonetheless, not "conducive to the public interest".[386] It is submitted that, corporate profits made at the expense

[380] Anthony Giddens, Central Problems in Social Theory: Action, Structure, and Contradiction (First published 1979, University of California Press 1983).

[381] ibid.

[382] ibid.

[383] ibid.

[384] Merrick Dodd, "For whom are corporate managers trustee" (1932) 45 Harvard Law Review 7, 1146.

[385] Amy YT Chen, *Corporate Governance: Shareholder Value and the Pursuit of Short-Termism* (LLM Dissertation, Lancaster University, 2013).

[386] John Edward Parkinson, *Corporate power and responsibility: Issues in the theory of Company Law* (1st edn, Oxford University Press, 1992) 41.

of all other interest, i.e. not preventing a client's criminal and/or deviant tendencies, may in fact reduce the aggregate social welfare due to its failure to account other competing and/or regulatory interests. It can therefore be inferred that the traditional agency perspective can be criticised for its narrow focus on profit maximisation whilst disregarding ethical considerations, such as money laundering. In short, the management paradigm suggests that agency issues may be more complex than profit maximisation, and to examine the agency model, from a very restricted set of assumptions is not conducive to the public interest. It is submitted that the traditional agency perspective may be an inaccurate view of interpersonal relationships between the principal and the agent

Overall, the cornerstone of agency theory focuses on the relationship between an individual principal and the agent; however, a strict adherence to these rules will lead to suboptimal outcomes. For instance, the assumption that agents are risk averseness must be relaxed and re-examined. From a behavioural perspective, individual agents may display different attitudes towards risk. In support of this assertion, Kahneman and Tversky, observed agents to be risk averse in satisfactory circumstances and risk prone in unsatisfactory situations.[387] Thus, depending on the situation and an individual's response are framed in relation to gains versus loses, the latter promotes risk taking.[388] In the context of a crypto firm, losing a client influences the company's bottom line, which could potentially promote risk taking behaviours. Thus, depending on the situation, some agents in certain circumstances may not be risk averse, and may, in fact, exhibit risk taking behaviours, such as approving suspicious transactions in order to improve the company's bottom line. Henceforth, it can be inferred that the concept of risk is underdeveloped in the traditional agency paradigm since it assumes agents are risk averse.[389]

[387] Daniel Kahneman and Amos Tversky, "Prospect Theory: An Analysis of Decision under Risk" (1979) 47 The Econometrica Society 2.

[388] ibid.

[389] Supra (n 337) Jenson and Meckling.

The agency theory and crypto firms

It is viewed that, principals with criminal tendencies will avoid risk averse agents in favour of risk prone agents because, under these circumstances, risk prone agents can satisfy the principal's criminal objectives. In this context, the examination of the relationship between the principal and the agent must be viewed through a more dynamic framework whilst relaxing ridge assumptions. Here, the assumption of utility maximisation at the firm level in relation to the agent and principal relationship must also be re-examined. The implications of this assertation rest upon the notion that the larger the firm, the higher the potential agency costs; this generalisation essentially states individuals are utility maximisers, and as a result, a larger collection of individuals, the larger are the total agency costs.[390] Such contentions may in fact produce adverse outcomes; it is submitted that, situations involving cooperative effort of others in order to carry out tasks, the team as a whole, must absorb all potential risks as well as any negative externalities conducted by a rogue employee. Thus, as the number of employees rises, the shirking of agency costs will essentially reduce the overall net agency cost. In order words, the larger the team, the team as a whole can, in turn, hold rogue individuals accountable. Here, the team must absorb the risk as well as any negative externalities conducted by a rogue employee. For instance, institutional investors, as well as retail investors, are more confident in cryptoassets now that the world's largest crypto exchange, Coinbase, is a public traded company on the Nasdaq.[391] Following Coinbase's Initial Public Offering, the total crypto market cap has risen 45% to over USD $2 trillion.[392] Community members on the infamous Reddit "ask me anything" AMA, Brian Armstrong compares Coinbase to Amazon, and concludes that this crypto exchange is "*like Amazon in the early days*".[393]

[390] Supra (n 337) Jenson and Meckling.

[391] Izabella Kaminska, "Coinbase Listing is a lament for some bitcoin believers: Purists believe the platform has forsaken crypto's true principles" (The Financial Times, 18 April 2021) <https://www.ft.com/content/ba47468b-ddb8-4740-af63-d5629ca8364e> accessed 28 August 2021.

[392] Billy Bambrough, "Radical New Bitcoin Price Model Reveals When Shock Bitcoin Rally Could Peak" (Forbes, 13 April 2021) <https://www.forbes.com/sites/billybambrough/2021/04/13/new-radical-bitcoin-price-model-reveals-when-the-shock-bitcoin-rally-could-peak/?sh=53d853cd914c> accessed 28 August 2021.

[393] Martin Young, "Coinbase's Reddit AMA: It's like Amazon in the early days" (Cointelegraph, 24 March 2021) <https://cointelegraph.com/news/coinbase-s-reddit-ama-it-s-like-amazon-in-the-early-days> accessed 28 August 2021.

Thus as the number of employees within a crypto firm rises, the potential for shrinking increases because it becomes progressively more complex, reinforced by more checks and balances, coupled with enhanced compliance measures to monitor individual employees. On the other hand, traditional agency theorists asserts that agency cost rises in any situation involving cooperative effort, and as the firm increases in size, the more potential for increased agency costs.[394] However, it is submitted that, teams are contractually formed and as the number of employees increases within a crypto firm, the potential for shrinking also rises since each team member is confronted with same negative externalities since any output, are made possible by a mutual team effort. In this context, a crypto firm must be viewed as a team whose members act from self-interest, but their careers depend on the survival of the team.[395] Following the management paradigm, as the number of team members increases, the potential for shrinking rises because the output benefit and negative are divided amongst the team.

In addition, the team, is also member to a set of horizontally related teams who are in competition with other related teams within the organisation. For instance, the sales team versus the compliance team, will have competing goals and self-interests that compliments one another. On the one hand, the sales team want to efficiently close transactions. On the other hand, the compliance team wants to ensure each transaction is AML and KYC compliant. In this context, members of each team must recognise that their employment depends on the long-term viability of the team as well as a firm's other related teams. In Tom Tyler's book, "*Why People Obey the Law*", it is contended that if agents believe that internal AML compliance rules are legitimate, employees generally feel that they have a strong obligation to obey internal AML/KYC protocols.[396] The main premise of this book is that firms should make rules and internal protocols worthy of respect amongst its employees.[397] It is submitted that, agents generally feel that they have a strong obligation to obey internal protocols as well as compliance rules. Here, employment training about the firm's ethical standards should be conducted in a

[394] Supra (n 337) Jenson and Meckling.

[395] Eugene Fama, "Agency problems and the theory of the firm" (1980) 88 Journal of Political Economy 288, 289.

[396] Tom R Tyler, *Why people obey the law* (1st edn, Princeton University Press 2021).

[397] ibid.

supportive environment, in order to ensure AML/KYC compliance.[398] However, traditional agency theorists overemphasise the threat of detection and punishment, which asserts that agents are rational maximisers of self-interest, thus only responsive to personal costs and benefits of their choices, whilst indifferent to the moral legitimacy of their actions.[399]

Although, discipline is necessary, an overemphasis on the potential punishment can be counterproductive. For instance, agents may rebel against internal controls that stress punishment, and imposed without community involvement. For instance, introducing AML/KYC compliance rules observed by a tier 1 investment banks, such as JP Morgan, and in turn, demanding crypto firms to be just a compliant, may be counterproductive. Nonetheless, penalties for the infringement of legitimate AML/KYC compliance requirements, are seen as fair and appropriate. However, an overemphasis on the potential punishment can be superfluous and even counterproductive because firms can just migrate to a more crypto friendly jurisdiction, such as Zug, Switzerland's Crypto Valley.[400] In this context, an aggrieved crypto firm can also operate their business underground via the DeepDotWeb, where unindexed dark web users can access a number of illicit marketplaces.[401] Here, dark web users can move crypto through a web of shell companies and different marketplaces in order to launder illicit funds.[402] In short, an aggrieved crypto-firm can rebel against draconian AML rules especially, if the AML requirements are designed and imposed without the community's involvement; or if the FCA's AML standards are too unrealistic for the crypto sector. One example of this impact can be seen in the recent mandate for crypto firms to meet the FCA's AML requirements which increases the overall costs; and as a consequence, many crypto firms were forced to withdraw from the market. What is not know is how many of these small crypto firms have decided to

[398] Lynn Paine, "Managing for Organisational Integrity" (Harvard Business Review, April 1994) <https://hbr.org/1994/03/managing-for-organizational-integrity> accessed 28 August 2021.

[399] Alexandre Padilla, "Can agency theory justify the regulation of insider trading" (2002) 5 The Quarterly Journal of Austrian Economics 38.

[400] Tanzeel Akhtar, 'Switzerland's 'Crypto Valley' has started accepting Bitcoin, Ether for Tax payments' (*Coindesk*, 18 February 2021) <https://www.coindesk.com/switzerlands-crypto-valley-has-started-accepting-bitcoin-ether-for-tax-payments> accessed 28 August 2021.

[401] Danny Nelson, "DeepDotWeb Operator Pleads guilty to laundering $8.4M in Bitcoin Kickbacks' (*Coindesk*, 31 March 2021) <https://www.coindesk.com/deepdotweb-operator-pleads-guilty-to-laundering-8-4m-in-bitcoin-kickbacks> accessed 28 August 2021.

[402] ibid.

continue operating in another jurisdiction or use more illicit protocols to supply their services to clients that falls outside the current regulatory framework.

Integrity Governance

Unfortunately, even the best regulations, legal compliance is unlikely to unleash much enthusiasm or commitment. However, if it is framed in a manner that it is good for business, a strategy based on customer integrity, which may in turn, hold the crypto sector to a more robust moral standard. Whilst legal compliance is rooted in avoiding FCA sanctions, organisational integrity is based on the concept of self-governance, similar to the UK Corporate Governance Code.[403] The UK Corporate Governance Code, adopts a principal-based approach, whereby the Code provides general guidelines of best practice, for instance the FCA listing rules requires public listed company[404] to publicise how they have complied with the Code and describe in the company's annual report how their obligations, as per section 172 of the Companies Act 2006, have been considered in their day-to-day operations.[405] The Code is a guide to a number of key good governance concepts such as: [1] accountability, [2] transparency, [3] probity and [4] sustainable success of a company over the long term.[406]

Thus, from the perspective of integrity governance, organisational integrity is based on self-governance. As a result, the agent must promote the firm's guiding values, in order to create a space that supports ethically sound behaviours, this will install a sense of shared responsibility amongst community members.[407] Thereafter, the need to obey good governance principles will be viewed as a positive control, rather than an unwelcome constraint imposed by the management. In order words, this integrity strategy is driven by a notion of ethics, thus the values created by the community will essentially design the decision-making process of the firm and its employees. Here, the onus will be on the firm and its employees to design the appropriate internal AML/KYC controls, that is 'fit for purpose', which also serves as a

[403] Financial Reporting Council, *The UK Corporate Governance Code* (FRC, July 2018).

[404] Financial Services and Markets Act 2000.

[405] Companies Act 2006, section 172.

[406] Financial Reporting Council, *The UK Corporate Governance Code* (FRC, April 2016).

[407] Financial Reporting Council, "Corporate Governance and Stewardship" (FRC, 2021) <https://www.frc.org.uk/directors/corporate-governance-and-stewardship> accessed 28 August 2021.

unifying force across different lines of business and teams within an organisation. As a result, it can be argued that the integrity model also has many structural features common to the rule-based approach.

It is contended that, the aforementioned integrity approach is essentially broader and more demanding than the rule-based approach. It is therefore submitted that, the integrity approach is broader because it seeks to enable responsible conduct, the onus will be on the employees to design the code of conduct that is suitable, in order to establish a foundation that helps employees define what their firm is and what it stands for. It is thus deeper because it cuts to the ethos and defines what the crypto firm is, and in turn, provides guiding values and patterns of thought and action. More importantly, the integrity approach requires managers as well as employees at all levels and across different lines of business to be involved in the process. For instance, in the rule-based approach, the company's ethos is simple, to conform with externally imposed standards, whilst preventing criminal misconduct amongst its employees. By contrast, the driving characteristic of the integrity model is essentially self-governance and creating distinctive standards that are 'fit for purpose', whilst enabling responsible patterns of thought and action. Here, the behaviour assumption is that agents are guided by material self-interest as well as through the value and ideals of their peers. Conversely, the rule-based approach hinges on the notion that agents are autonomous beings purely guided by material self-interest.

The rule-based approach is usually externally driven; thus, the company's values and standards are based on the criminal law as well as regulatory standards developed by the government. Whilst in the integrity model, the company's values and standards are developed by its employees through a self-governance approach that incorporates the company values, aspirations, and social obligations. Here, training is implemented through company values and standards which are taught and communicated to staff, through an integrated system supported internally to assess the values and performance of its employees. For instance, at Linklaters, the firm's ethos is entrenched in its ethical code the notion of Team Linklaters – "One Team", which instil a sense of shared accountability amongst its employees.[408] Similarly, at Amazon,

[408] Linklaters, "Our Ethical Code: Delivering legal certainty in a changing world" (*Linklaters*, 2021) <https://www.linklaters.com/en/about-us/our-firm-at-a-glance/our-ethical-code> accessed 28 August 2021.

employees are encouraged to learn and be curious whilst insisting on the highest standards.[409] As a result, modern companies are focused on core values that reflect basic social obligations, such as, inclusion, honesty and obedience to the law.

For instance, Aristotle introduced the concept of courage as the underlying commitment to virtue.[410] Thus companies seeking to implement ethical behaviours must design a code of conduct that specify the appropriate and desired behaviours, such as honesty and fair dealing. The assumption is that personal commitment and the appropriate code of conduct will lead to the desired outcomes. For instance, at Linklaters, the firm promotes the principle of Team Linklaters, as being: "*united, inclusive and collaborative, delivering the whole firm to clients*".[411] Here, the firm is focused on a specific outcome whilst creating a decision-making model that reflect the firm's values, such as striving for excellence, embracing diversity, leadership and integrity.[412] In order words, the integrity model encourages exemplary conduct as a means to prevent misconduct amongst its employees. As a result, employees are more motivated to transmit positive interactions to others within an organisation.[413]

Accordingly, the traditional agency paradigm believes agency costs rises as the size of the organisation increases.[414] However, it is submitted that, agents in multilateral relationships can act cooperatively to each other in their exchanges,[415] and as a result, the agency costs does not rise as the organisation expands and may actually culminate optimal outcomes. For instance, in this context, crypto investors fear exit scams.[416] For instance, the volume of trade in Turkish

[409] Amazon, "Leadership Principles" (Amazon, 2021) <https://www.amazon.jobs/en/principles> accessed 28 August 2021.

[410] Denise Vigani, 'Aristotle's Account of Courage' (2017) 34 History of Philosophy Quarterly 4, 313.

[411] Linklaters, "Purpose and values: Delivering legal certainty in a changing world" (*Linklaters*, 2021) <https://www.linklaters.com/en/about-us/our-firm-at-a-glance/purpose-and-values> accessed 28 August 2021.

[412] ibid.

[413] David Willer, Pamela Emanuelson, Michael Lovaglia and Brent Simpson, "Elementary Theory: 25 Years of Expanding Scope and Increasing Precision" (*Research Gate*, August 2014) <https://www.researchgate.net/publication/285985192_Elementary_Theory_25_Years_of_Expanding_Scope_and_Increasing_Precision> accessed 28 August 2021.

[414] Supra (n 363) Fama and Jensen.

[415] Supra (n 340) Wright.

[416] Marie Huillet, "Turkish police detained 62 over $2B Thodex crypto exchange fraud" (*CoinTelegraph*, 23 April 2021) <https://cointelegraph.com/news/turkish-police-detain-62-over-alleged-2b-thodex-crypto-exchange-fraud> accessed 25 April 2021.

crypto markets is over USD1.2 billion; by contrast, a founder can create a crypto exchange with just USD 6,000 in capital.[417] Thodex, one of Turkey's largest crypto exchanges with 391,000 active users fear that their life savings have been lost as the exchange goes offline and its CEO, Faruk Fatih Ozer, [418] fled the country, allegedly taking over $2 billion of investors' funds with him.[419] Turkish prosecutors have issued arrest warrants for 75 Thodex employees.[420] Due to the prevalence of exit scam, crypto investors are more willing to invest through regulated crypto exchanges, who are AML/KYC compliant. As evidenced through, Coinbase's IPO on the Nasdaq, which exceed all expectations,[421] thus indicating investors support for regulated exchanges.[422]

Coinbase has over 43million KYC verified users with over USD 90 billion assets currently on the platform, coupled with an impressive USD 456 billion lifetime trading volume.[423] In Coinbase's SEC Form S-1 under the Securities Act 1933, Brian Armstrong, CEO of Coinbase asserts that: "[*t]rust is critical when it comes to storing money. From the early*

---

[417] Taylan Bilgic and Firat Kozok, " Turkish Crypto Exchange goes bust as Founder Flees Country" (*Yahoo News*, 22 April 2012) <https://uk.news.yahoo.com/turks-suspect-big-crypto-losses-095946382.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAADv5uAiepR4gUj876WKhbUugIEAJ5x1Trfzpi9m6iQ0ZOlBleyeV69pdqAFtEjEMzFyR2GNYp7t-E7W7navTsvDDU46P_YuA9G0losUgRwYDf0pqnNiVPdzU9eLQSyNxyPZt91Txg_tArC_uuY1c0tpCGv1nX-dGWi_G15nNdQLx> accessed 25 April 2021.

[418] Taylan Bilgic and Firat Kozok, "Turks Suspect Big Crypto Losses as Exchange CEO goes Missing" (Bloomberg News, 22 April 2021)< https://www.bloomberg.com/news/articles/2021-04-22/turks-suspect-massive-crypto-losses-as-exchange-ceo-goes-missing?utm_content=business&utm_medium=social&cmpid=socialflow-facebook-business&utm_campaign=socialflow-organic&utm_source=facebook&fbclid=IwAR1Pwnub0VfdvinqeOtm5JjY9vbwT3M8VUpmkP14-Cl0mA56Gat4gGhYf3g> accessed 25 April 2021.

[419] Kevin Helms, "Turkish Crypto Exchange Exit Scam: CEO Flees Country, 62 People Detained, Users cannot access $2 Billion of Funds" (Bitcoin.com, 24 April 2021) <https://news.bitcoin.com/turkish-crypto-exchange-exit-scam-ceo-flees-country-people-detained-users-cannot-access-2-billion-funds/> accessed 25 April 2021.

[420] JP Buntinx, "Prosecutors issue arrest warrants for 75 Thordex employees, 62 arrested so far" (CryptoMode, 23 April 2021) <https://cryptomode.com/prosecutors-issue-arrest-warrants-for-75-thodex-employees-62-arrested-so-far/> accessed 25 April 2021.

[421] Bitcoin Magazine, "Coincase IPO exceeds all expectations, showing more promise for Bitcoin" (*Nasdaq*, 19 April 2021) <https://www.nasdaq.com/articles/coinbase-ipo-exceeds-all-expectations-showing-more-promise-for-bitcoin-2021-04-19> accessed 25 April 2021.

[422] Ryan Browne, "Turkish crypto exchange boss goes missing, reportedly taking $2 billion of investors' funds with him" (*CNBC*, 23 April 2021) <https://www.cnbc.com/2021/04/23/bitcoin-btc-ceo-of-turkish-cryptocurrency-exchange-thodex-missing.html> accessed 25 April 2021.

[423] Coinbase, "SEC Form S-1 Regulation Statement under the Securities Act 1933: Coinbase Global Inc" (*SEC.Gov*, 25 February 2021) <https://www.sec.gov/Archives/edgar/data/1679788/000162828021003168/coinbaseglobalincs-1.htm> accessed 25 April 2021.

days, we decided to focus on compliance, reaching out to regulators proactively to be an educational resource, and pursuing licenses even before they were needed".[424] Coinbase is a crypto powerhouse, generating over USD 3.4 billion in revenue, largely from transaction fees derived from volume-based trades by retail as well as institutional investors.[425] Here, the exchange supports over 90 different types of cryptoassets. Over a span of 8 years, Coinbase's overall market capitalisation of cryptoassets grew 1564%, from less than USD 500 million to USD 782 billion – representing a compound annual growth rate of over 150%.[426] Over the same period, retail investors grew from 13,000 to 43million and institutional investors from 1,000 to 7,000.[427] As a result, Coinbase grew, from 199 employees to 1,249 employees,[428] and underlines that a "*failure to scale and preserve our company culture with growth could harm our future success, including our ability to retain and recruit personnel and to effectively focus on and purpose our corporate objectives*".[429]

Thus, to control agency costs, there is a need to verify the conduct of agents as well as principals, thus vigilant monitoring is required since there still remains "some divergence between the agent's decision and those decision which would maximise the welfare of the principal".[430] In this context, the remaining divergence represents the residual loss. Here, the assumption underlines the notion that agents are self-interested and are competitively related to each other, thus as the organisation expands, the firm's agency cost also increases.[431] As a result, it is argued that as the firm increases in size, it will have an adverse effect on the overall efficiency of the organisation.[432] By contrast, it is asserted that, agents are not universally competitive. For instance, the self-interests of an agent may be cooperative interrelated, especially when the organisation encourages exemplary conduct amongst its employees. Under these circumstances, employment contracts, internal systems of control and monitoring, as well as bonding initiatives, could minimise, and thus, negate the residual loss.

[424] ibid.
[425] ibid.
[426] ibid.
[427] ibid.
[428] ibid.
[429] ibid.
[430] Supra (n 363) Fama and Jensen.
[431] ibid.
[432] ibid.

It is evident from the process of money laundering that understanding the conflicting nature of a firm's dual agency role will determine whether the FCA has influence over the way client accounts are managed. Here, the principal is the FCA, and the agent is the crypto firm. As a result, crypto firms must balance two agency roles, the FCA and the client. However, these agency roles are in conflict: on the one hand, the client expects quick onboarding and seamless transactions, on the other hand, the FCA expect firms to implement its additional AML/KYC measures, which slows the onboarding process and delays client transactions. The question posed here is, how can a crypto firm facilitate its client's business whilst simultaneously overseeing the implementation of national as well as international AML efforts?

The cost of regulation

As previously stated, MLR was amended to transpose the EU's 5th Directive to include the unique AML risks posed by cryptoassets and to undermine the money laundering system used by drug cartels and terrorist networks. Here, it is important to note the negative externalities posed by crypto money laundering, namely, it causes economic, political, social as well as compliance loss to both the crypto firm and the FCA. However, will the agency role between the FCA and crypto firms work to the advantage of the regulator? Following traditional agency assumptions, agents tend to work from a position of self-interest, and in this vein, for a principal and agency relationship to work, there needs to be mutual benefit as well as gains to both parties. As noted above, in the client (principal) and agent relationship, this mutual benefit occurs in the facilitation services, coupled with the generation of profit. By contrast, in the FCA (principal) and agent relationship, how is this relationship mutually supportive to the crypto firm? Here, the relationship is based on a threatening relationship of adhering to AML rules or face the threat of prosecution, fines, or revoked licenses. The benefit to the crypto firm is to avoid prosecution either by complying and losing profits or not complying and not being caught. From these examples, it can be seen that the impact of AML regulation reaches far beyond managing the crypto firm. Thus, in addition to monitoring AML compliance, MLR can force crypto firms to close and lead smaller firms into providing their services in unregulated or foreign markets.

The FCA should not impede legitimate and innovative businesses from operating in the crypto space. Nonetheless, countries must work together to develop a coordinated international response to protect crypto investors as well as businesses from fraudulent conduct and money laundering schemes that threaten the integrity of the crypto market.[433] However, as mentioned above, once the agency paradigm is applied to AML regulation and compliance situations in the crypto space; it is argued that, as soon as the costs of regulation to the crypto sector becomes higher than penalties due to non-compliance, then the regulation is no longer efficient. For instance, although the FCA advocates for the use of a flexible and risk-based approach in relation to a firm's AML system, the challenge that crypto firms are faced with is having to develop its own AML/KYC systems that can manage the risk assessment process. It is submitted that these internal AML/KYC systems cost money and require a high level of expertise not readily available to crypto firms. All these factors add additional pressure to the already tense agency relationship that exist between crypto firms and the FCA. Here, Gregory Elliehausen, defines "cost of regulation" as the regulatory costs that are aligned and used to measure the efficiency and quality of regulations that may lead to the underestimation of costs due to inefficient regulatory choices.[434] Wim Marneffe and Lode Vereeck, argues that the cost of regulation must also consider the direct as well as indirect costs to crypto firms when designing an effective regulatory approach.[435]In short, regulatory costs must reflect the inherent loss of welfare, plus the negative impact on the business's bottom line. Hence, proportionality must be applied since administrative, monitoring and enforcement of the FCA's AML mandate tends to be substantial and labour intensive. Donato Masiandaro argues that money laundering is a multiplier of criminal financial activities since crypto money laundering allows the reinvestment of laundered funds thus the FCA's tolerance towards both the damages caused by money laundering and the cost of regulations determines the strictness of AML rules.[436] It is submitted that the FCA must examine the trade-offs between protecting the integrity of the

[433] Fraklin Edwards, Kathleen Hanley, Robert Litan and Roman Weil, "Crypto Asserts require better regulation: Statement of the financial Economists Roundtable on Crypto Assets (2019) 75 Financial Analysts Journal 2, 18.

[434] Gregory Elliehausen, "The cost of banking regulation: a review of the evidence" (IDEAS, 1998) <https://ideas.repec.org/p/fip/fedgss/171.html> accessed 29 August 2021.

[435] Wim Marneffe and Lode Vereeck, "The meaning of regulatory costs" (2011) 32 European Journal of Law and Economics 3.

[436] Donato Masiandaro, "Money Laundering: the Economics of Regulation" (1999) 7 European Journal of Law and Economics 3.

economic system and the crypto space by designing an effective AML regime that acknowledges the premise that regulation impairs the innovative efficiency of crypto due to regulation related costs. In order words, the FCA's tolerance towards both the damages caused by crypto money laundering and the costs of regulation determines the strictness of AML policy. However to increase the effectiveness of crypto AML regulation rests upon the FCA to rationalise the direct and indirect cost of regulation.

The application of agency theory shows that basic cost benefit analysis would provide that, as soon as the costs of regulation to the crypto space becomes higher than the penalties occurred from non-AML compliance, then the AML regulation stop being a priority. However, Christina Davilas warns that increasing AML regulations would not in the long term address the AML and CFT problems, as outlined in Chapters 1 and 2.[437] In short, increasing AML regulations also add to the administrative burden of crypto firms, coupled with the increased associated costs of hiring and training employees to adhere to the KYC and AML checks. It is viewed that this can cause extreme reactions from the crypto community, as evidenced through the creation of DApps and decentralised finance applications (this will be discussed in more detail in the subsequent chapters), are deemed as the most cost-effective response, although such reactions may not be the most useful in addressing the AML issues for both the FCA and the international community. Accordingly, decentralised finance applications ("DeFi") do not require a custodial relationship amongst its users nor its corresponding digital assets. Here, the relevant digital asset is sent directly to the address of a smart contract (the code is stored directly on the blockchain network). The cryptoasset will remain locked until a user or the relevant code unlocks and sends the asset to another address.[438] The scale of DeFi grew significantly; data provided by DeFi Pulse shows that the total value locked in DApps via smart contracts soared to over USD $50 billion.[439] Interestingly, when the 2019 FATF guidance was published, DeFi was barely on the radar. This rapid growth in cryptoasset activity through DeFi protocols and decentralised exchanges (such as Uniswap) without a readily identifiable intermediary (unlike Coinbase) adhering to AML/CFT/KYC compliance obligations has caught the FATF off guard.

[437] Christina Davilas, "AML compliance for foreign correspondent accounts: a primer on beneficial ownership requirements and other challenges" (2014) 15 Journal of Investment Compliance 1.

[438] ibid.

[439] Crypti, 'DeFi Grows as Total Value locked Tops $50 Billion" (Crypti, 9 April 2021) <https://crypti.io/defi-grows-as-total-value-locked-tops-50-billion> accessed 4 May 2021.

The critical question posed here for future research: is how will the FCA impose AML/CFT/KYC compliance measures on a decentralised crypto exchange without an identifiable human founder or corporate entity?

As pointed out in the previous section, the concept of risk assessment and risk management underlines the tension between the traditional rule-based approach and the integrity model. According to Pellegrina and Masciandaro, the rule-based approach in relation to AML/KYC compliance have "…in fact produced insufficient information to fight and prevent the money laundering phenomenon".[440] Here, the scholars have argued that there is a tipping point at which crypto-firms will decide that the regulatory burden is too high.[441] In general, the impact of rule-based AML/KYC policies on organised crime is viewed to be unsatisfactory.[442] As a result, the ongoing relationship between the FCA and crypto firms can affect the effectiveness of AML/KYC rules and enforcement. The aim of the FCA is to elicit a high level of outcomes in terms of AML/KYC controls from self-interested crypto firms (the agents) who own private information in relation to their principals (the client). This section will examine how the relationship between crypto firms and the FCA can affect the effectiveness of AML/KYC rules using the principal and agent framework, as discussed in the previous section.

The agency problem between crypto firms and regulators, surrounds the notion of incentive arising in a three-layer hierarchy that include regulators, crypto firms, and the clients. In this section, this research examines the principal-agent approach, both at a general level and in relation to specific circumstances relating to crypto firms. In short, it will be argued that the traditional rule-based or risk-based approach is ineffective in redressing organised crime and money laundering activities. As noted above, the MLR requires a risk-based approach to AML risks, however, without further guidance from the FCA, this can cause extreme response reactions that is deemed to be the most cost-effective response for the crypto firm. In this context, the most cost-effective response for a crypto firm, may not be the most efficient or useful in addressing AML/KYC issues. For instance, an extreme example in relation to the

[440] Lucia Pellegrina and Donato Masciandaro, "The Risk-Based Approach in the New European Ant-Money Laundering Legislation: A Law and Economics View" (2009) 5 Review of Law and Economics 2, 6.

[441] ibid.

[442] ibid.

increased regulatory pressure, such as managing clients' accounts from known terrorist and/or war zone countries.[443] Here, it is more convenient for the firm to close account and refuse to allow clients from a sanctioned country to open a crypto account because it can be considered too costly and burdensome on AML/KYC compliance.[444] Subsequently, the firm may not have the expertise to implement effective internal controls to deal with such clients and failing to implement adequate AML/KYC controls would result in FCA sanctions and hefty fines. Unfortunately, such blanket bans will move such clients to unregulated crypto exchanges and/or other criminal banking services on the dark web.

Nonetheless, the agency dilemma as noted by Naheem, rest upon the notion that "principal-led" profit underlines the needs of clients and the profit focus of a crypto firm, which causes significant tense.[445] Here, the principle-led profit mantra may cause crypto firms to deliberately avoid AML regulations and encourage low risk KYC compliance measures.[446] For instance, crypto clients may be encouraged to register with an off-shore subsidiary of the UK parent company in order to avoid AML and KYC compliance obligations. This may expose the UK to increased money laundering and/or terrorist financing risks. Nonetheless, as crypto regulations as well as AML compliance measures becomes stricter, regulated crypto firms may no longer supply their services to these clients; notwithstanding this fact, criminals will still access other services provided by other unregulated crypto firms willing to accommodate their needs. Here, the third agency relationship in money laundering: between the criminal and their launderer. In this context, money laundering schemes are usually noticeable via suspicious transactions; and as a result, crypto firms are required to cooperate in a conscientious manner, in order to fight organised crime and money laundering.

Crypto firms can implement AML protocols using either the rule-based approach or the risk-based approach. As noted in the previous section, the traditional rule-based approach,

[443] Lisa Bachelor, "HSBC accused of closing UK accounts held by Syrians" (*The Guardian*, 8 August 2014) <https://www.theguardian.com/money/2014/aug/08/hsbc-accused-closing-bank-accounts-syrians#:~:text=One%20HSBC%20customer%2C%20Majid%20Maghout,was%20swallowed%20by%20the%20ATM.> accessed 26 April 2021.

[444] Supra (n 333) Naheem.

[445] ibid.

[446] ibid.

regulatory cooperation is usually passive and static. Here, agents apply a set of rules in relation to each transaction, and if a transaction meets the condition as specified in the rule, then the transaction is flagged as suspicious. Unfortunately, as laundering schemes become more complex, transactions are usually disguised to avoid detection; thus, a more conscientious cooperation is required. Agents must be trained to detect suspicious transactions and work alongside regulators to create a more comprehensive approach. However, in the agency dilemma, as coined by Naheem, when the cost and pressure from the FCA becomes too much for the regulated crypto firm to deal with, unregulated crypto firms will be rewarded more lucratively for the risks they take, thus the money laundering phenomenon still resides.[447] It is submitted that, sophisticated criminals may understand, and can navigate the AML rules, which enables them to adjust their money laundering schemes to comply with the codified rules, and as a consequence, making suspicious transactions indistinguishable from regulator transactions. In this context, sophisticated criminals have a deep understanding of the detection risks, and as a result, take countermeasures to hide their financial activities and implements measures to distinguish suspicious transactions.[448]

Subsequently, in the risk-based approach, cooperation between the crypto firm and the FCA, aims to be more active and dynamic. Here, the firm must design its own internal AML framework that is suitable for their day-to-day business. In this context, crypto firms must adopt a risk management protocol used to identify and manage money laundering risks in a flexible and less predictable manner. Additionally, firms must also train their employees to use their intuition, knowledge as well as expertise to fight against money laundering risks. By contrast, in the rule-based approach the concept of 'suspicious' is usually very narrow and vague, whilst the risk-based model aims to be more flexible and less predictable, thus more difficult for criminals to navigate. It is asserted that, due to the evolution of technology, money laundering techniques has become more difficult to detect because sophisticated criminals have separated of the three components of money laundering, namely [1] placement; [2] layering and [3]

[447] Supra (n 333) Naheem.

[448] Financial Action Task Force, "Guidance on the Risk-Based Approach" (*FATF*, 2007) <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatfguidanceontherisk-basedapproachtocombatingmoneylaunderingandterroristfinancing-highlevelprinciplesandprocedures.html#:~:text=The%20Guidance%20on%20the%20Risk,was%20published%20in%20June%202007> accessed 26 April 2021.

integration.[449] For instance, as compare to traditional money launders, sophisticated criminals would offshore its transactions and create various accounts via regulated as well as unregulated crypto-exchanges in order to disguise or misrepresent the illicit transaction(s). As a result, detecting money laundering is not a straightforward process because transaction that may show irregularities may actually be a legitimate transaction. In this context, managing AML risks is becoming ever more challenging for crypto firms.

As demonstrated through this chapter, in order to implement effective AML protocols, the behaviours of at least three agents must be considered: [1] the FCA; [2] the crypto firm; and [3] the employee. Here, the FCA oversees the UK's AML regulation. Thereafter, the crypto firm is a private for-profit company and because of its business, it has private information over its clients. This valuable information is a useful asset in relation to the UK's national fight against money laundering, and in turn, can be used to implement an AML model that evaluates and assesses money laundering risks. However, the effectiveness of the relevant AML information depends on the efforts of an individual crypto firm, which is costly, and its implementation cannot be observed by the FCA. In addition, ongoing AML training is required in order to increase the effectiveness as well as the efficiency of the AML rules, whilst avoiding the FCA from obtaining private benefits from information in relation to their legitimate clients. Here, employees are essential because the must detect suspicious transactions as they are "difficult to recognise ex ante and to verify ex post".[450] In short, there are two potential costs a crypto firm must undertake: [1] the capital investment required to implement the internal AML framework; and [2] the diminished secrecy with respect to their clients.[451]

In conclusion, implementing an internal AML protocol is not straightforward, there may be several barriers for a crypto firm to overcome in order to implement an efficient as well as effective AML system. In this chapter, we have examined the traditional rule-based versus risk-based approaches, through a principal-agent methodology. It is submitted that, a multi-layered hierarchical organisation, can in turn, minimise the agency costs, through a cooperative, integrity model. Furthermore, excessive sanctions and/or fines would not necessarily provide

[449] Supra (n 340) Wright.
[450] ibid.
[451] ibid.

incentives for the crypto firm to improve its AML compliance. As demonstrated through the perspective of the 'tipping point' at which crypto firms will decide whether the regulatory burden is too high; and as a result, decide to not comply or refuse to deal with a particular client because the regulatory costs are too high. Finally, this theoretical framework as examined in this chapter can be useful as it extended in different ways. In short, the impact of rule-based AML/KYC policies on organised crime is viewed to be unsatisfactory.[452] It is submitted that the FCA must examine the trade-offs between protecting the integrity of the economic system and the crypto space by designing an effective AML regime that acknowledges the premise that regulation impairs the innovative efficiency of crypto firms due to regulation related costs. Agency theory shows that basic cost benefit analysis would provide that, as soon as the costs of regulation to the crypto space becomes higher than the penalties occurred from non-AML compliance, then the regulation stop being a priority. Thus, it is not apparent from an agency perspective where the advantage to the crypto firm lies in supporting the FCA as a principal. From the FCA perspective, it would appear that crypto firms are viewed as being a part of the government, and in turn, enforcing the law. This is a dangerous assumption since crypto firms are ultimately private companies that are for profit. Hence, agency theory enables researchers to map out the human response to managing increased regulatory pressure from the FCA. In crypto money laundering context, there are two sides working with AML regulation, [1] the crypto firm and the FCA both trying to manage accounts and ensuring money laundering is not occurring whilst [2] the criminals and programmers are trying to outsmart the current AML framework. As a result, agency theory explored the human response underpinning money laundering activity within the crypto sector This chapter considered a number of approaches and agency theory was used as the base theory because it identifies the core relationships between the crypto firm, the FCA and criminal clients. It is submitted that the agent is not working for the principal thus by increasing the regulatory threat towards crypto firms, this agency relationship could backfire on the FCA. Ultimately, the agent and the principal must be in a mutually agreeable relationship and both parties need to derive actual benefits from the contract. If these conditions are not met, increasing AML obligations would not in the long term address the money laundering problem; since it is hard to identify where the advantage for the crypto firm lies in supporting the FCA as a principal. As a result, this will incentives the agent

[452] ibid.

to completely sabotage the relationship and provoke extreme reactions from the crypto community. For instance, the development of DeFi has generally been a known side effect of trying to control the crypto community. Thus, as the cost of regulation becomes too high for crypto firms to deal with, programmers will be rewarded more lucratively for developing new protocols that are harder to detect, and in turn, fall outside the current regulatory framework. As a result, the rapid growth of DeFi protocols and decentralised exchanges (such as Uniswap) without a readily identifiable intermediary (unlike Coinbase) adhering to AML/CFT/KYC compliance obligations has caught the FCA off guard. Reactionary responses such as this are convenient and practical for crypto programmers, especially when a position is reached whereby adhering to the new crypto AML laws are considered to be too costly or too burdensome for the crypto sector. Unfortunately, reactionary responses such as this opens the door for criminal crypto services to operate because a decentralised protocol is now available.

Chapter 4: Criminal Proscription

This chapter will examine the crypto landscape concerning crypto money laundering and the UK's POCA. Each money laundering offence will be assessed through the crypto lens whilst outlining relevant scenarios for each money laundering offence. As a result, this chapter consists of three primary sections: [1] the concealing offence: section 327, the POCA, [2] the arranging offence: section 328, the POCA, and [3] the acquisition, use and possession offence: section 329, the POCA. It is important to note, the case law regarding the primary POCA offences and crypto money laundering is still developing. As a result, this Chapter offers originality in providing a thorough overview of the POCA offences from a crypto perspective. However, in the absence of a leading precedent establishing a consistent principled rule for crypto money laundering, it is difficult for crypto firms to understand the FCA guidelines and the relevant money laundering offences. For instance, in conventional cases, the court interprets aspects of the law that may be unclear and explains how the law is established in that particular case. Thus, the lack of established case law are factors that add further pressure to the already fragile agency relationship; since there has been little in the way of guidance to the crypto firms as to how they should implement this regulation. There is clearly a gap in the judicial interpretation of cryptoassets and crypto money laundering offences. The question from an academic perspective is: can established case law bridge the gap between the agent and principal divide?

The Financial Stability Institute of the Bank for International Settlements published a report in relation to crypto money laundering.[453] The report notes that one of the growing areas of regulation and compliance for crypto firms has been in AML and its only beginning to be implemented around the world, with only a few countries performing active surveillance.[454] The report asserts that much work remains concerning the impact and implementation of AML/CFT/KYC standards on crypto firms.[455] Nonetheless, the report notes that most jurisdictions have implemented or are in the process of implementing the FATF's

[453] Rodrigo Coelho, Jonathan Fishman and Denise Garcia Ocampo, *FSI Insights on policy implementation No 31: Supervising cryptoassets for anti-money laundering* (Financial Stability Institute, No 31, 2021).

[454] ibid.

[455] ibid.

recommendations in relation to the money cryptoassets and its service providers.[456] Thus, the question posed here depends on the outcome of national authorities' evaluation of cryptoassets and whether those risks are being captured by existing regulation or whether there is a gap in existing laws that need to be addressed.[457] It is asserted that "*for gaps in AML/CFT regulation, implementing standards, particularly those issued by the Financial Action Task Force, should provide a solid basis for effective AML/CFT compliance and guidance*". However, challenges remain when crypto instruments and operating models, such as DeFi,[458] do not conform to existing regulatory frameworks. On the one hand, centralised crypto exchanges, such as Coinbase and Binance,[459] its related activities would fall into the regulatory scope, and regulators can easily apply the basic principle of "*same business, same risks, same rules*".[460] These exchanges are essentially private companies that offer services to their clients to trade cryptoassets. The FCA suggests that the regulatory treatment of regulated crypto firms will be akin to those of financial institutions or e-money institutions; as a result, regulatory compliance measures must be adhered to, such as AML/KYC compliance. On the other hand, unregulated crypto platforms, such as Uniswap,[461] are an automated liquidity protocol used to exchange cryptoassets using smart contracts powered through the Ethereum platform.[462] Here, as compared to Coinbase, Uniswap is a publicly owned and self-sustainable protocol.[463] The founder is anonymous, and the users of the platform are anonymous. As a result, FCA cannot mandated AML/KYC compliance, since the platform is computerised through a self-sustained protocol, and transaction is done directly from the user's digital wallet.[464] In such cases, the regulatory identification of such a novel instrument and its operating model will not be as straightforward. As a result, Rold van Wegberg, Jan-Jaap Oerlemans and Oskar van Deventer

[456] ibid.

[457] ibid.

[458] For more information re DeFi see Chapter 6.

[459] Luke Conway, "Best Crypto Exchanges" (Investopedia, 9 April 2021) <https://www.investopedia.com/best-crypto-exchanges-507185> accessed 29 April 2021.

[460] ibid.

[461] Warner Vermaak, "Uniswap vs PancakeSwap", (CoinMarketCap, 5 March 2021) <https://coinmarketcap.com/alexandria/article/uniswap-vs-pancakeswap> accessed 30 April 2021.

[462] Uniswap, "Decentralised Trading Protocol: Guaranteed Liquidity for millions of users and hundreds of Ethereum applications" (Uniswap, 2021) <https://uniswap.org/> accessed 29 April 2021.

[463] Uniswap, "Introducing Uni" (Uniswap, 16 September 2020) <https://uniswap.org/blog/uni/> accessed 29 April 2021.

[464] Daniel Lesnick, "Crypto AM: Definitively DeFi's guide to using Uniswap" (CityAM, 26 September 2020) <https://www.cityam.com/crypto-am-definitively-defis-guide-to-using-uniswap/> accessed 29 April 2021.

argues that the technology used in crypto money laundering does not conform to existing regulatory definitions.[465] Thus the question from an academic perspective is: can established legal principles in relation to money laundering be applied in the crypto sector?[466]

This chapter considers the challenges and obstacles in enforcing the POCA offences in the crypto sector.[467] Parliament via the POCA, created a dual regulatory and AML system that tries to impose regulation on the crypto community to be part of the state and law enforcement[468] by overseeing AML compliance and reporting suspicious transactions to the FCA or the NCA. Notwithstanding the UK's AML position, the case law in relation to cryptoassets are still developing, and as a result, this research extends to the forefront of the legal discipline. As of June 2021, only five crypto firms have received the appropriate AML designation from the FCA to operate in the UK.[469] As a result, most crypto firms in the UK are not authorised by the FCA.[470] For instance, Binance, listed as the "*best and cheapest crypto exchange in the UK*",[471] was recently banned by the FCA from undertaking any regulated activities in the UK. Shortly after the ban, its UK consumers were frozen from their accounts and are unable to withdraw sterling.[472] The sentiment in the UK underlines the premise that cryptoassets are used by criminals for money laundering purposes. In this vein, the examples submitted within this chapter are original and are thus, used to conceptualise the existing AML framework within the crypto space. As seen throughout this thesis, the law regarding cryptoassets is still developing. Decisions, such as *AA v Persons Unknown*[473] and *Ion Science Ltd v Persons Unknown*,[474] are all critical *interim* decisions transforming the law within the crypto space. However, interim judgments are granted at an early stage in the legal proceeding

[465] Rold van Wegberg, Jan-Jaap Oerlemans and Oskar van Deventer, "Bitcoin money laundering: mix results? An explorative study on money laundering of cybercrime proceeds using bitcoin" (2018) 25 Journal of Financial Crime 2.

[466] ibid.

[467] POCA, s 327-328.

[468] For instance, the Norwich Pharmacal Orders or the Bankers Trust Orders, which requires the Crypto exchange to disclosure the correspondence, transactions as well as records in relation to accounts held by alleged criminals; in order to ascertain and prevent the disposal of criminal property.

[469] Supra (n 66) Oliver

[470] Supra (n 50) Russon.

[471] Supra (n 51) Michael.

[472] Supra (n 53) Samson.

[473] [2019] EWHC 3556 (Comm).

[474] (unreported), 21 December 2020 (Commercial Court).

thus not considered a leading judgment. Thus, the crypto community must await the final decision in the hope that the court will add to the understanding of the FCA's AML guidelines and interpret aspect of the law that may be unclear. It is viewed that the UK places great value on leading cases as a means to create consistent legal principles which can be applied to future cases. As a consequence, crypto firms experience more hurdles than conventional financial institutions because the law is not fully developed since leading judgments are usually derived from decisions issued by judges in previous cases. As a result, the crypto sector remains uninformed as to how the FCA's AML guidelines work; and in turn, this research aims add to the understanding of the guidelines and interpret aspect of the POCA offences that may be unclear.

Civil and criminal liability may be incurred by "relevant persons" for failure to comply with the requirements as imposed by MLR; however, section 37 of the Serious Crime Act 2015, amended section 338 of POCA, excludes civil liability for disclosures made in "good faith" by "relevant persons". This amendment protects crypto firms from civil liability in circumstances where the relevant firm had made an authorised disclosure following a suspicious transaction and is then required to restrict or freeze client accounts, whilst the NCA or the FCA decides whether to take further action. Here, "relevant persons", as amended by MLR, for the purposes of Regulation 8 of MLR 2017, includes crypto exchanges and crypto storage providers. As of December 2020, the AMLD4, AMLD5 will be transposed and governed by the Sanctions and Anti-Money Laundering Act 2018 ("SAMLA"). The HM Treasury has nonetheless advised that the same MLR regime will remain in place as it departs from the EU.[475] Notwithstanding this fact, the UK has been a member of the FATF since 1990, and as a result, the UK is expected to continue to follow the FATF's AML/CFT guidelines and recommendations.[476]

As a consequence, the MLR regime, as well as the FATF recommendations, will still be relevant post Brexit. The AMLD4, AMLD5 will form part of the UK's AML and CFT regime. The UK government transposed AMLD4, AMLD5, as well as the revised Wire Transfer Regulation (Regulation 2015/845) into UK law. This section aims to explore the primary money

[475] The Law Society, "Anti-money laundering after Brexit" (The Law Society, 1 April 2021) <https://www.lawsociety.org.uk/en/topics/brexit/anti-money-laundering-after-brexit> accessed 29 April 2021.
[476] ibid.

laundering offences under sections 327 to 329 of the POCA. More importantly, the offences committed by a crypto firm or its employees[477] when discovering a suspicious crypto transaction; and, after that failing to report the suspicious transaction to the FCA or the NCA. The UK's AML framework contains both civil and criminal enforcement powers. The question posed here is, how can we define money laundering within the crypto context? It is submitted that, *crypto-money laundering can be defined as the process by which the proceeds of crime are dealt with and transferred into the crypto space. Here, the illicit funds are funnelled through a web of shell companies and then placed in various crypto marketplaces to disguise their criminal origins. Generally, criminals tend to seek out crypto exchanges domiciled in countries with a low risk of detection due to weak or ineffective AML adherence. The end objective is to re-integrate the illicit funds back into the mainstream economy as a legitimate transaction*. At the present, crypto money laundering is a new phenomenon, thus the existing common law examples as presented in this chapter, underlines the primary POCA offences following traditional money laundering cases.

POCA: Money Laundering Offences

As noted previously, both natural persons and legal entities can commit money laundering in the UK. Thus, both natural persons and legal entities in the UK, could, in theory, commit offences under the POCA. For example, an employee assisting with a customer's transfer of illicit funds[478] or an employee failing to report a suspicious transaction to the FCA or NCA[479] – are all actionable offences under the POCA. Subsequently, there are three primary money laundering offences under the POCA. For both natural and legal persons in the UK, it is an offence to [1] conceal, disguise or transfer criminal property or remove criminal property from the UK [***the basic money laundering offence***].[480] For instance, a criminal may use crypto to conceal, disguise and move criminal property from one jurisdiction to another. [2] It is also an offence to enter or become involved in a money laundering arrangement. The alleged defendant must know or suspect the retention, use or control of criminal property [***the aiding***

[477] Both natural and legal persons can be prosecuted for money laundering in the UK; thus a corporate can be held criminally responsible under UK law.

[478] POCA, s 327-328.

[479] POCA, s 330-331.

[480] POCA, s 327.

and abetting offence].[481] Here, the crypto-firm or an employee may be liable under these circumstances when it is evidenced that they *knew or suspect* the crypto-account, or the transactions derived from proceeds of crime. Finally, [3] third the offence is known as the handing of stolen goods offence, here the alleged defendant acquires, uses, or is in possession of criminal property [**the possession offence**].[482]

Extraterritorial offences refer to the UK's jurisdiction over crimes committed overseas. The POCA will capture any criminal proceeds generated within the UK.[483] However, there is a presumption that the POCA offences created by Parliament did not intend to provide extraterritorial jurisdiction over unlawful conduct(s) committed abroad.[484] However, when a significant part of the underlying criminal conduct took place in the UK, and illicit conduct continues to deprive the victims of their property. There is no reasonable basis for withholding jurisdiction. In Michael Hirst's book "Jurisdiction and the Ambit of the Criminal Law", he underlines the complexity of international fraud and money laundering. Hirst submits that the POCA will be difficult to apply on a limited territorial basis.[485] According to Rudi Fortson QC, *R v Rogers* was a significant case regarding the Court's decision and confirming the extraterritorial reach of the POCA offences.[486] The Court in *Rogers* defined the breadth and limits concerning the extraterritorial reach and effect of the money laundering offences, as prescribed by the POCA.[487] Here, "criminal conduct" is defined in section 340(2) of the POCA, as conduct that constitutes an offence in any part of the UK, or would be considered as such, if it had occurred in the UK. In order words, the POCA considers the impact of the conduct on victims in the UK as a means to determine whether the relevant property is criminal property.[488] The main impetus surrounding the extraterritorial reach of the POCA underlines the notion that

[481] POCA, s 328.

[482] POCA, s 329.

[483] POCA, s 340(2)(a).

[484] Air India v Wiggins [1980] 2 All ER 593; Cox v Army Council [1963] AC 48.

[485]Michael Hirst, *Jurisdiction and the Ambit of the Criminal Law* (1st edn, Oxford University Press 2003).

[486] Rudi Fortson, "R v Rogers (Bradley David): Money laundering -jurisdiction – Proceeds of Crime 2002 s327(1)(c) Court of Appeal (Criminal Division): Treacy L.J. Lang J. and Judge Bevan QC: August 1, 2014; [2010] EWVA Crim 1680" (2014) 910 Criminal Law Review 12.

[487] Richard Card, Rupert Cross and Philip Asterley, *Card, Cross & Jones Criminal Law* (21st edn, Oxford University Press 2014) 10.

[488] William Blaire, *Banks and financial crime: the International law of tainted money* (2nd edn, Oxford University Press 2017).

as the crypto economy continues to grow, the risk of international money laundering increases simultaneously.[489]

Thus, any benefits deriving from a criminal conduct committed abroad, are thus deemed to be criminal property, and will be caught by the POCA.[490] Notwithstanding this fact, the Court inserted a crucial caveat to what is considered 'criminal property' and crimes committed abroad, it submits an element of *de minimis*[491] to the legislation. [492] Here: [1] the conduct must be considered a criminal offence in the host country; and [2] in addition the conduct must be unlawful in the UK and must be punishable by more than one year in prison.[493] The rationale behind the extraterritorial reach of the POCA was cemented in *R v Smith*[494] and *R v Rogers*.[495] The former underlines that there is no geographical limitation to sections 237 to 239 of the POCA. Nonetheless, the substantial underlying criminal activity must occur within the UK. The latter case reaffirmed this notion; the Court held that the money obtained by fraud in the UK did not cease to be criminal property even when the money was transferred aboard.[496] It was subsequently held that a "significant part of the criminality underlying the case" occurred in the UK. As a result, there was no reasonable basis for withholding jurisdiction, as it was unlikely to be an offence in which local Spanish authorities would have been interested. In order words, the Court found that Parliament intended for the three primary money laundering offences (sections 327-329) to have an extraterritorial effect, allowing foreign suspects to be prosecuted in the UK, even if their conduct occurred entirely outside the jurisdiction of the UK.[497]

The above decisions were essential in clarifying the extraterritorial effect of the POCA. As a result, it shows the Court's willingness to develop the case law to redress the international

[489] ibid.

[490] POCA, s 340(2)(b).

[491] The court inserted this crucial caveat as a means to control the floodgates as well as to prevent parties from bringing legal action where the impact of the breach is negligible or immaterial.

[492] R v Smith (Wallace Duncan) (No 4) [2004] Cr App R 17.

[493] R v Rogers (Bradley David) [2014] EWCA Crim 1680.

[494] R v Smith (Wallace Duncan) (No 4) [2004] Cr App R 17.

[495] R v Rogers (Bradley David) [2014] EWCA Crim 1680.

[496] ibid.

[497] ibid.

nature of money laundering. Nonetheless, the Court inserted a crucial caveat whereby a significant part of the underlying criminality must have occurred in the UK. As a result, it must have harmful consequences for members of the public in the UK.[498] For instance, in *R v Rogers,* the defendant[499] appealed against his conviction arguing the UK court had no jurisdiction to deal with the allegations against him since he lived and worked in Spain. *Rogers* claimed he had not committed any part of the offence regarding the fraudulent scheme that lured clients in the UK to pay advance fees for never performed services.[500] Here, the fraudsters based in the UK then transferred the victim's money to bank accounts in Spain held by *Rogers*. As a result, it was transpired that approximately GBP 5.7 million was obtained from the scheme.[501] In this vein, *Rogers* allowed GBP 715,000 to be transferred into his Spanish bank account; then, he permitted the other fraudsters to withdraw money from his account.[502] The following extradition from Spain, Rogers was convicted of converting criminal property and sentenced to two years and ten months' imprisonment.[503] Subsequently, *Rogers* appealed against his conviction arguing the Courts of England and Wales had no jurisdiction to deal with the allegations against him. The Court of Appeal acknowledged the established presumption that, in the absence of explicit words to the contrary,[504] it is implied that Parliament did not intend to make an offence extraterritorial. However, the Court of Appeal found that Parliament did, in fact, intend to make the POCA offences extraterritorial, thus triable and are within its jurisdiction.

More specifically, the Court of Appeal found that Parliament intended for sections 327-329 offences to have an extraterritorial effect due to the international provisions found in sections 2A, 340(2)(b), 340(9) and 340(11)(d), supports the primary money laundering offences. It was submitted that the illicit funds obtained by fraud in England became criminal

[498] POCA 2002, s 282A(1)

[499] The defendant was a UK citizen who resided in Spain – in this case, he allowed £715,000 of illicit funds to be paid into his Spanish bank account.

[500] ibid.

[501] ibid.

[502] ibid.

[503] POCA, s 327(1).

[504] Example of provisions with extra-territorial jurisdiction: Section 1 of the Aviation Security Act, Section 31 of the Criminal Justice Act 1948, Section 9 of the Offences Against the Persons Act 1861, Section 72 of the Sexual Offences Act 2003, etc.

property once the property reached the principal fraudster's bank account based in the UK. More importantly, the relevant property did not cease to be criminal property when it reached Rogers' bank account in Spain.[505] Effectively, *Rogers* had converted criminal property, as per section 327(1) of the POCA, by allowing his Spanish bank account to be used for receiving and withdrawing criminal property. As a result, the defendant's conduct in Spain was directly linked to the criminal conduct carried out in England and subsequently, through his conversion of the illegal property. In this vein, the Court of Appeal held that the POCA had no geographical limitation in relation to sections 327-329 offences, when a substantial measure of the criminal property or activity took place in the UK unless the local courts in the host jurisdiction must deal with the prohibited conduct as a means to uphold international comity.[506] Nonetheless, law enforcement should refrain from trialling foreign suspects, unless the criminal conduct directly or indirectly harms the UK.[507] Here, the Court of Appeal set out the principal rule on the POCA, whereby "*par excellence an offence which is no respecter of national boundaries. It would be surprising indeed if Parliament had not intended the Act to have extraterritorial effect*".[508] This assertion on the extraterritorial impact of the POCA and the enforcement of English orders abroad will be examined in Chapter 5.

Subsequently, section 2A underlines that it is a defence if the defendant based abroad knows or believes that the criminal conduct was lawful in the defendant's country when the offence occurred.[509] For instance, a crypto criminal based in EL Salvador may use a section 2A defence, alleging that Bitcoin is a legal tender in El Salvador. As a result, the suspicious transactions flagged by the NCA are not in violation of international AML and CTF standards.[510] In this vein, the updated government guidance concerning section 2A of POCA notes that non-conviction-based powers such as forfeiture, civil recovery as well as taxation should also be considered in relation to the alleged criminal conduct and the recovery of

[505] R. v Rogers (Bradley David) [2014] EWCA Crim 1680.

[506] ibid.

[507] ibid.

[508] ibid.

[509] POCA, s 2A.

[510] Rodrigo Campos, "El Salvador bitcoin move opens banks to money laundering, terrorism financing risks – Fintech" (Reuters, 25 June 2021) <https://www.reuters.com/technology/el-salvador-bitcoin-move-opens-banks-money-laundering-terrorism-financing-risks-2021-06-25/> accessed 28 July 2021.

criminal proceeds. Non-conviction based capabilities of the POCA[511] offers broad discretion to the relevant authorities, such as the NCA, the Serious Fraud Office, the FCA, and HMRC, to use as an alternative to criminal investigations as well as prosecution in circumstances where "*the only known criminality is overseas, and there is no extraterritorial jurisdiction to pursue a criminal case in the courts of England and Wales, Scotland or Northern Ireland*".[512] Here, asset recovery powers are seen as an appropriate alternative to criminal investigations,[513] where there is no identifiable suspect within the jurisdiction of the UK, or it is not realistically possible to extradite the suspect to the jurisdiction.[514] Subsequently, if and when the proceeds of crime have been identified but cannot be linked to an identifiable suspect, or it is not realistically possible to extradite the suspect to the UK, an asset recovery approach should be considered to achieve the objective under the POCA.[515] The purpose of the POCA is to deprive criminals from benefiting from their illicit gains. In conjunction with the deterrent effect of criminal sentences, asset recovery powers must be proportionate, and it is not meant to act as a fine nor further punishment.[516] In *R v Rizvi,*[517] the House of Lords underlines the three legitimate aims of the Government's asset recovery approach are: [1] to punish offenders; [2] to deter the commission of further AML/CFT offences; and [3] to reduce the profits circulating to fund additional money laundering or terrorist financing schemes.[518]

Section 340(2)(b) of the POCA defines criminal conduct as any prohibited act which is considered an offence in the UK ***as if it*** had occurred in the UK. As a result, the Court of Appeal, in Rogers,[519] found that Parliament did in fact intend for the POCA to have extraterritorial effect. In support of this notion, section 340(9) underlines that the FCA or the NCA established that the relevant property was criminal property, once deemed as criminal property regulators,

[511] For instance, Part 5 of POCA includes civil recovery, cash forfeiture, forfeiture of certain personal property and forfeiture of money. Part 6 underlines civil recover through taxation; finally, Part 8 provides for investigation powers in relation to asset recover via civil recovery.

[512] GOV.UK, "Guidance issued under section 2a of the Proceed of Crime Act 2002" (Gov.uk, 31 January 2018) <https://www.gov.uk/government/publications/the-proceeds-of-crime-act-section-2a> accessed 25 May 2021.

[513] R v Waya [2012] UK SC 51.

[514] Supra (n 514) GOV.UK.

[515] ibid.

[516] ibid.

[517] [2002] UKHL 1.

[518] R v Benjafield and others [2002] UKHL 2.

[519] [2014] EWCA Crim 1680.

can confiscate the "property", which includes "*all property whatever situated and includes:*" [1] money;[520] [2] all forms of property, real or personal, heritable or moveable;[521] or [3] things in action or other intangible or incorporeal property.[522] Here, the definition of "property", as outlined in section 340(9) of the POCA, essentially captures cryptoassets as well as other intangible properties. Accordingly, section 205 of the Law of Property Act 1925, also supports this notion and defines property as "any thing in action and any interest in real or personal property" and as a result, a cryptoasset is considered "property" under the POCA, which is capable of being laundered. Subsequently, section 340(11)(d) of the POCA, defines money laundering as a prohibited act that constitutes an offence under section 327-329 ***as if it*** had occurred in the UK. In order words, the language captures offences committed outside the UK, thus giving rise to the notion that Parliament did, intend to make POCA offences extraterritorial.

All three principal money laundering offences, as per the POCA, require either knowledge or suspicion of money laundering. To prove 'knowledge or suspicion' of crypto-money laundering is essentially two-fold. On the one hand, to establish 'knowledge', the prosecution must prove that the alleged offender knew that the crypto originated from proceeds of crime. For instance, following a KYC check, it was known to the crypto firm that the account holder was a drug cartel. After speaking to the customer, the criminal overtly disclosed to the employee that the investment and the funds received were derived from human trafficking and drugs. On the other hand, in order to prove 'suspicion', the suspicion does not have to be precise but must be more than merely fanciful.[523] Accordingly, the POCA does not require the suspicion element of money laundering to be exact or firmly grounded or based upon reasonable grounds.[524] Hence, within the context of crypto, if the crypto-firm or employee had any inkling or fleeting notion that the money being paid to the firm may have been derived from illicit sources; and the firm nor its employees submitted a report to the relevant authority, this transgression would suffice as an offence under the POCA.[525] However, a vague feeling of unease would not suffice; thus, one must have reasonable grounds to suspect that the crypto in

[520] POCA, 340(9)(a).
[521] POCA, 340(9)(b).
[522] POCA, 340(9)(c).
[523] R v Da Silva [2006] EWCA Crim 1654.
[524] ibid.
[525] R v Gillard (Simon Paul) (1988) Cr. App R 189.

question derived from illicit sources. As a result, the POCA intended to capture both 'front line' criminals and those facilitating or benefiting from the proceeds of crime (such as crypto firms, ICO consultants, etc.). For instance, if a crypto-firm knew or suspected the funds originated from the proceeds of crime, and nonetheless facilitate the conversion of the illicit funds into crypto then subsequently, transferred the relevant crypto to different crypto-marketplaces then converting the relevant crypto to fiat – this is an actionable offence under the POCA.[526]

The POCA defines criminal property as any benefit from illegal activity; hence, the criminal property includes money, goods, and chattels with a value. In this vein, the statute notes that the property becomes 'criminal property at the point of entry.[527] For instance, an account becomes criminal property once the illicit fund enters into the account.[528] Interestingly, an individual who allows their crypto-account to be operated and used by a criminal, and although their actions are considered 'passive'; the person in question, committed the actus reus required in relation to the aiding and abetting offence under section 328 of the POCA.[529] In *R v GH*,[530] the defendant opened two bank accounts which a criminal subsequently used. The prosecutor alleged that the defendant must have *known or suspected* that the account was to be used for some illegal purpose. Here, the actus reus requirement under the natural meaning of section 328 of the POCA underlines that it is an offence, whereby the defendant is seen to have arranged or facilitate the retention, use or control of "criminal property".[531] It is submitted that the offence of money laundering under the POCA would only be committed when the property in question was deemed "criminal property" at the time of the relevant arrangement.[532] Section 340 of the POCA notes that the prosecutor must prove that the laundered proceeds are thus "criminal property", [533] as a result, the property must constitute a person's benefit from criminal

[526] POCA, s 328.
[527] R v GH [2015] UKSC 24.
[528] ibid.
[529] ibid.
[530] [2015] UKSC 24.
[531] Kensington International Ltd v Republic of Congo [2007] EWCA Civ 1128.
[532] R v Akhtar (Urfan) [2011] EWCA Crim 146.
[533] POCA, s340.

conduct or that it represents such as benefit (*in whole or part and whether directly or indirectly*).[534]

Subsequently, there is no distinction between the proceeds of the defendant's crimes and the proceeds of crimes committed by other individuals. The POCA underlines the premise that "*laundering one's proceeds is just as money laundering, as similar activities performed by someone else, notable professional launderers on behalf of the authors of the predicate or underlying offences*".[535] In support of this assumption, the property includes [1] money, [2] all forms of property or real estate, and [3] things in action as well as other intangible or incorporeal property. Following the legal statement published by the Jurisdiction Taskforce, cryptoassets are thus deemed to be property in the UK[536] and within the scope of the POCA. The legal statement focused on identifying the critical features of a cryptoasset and whether cryptoassets constitute "property" under English law.[537] In *National Provincial Bank v Ainsworth,*[538] Lord Wilberforce set out the traditional principles concerning what is considered property: it must be definable, identifiable by third parties. It must also have some degree of permanence or stability. Thus, within the context of cryptoassets, the law will, as a result, treat them as property because there is ample evidence that there is a large and active crypto market in which cryptoassets are being bought and sold as things of value. In short, cryptoassets have all the legal characteristics of property under the POCA.[539]

In this vein, the 'actus reus' of the POCA offences must demonstrate the act of money laundering and the 'mens rea' element requires the prerequisite of knowledge or suspicion. As a result, the latter element on the knowledge or suspicion is read vaguely so that it catches both 'front line' criminals as well as those facilitating or benefiting from crime.[540] For instance, individuals or otherwise legitimate crypto firms, who knows or suspects that they are laundering

[534] Crown Prosecution Services "Money Laundering Offences" (CPS, 11 June 2021) <https://www.cps.gov.uk/legal-guidance/proceeds-crime-act-2002-part-7-money-laundering-offences>access 21 August 2021.

[535] ibid.

[536] Supra (n 6) UK Jurisdictional Taskforce.

[537] ibid.

[538] [1965] UKHL 1.

[539] AA v Persons Unknow [2019] EWHC 3556.

[540] R v Loizou (Lisa) [2005] EWCA Crim 1579.

for a criminal, as well as family members living a lavish lifestyle deriving from a life of crime.[541] More importantly, following the Code for Crown Prosecutors, there is no limitation concerning the amount of money (the maximum penalty is thus an unlimited fine) or the level of conduct that can lead to prosecution under the POCA offences.[542] Subsequently, for offences committed in the UK, there are no limitation periods in relation to the primary money laundering offences as per POCA[543] or for failure to comply with the regulations and administrative AML requirements, as per section 330 of the POCA.[544] In relation to a crypto firm, the latter offence, as outlined in section 330 of the POCA, pertains to crimes relating to a crypto firms failure to report money laundering and is also subject to the maximum penalty of an unlimited fine. Here, these offences relate to an employee's action and inaction upon discovering *potential* money laundering suspicions concerning a client. As a result, within the context of crypto-money laundering, this chapter examines in detail the [1] concealing offence;[545] [2] the arranging offence;[546] [3] the acquisition, use and possession offence;[547] as well as [4] the POCA regulations concerning a crypto firm's failure to comply with its AML requirements.[548]

Concealing offence: POCA, section 327

"Section 327 Concealing [Offence]

(1) 327(1) A person commits an offence if he—

(a) conceals criminal property;

(b) disguises criminal property;

(c) converts criminal property;

[541] For instance: R v Rezvi [2002] UKHL 1 and R v Waya [2012] UKSC 51.

[542] Crown Prosecution Service, "Legal Guidance, Proceeds of Crime" (*CPS*, 19 December 2021) <https://www.cps.gov.uk/legal-guidance/proceeds-crime> accessed 27 May 2021.

[543] POCA, s 327-329.

[544] ICIG.com, "UK: Ani- Money Laundering Laws and Regulations 2021" (ICIG.com, 25 May 2021) <https://iclg.com/practice-areas/anti-money-laundering-laws-and-regulations/united-kingdom#:~:text=As%20is%20the%20general%20rule,under%20POCA%20or%20the%20Regulations> accessed 27 May 2021.

[545] POCA, s 327.

[546] POCA, s 328.

[547] POCA, s 329.

[548] POCA, s 330.

(d) transfers criminal property;

(e) removes criminal property from England and Wales or from Scotland or from Northern Ireland.

(2) But a person does not commit such an offence if—

(a) he makes an authorised disclosure under section 338 and (if the disclosure is made before he does the act mentioned in subsection (1)) he has the appropriate consent;

(b) he intended to make such a disclosure but had a reasonable excuse for not doing so;

(c) the act he does is done in carrying out a function he has relating to the enforcement of any provision of this Act or of any other enactment relating to criminal conduct or benefit from criminal conduct".[549]

Under section 327(1) of the POCA, it is an offence for an alleged defendant to [1] conceal, [2] disguise, [3] convert, [4] transfer criminal property, as well as to [5] remove criminal property from the UK. A section 327 offence is committed by an individual who "knows or suspects" that the relevant property is deemed "criminal property".[550] The prosecution does not need to prove the action was dishonest or that the alleged defendant was aware of the precise nature of the criminality.[551] Nonetheless, the prosecution must prove all elements of the concealing offence to the criminal standard, namely "beyond reasonable doubt".[552] In this vein, the alleged defendant must "knows or suspects" that the relevant property is "criminal" property. The premise underlines the assertion that the appropriate individual *has* knowledge; thus, there is no need for the prosecution to prove that the alleged defendant "knows" that the relevant property derived from the proceeds of crime. Here, the only element the prosecution must meet is the "suspicion" requirement. As a result, the prosecution must prove that a defendant *suspects* that the relevant property *may* have derived from the proceeds of crime. In practice, the suspicion requirement can be applied very widely; and in some instances, the evidence may be a covert recording of a known crypto client supplying drugs for cash.

[549] POCA, s 327(1)-(2).

[550] POCA, s 340(3).

[551] R v Anwar [2013] EWCA Crim 1865.

[552] Woolmington v DPP [1935] UKHL 1.

Pre-POCA authority, *R v Da Silva,*[553] remains the leading authority on the legal concept of 'suspicion'. Here, the notion of 'suspect' lies from the premise that the alleged defendant must think there is a 'possibility, which is "more than fanciful", that the relevant crypto property derived from the proceeds of crime.[554] However, a vague feeling of unease would not satisfy this legal requirement, as per *R v Da Silva.* Nonetheless, the alleged suspicion does not have to be "clear, firmly grounded nor even based on reasonable grounds".[555] In practice, the rule outlined in *R v Da Silva* can be applied very widely, thus capturing front-line criminals, from small to large scale criminal enterprises and professional to non-professional within the crypto sector. For instance, a peer-to-peer crypto investor can commit a money laundering offence by purchasing cryptoassets that are allegedly stolen, or by accepting a large deposit for a relevant ICO in their capacity as a financial broker or as a solicitor. Effectively, the requirement of suspicion can arise in numerous ways. Thus, the application can be extensive, from noticing something unusual or unexpected will essentially meet the relevant condition for suspicion. Notwithstanding this assertion, the mere suspicion that the relevant property might have been derived from crime is insufficient to constitute the required mental element; mens rea remains a subjective test.

Subsequently, in *Pace and Anor v R*,[556] the Court of Appeal held that a mere suspicion that the relevant property might be criminal property is nonetheless insufficient to constitute the mens rea requirement in a prosecution on a section 327 offence. Effectively, the primary element for a section 327 offence of converting criminal property surrounds the notion that the relevant property must derive from an unlawful conduct. Here, the alleged defendant must be found to have ***known*** that the relevant property was criminal property; thus, the mere proof of 'suspicion' would not suffice. Notwithstanding the guidance provided in *Pace*, in *R v Thompson,*[557] the alleged defendant claimed to have purchased a train set from a market stall, which he later sold to a shop owner for GBP 180. However, it was later transpired that the train set was stolen a few days earlier and had a value of GBP 3,500. Thus, it is uncertain whether

[553] [2006] EWCA Crim 1654.
[554] ibid.
[555] ibid.
[556] [2014] EWCA Crim 186.
[557] [2010] EWCA Crim 1216.

the jury believed the defendant had allegedly purchased the train set from the market stall.[558] Nonetheless, the train set was stolen property and was subsequently sold for a fraction of its value; it was enough to enable the jury to convict the defendant of committing an offence under section 327.[559] As a result, a section 327 offence does not just capture front line criminals, employees or the crypto firm collectively can be involved in money laundering. Here, even if the alleged defendant is innocent and the stolen cryptoasset was transferred and moved around without the required evidential 'proof' that the alleged defendant knew that the relevant property was, in fact, criminal property.

Notwithstanding the above, there are important parallels concerning the following money laundering offences: Thomas could potentially have been charged with either a money laundering offence[560] or a handling stolen goods offence.[561] Here, there are two crucial differences concerning money laundering and the handling of stolen goods. The former does not require a dishonest act. Thus, a lower standard than a section 22 offence, as per the Theft Act 1968, since the alleged defendant must "know or believe" that the goods are in fact stolen, and as a result, acts "dishonestly". By contrast, a section 327 offence under the POCA, the alleged defendant does not need to act "dishonestly", and thus requires a lower standard, here he or she only needs to "suspect" rather than "believe" that the relevant property was criminal property.

Following the above assumption, the prosecution must also prove that the relevant property was, in fact, criminal property. According to section 340(3) of the POCA, criminal property is deemed to be "property that constitutes a person's benefit from criminal conduct, or which represents such a benefit, wholly or partly, and indirectly or directly".[562] In this vein, the alleged defendant must also *know or suspect* that the relevant property is criminal. Here, the property includes all forms of property, which contains cryptoassets.[563] As a result, the legal test on whether a suitable item is deemed property is subsequently low. Thus, an alleged

[558] ibid.
[559] ibid.
[560] POCA, s 327.
[561] Theft Act 1968, s 22.
[562] POCA, s 340(3).
[563] POCA, s 340(9).

defendant or a person obtains an item (tangible or intangible) in which they have an interest in it, then the relevant item is considered 'property', as per section 340(9), POCA. As aforementioned previously, the POCA captures intangible items such as cryptoassets; once a relevant item is deemed 'criminal property', thus the prosecution must prove that the relevant property is derived from the proceeds of crime. In this vein, property includes cryptoassets and all other forms of property, whether real, personal or moveable. The standard legal test of "property" applies, whereby the alleged defendant must at some point have an interest in the relevant criminal property. Following *R v Anwoir and others*,[564] the prosecution must prove a direct or indirect connection between the relevant property and the crime: [1] by showing that the property derived from an illicit or unlawful conduct;[565] and [2] by linking the circumstance to an inference that the relevant property could only be derived from crime.[566]

The above is essentially a two-limb test. The first limb requires evidential proof that the relevant property is derived from proceed of crime, for instance, hacking, fraud, drug, or human trafficking. The second limb requires the prosecution to underline circumstances and examples, whereby an inference of crime can be drawn. Here, a wide range of circumstances and situations where an alleged defendant transfer the relevant property, namely fiat currency or cryptoassets, for another, knowing or suspecting that the other person had no legitimate means of possessing the relevant cryptoasset. Effectively, the prosecution must prove that the relevant property was essentially criminal property when concealed, disguised, or transferred.[567] As noted in the previous section, in *R v GH*,[568] once the lawful property is transferred into a bank account held by a fraudster, the relevant property becomes criminal property when the property was transferred into the fraudster's account.[569] In order words, the property obtains the status of 'criminal property' at the time of the alleged offence, regardless of how many times the relevant property has been concealed, disguised or transferred. Subsequently, in *R v Otegbola*,[570] the Court of Appeal dismissed an appeal concerning the money laundering

[564] [2008] EWCA Crim 1354.
[565] R v Gabriel (Janis) [2006] EWCA Crim 229, [2007] 1.W.L.R. 2272.
[566] Director of the Assets Recovery Agency v Green [2005] EWHC 3168 (admin).
[567] R v Loizou [2005] EWCA Crim 1579.
[568] [2015] UKSC 24.
[569] [2015] UKSC 24.
[570] [2017] EWCA Crim 1147

conviction on the basis that there was an 'irresistible" inference that the relevant property could only have been derived from crime. Here, the notion of 'irresistible' inference underlines the concept that there must be a direct link that shows the cryptoasset was transferred between digital wallets controlled by the alleged defendant(s), and more importantly, there must be no legitimate reason for such large sums of digital currencies to be transferred into the relevant accounts. For instance, the defendant is unemployed, and there is no legitimate reason why the defendant has multiple crypto trading accounts in the UK and abroad, worth more than GBP 10 million. In short, there is an irresistible inference that the relevant property was, in fact, criminal property.

The Supreme Court in *R v GH*[571] made it clear that, in the context of money laundering, the relevant property must have the status or quality of 'criminal property' at the time of the alleged offence. As a result, to prove the relevant property was the criminal property, *R v Anwoir,*[572] provides guidance concerning what is considered an "irresistible" inference. For instance, circumstances where the relevant property or the transaction are deemed to be quite substantial compared to the account holder's employment or net income.[573] After that, the prosecution must show that the digital asset was transferred and dealt with in a highly unusual way, and more importantly, the alleged defendant does not have an adequate explanation in relation to the various transactions carried out through its crypto account, for instance, legitimate income or inheritance, etc.[574] In such circumstances, the jury is entitled to infer that the relevant cryptoassets transferred were, in fact, proceeds of crime. As a result, the accused must have known that the relevant digital property was thus criminal property.[575] In short, for a criminal offence to be committed, there must be an illicit act. For example, crypto money laundering underlines an unlawful conduct or action which is central to the offence. In addition, the POCA offences also require a particular state of mind. Here, the mental element required for POCA offences resolves around the assumption of "knowledge or suspicion". Thus, the accused will be convicted of money laundering if the [1] money or cryptoasset derived from

[571] [2015] UKSC 24.
[572] [2008] EWCA Crim 1354.
[573] ibid.
[574] ibid.
[575] R v Otegbola [2017] EWCA Crim 1147.

the proceeds of crime was laundered, and [2] the defendant doing the laundering either "knew" or "suspected" that the money or cryptoasset derived from the proceeds of crime. Subsequently, the prosecution must adduce evidence to the criminal standard of *beyond reasonable doubt* that the defendant either knew or suspected that the relevant property was criminal property and, nonetheless, laundered the property.

As mentioned above, the mens rea element pertains to the defendant either "knew" or "suspected" that the relevant property derived from the proceeds of crime. The former simply means that the defendant has the knowledge rather than should have knowledge.[576] However, as mentioned previously, the prosecution does not need to prove the defendant knows the relevant property derived from the proceeds of crime. Here, the prosecution only needs to show that the defendant suspected that the relevant property derived from the proceeds of crime. The latter underlines the notion that the defendant must believe there is a possibility that is more than "fanciful"; thus, a vague feeling of unease will not satisfy this criminal requirement.[577] However, the suspicion does not have to be clear, firmly grounded, or even based on reasonable grounds.[578] As a result, following *R v Da Silva,*[579] suspicion can arise in numerous ways and can be applied very widely, from small to large scale criminal offences. In short, suspicion can arise simply from noticing an unusual or unexpected crypto transaction.

Subsequently, the actus reus must include the notion of criminal property, thus deemed an offence within the UK. Here, criminal conduct is understood to be any conduct that is a criminal offence in the UK. Alternatively, if the conduct was committed abroad, the conduct must constitute an offence as if it occurred in the UK.[580] The Serious Organised Crime and Police Act 2005 (the "SOCPA 2005") provides a defence related to a section 327 offence.[581] Here, a person does not commit a section 327 offence if all the following elements apply: if the alleged defendant *knew or believes* that [1] the relevant property derived from a conduct which

[576] R v Saik (Abdulrahman) [2006] UKHL 18.

[577] R v Da Silva [2006] EWCA Crim 1654.

[578] Jonathan Fisher, "Law Commission Suspicion" (Lexology, 20 January 2020) <https://www.lexology.com/library/detail.aspx?g=4766a27f-d2c0-4896-914c-0f4f853a53a3> accessed 14 August 2021.

[579] R v Da Silva [2006] EWCA Crim 1654.

[580] POCA, s 340(2).

[581] The Serious Organised Crime and Police Act 2005, s 102.

occurred in a country or territory outside the UK; and [2] subsequently, the conduct was not, at the time it happened, considered unlawful under the criminal law in the relevant country or territory; [582] and [3] the relevant criminal conduct does not fit the description prescribed by Parliament.[583]

The burden of proof is the legal standard that the Courts of England and Wales must adhere to when considering the standard of proof. For clarity, Andrew Choo argues that the burden of proof pertains to a party's duty to prove a particular fact to the Court.[584] Therefore, the failure to discharge this legal burden would mean the issue will be decided in favour of the other party.[585] By contrast, the evidential burden is provisional in order to satisfy the judge that the issue can be left to a properly instructed jury to reasonably decide the issue at hand.[586] Here, in the context of statutory defence, the evidential burden rests on the defendant whose case would fail if no further evidence on the issue was mentioned before the trial.[587] As a result, if the alleged defendant raises a statutory defence, the evidential burden of proof shifts to the defendant to prove their defence to the civil standard. In order words, the evidential burden is a provisional burden to produce evidence capable of supporting a fact in a case. On the other hand, the standard or the legal burden pertains to a party's duty to prove a particular fact supporting their case.[588]

Accordingly, the civil standard is based "*on a balance of probabilities*", which applies in all civil cases.[589] In *Bank St Petersburg PJSC and another v Arkhangelsky and another,*[590] the Court of Appeal ordered a retrial because the judge had previously applied the wrong standard of proof for dishonestly. The judge previously applied an exacting standard of proof

[582] Please note: The American Cyanamid principles in relation to the process surrounding the granting of an interim injunction pertaining to Worldwide Freezing Orders will be discussed and examined in Chapter 5 of this thesis.

[583] Serious Organised Crime and Police Act 2005, s 102 re a section 327 defence.

[584] Andrew L-T Choo, "Evidence" (5th edn, Oxford University Press 2018) 27.

[585] ibid

[586] ibid.

[587] Joseph Constantine Steamship Line Ltd v Imperial Smelting Corporation Ltd [1942] AC 154.

[588] Wakelin v London & South Western Railway Co [1886] 12 App CAS

[589] Miler v Minister of Pension [1947] 2 All ER 372.

[590] [2020] EWCA Civ 408.

for dishonestly.[591] The legal burden could only be discharged by showing the facts were incapable of an innocent explanation. However, the correct standard was "what explanation was more probable than not, having considered the nature and gravity of the allegations".[592] In short, the civil standard of proof is based "on a balance of probabilities", where the facts at hand are more probable than not. Nonetheless, some commentators suggest that the standard of proof may vary depending on the gravity of the misconduct alleged.[593] Lord Nicholls provides that the standard of proof should vary depending on the seriousness of the consequence for the individual(s) concerned.[594] Subsequently, Lord Nicholls indicates that the Court should be mindful of the factors appropriate in the particular case, "*that the more serious the allegations, the less likely it is that the event occurred and, hence, the stronger should be the evidence before the court concludes that the allegation is established on the balance of probability*".[595] However, the House of Lords rejected Lord Nicholls's assumption *in Re S-B (Children)*.[596] The House of Lords held that neither the seriousness of the alleged conduct nor the consequences should make any difference when determining the facts. More importantly, *Re S-B (Children)* confirmed that the principle "*the more serious the allegation, the more cogent the evidence needed to prove it was a misinterpretation of what Lord Nicholls had said*".[597] As a result, this case clarified the application of the civil standard of proof in cases where serious allegations of misconduct are made. In *Re Doherty,*[598] the Lords reconfirmed the civil standard of proof in cases where serious allegations are made. However, the Lords expressed different views surrounding the seriousness of the consequences for the respondent(s) if the alleged misconduct is established.[599] For instance, Lord Carswell and Lord Brown views differed in relation to the

[591] Gordon Exall, "Court of Appeal overturns findings of fact: the standard of proof for dishonestly: Also delay of 22 months in giving judgment unacceptable" (Civil Litigation Brief, 18 March 2020) <https://www.civillitigationbrief.com/2020/03/18/court-of-appeal-overturns-findings-of-fact-the-standard-of-proof-for-dishonesty-also-delay-of-22-months-in-giving-judgment-unacceptable/> accessed 10 August 2021.

[592] John Rogerson and William Obree, "Proving Fraud in the English Courts – a higher standard?" (White & Case LLP, 2 April 2020) <https://www.whitecase.com/publications/alert/proving-fraud-english-courts-higher-standard> accessed 10 August 2021.

[593] John Calvin Jeffries and Paul Stephen, "Defenses, Presumptions, and Burden of Proof in the Criminal Law" (1979) 88 The Yale Law Journal 7.

[594] Re Doherty [2008] UKHL 33.

[595] Re H (Minors) (Sexual Abuse: Standard of Proof) [1996] AC 563.

[596] [2008] UKHL 35.

[597] ibid at paragraph 13.

[598] [2008] UKHL 33.

[599] ibid.

relevant of the seriousness of consequences. On the one hand, Lord Carswell submits that the seriousness of the consequences must be deemed as a factor inherent to the likelihood of the event having occurred.[600] In other words, a defendant is less likely to commit a crime if the consequences are deemed to be serious. On the other hand, Lord Brown express concerns in relation to Lord Carswell's view, and as a result, he provides that cogent evidence must be required to establish allegations which may have serious consequences, even when the matter is inherently improbable.[601]

It is submitted that further clarification will be required since, despite these clear statements of authority,[602] it appears that some courts continue to apply a third "intermediate" standard of proof in cases where serious allegations are made. It is observed that the extent to which some courts apply the third "intermediate" standard of proof will depend on the facts of a particular case. For instance, in *Ion Sciences Ltd v Persons Unknown and others*,[603] Binance Holdings Limited was implicated in an interim judgment (and without an opportunity to answer the claimants' allegations). The Exchange was subsequently banned from operating in Europe.[604] As a result, in *JSC BTA Bank v Ablyazov and others*[605] warned that although the standard of proof was the civil standard (on the balance of probabilities), the evidence relied upon must be commensurate with the seriousness of the misconduct alleged. Here, when assessing the balance of probabilities, some courts would consider that the more serious the alleged misconduct, the less likely it was to be true, and as a result, the stronger the evidence required.[606] It is submitted that a higher standard of proof may be appropriate in a civil proceeding with potentially serious consequences.[607]

---

[600] ibid.

[601] ibid.

[602] For instance, in Re H (Minors) (Sexual Abuse: Standard of Proof) [1996] AC 563, the House of Lords provided that the UK does not recognise a third, "intermediate" standard of proof.

[603] 21 December 2020 (Commercial Court).

[604] Tom Wilson, "As scrutiny mounts, crypto exchange Binance to wind down derivatives in Europe" (Reuters, 20 July 2021) <https://www.reuters.com/technology/crypto-exchange-binance-wind-down-futures-derivatives-offerings-europe-2021-07-30/> accessed 18 August 2021.

[605] [2013] EWHC 510 (Comm).

[606] Burns v The Financial Conduct Authority [2017] EWCA Civ 2140.

[607] Commissioners of Police of the Metropolis v Ebanks [2012] EWHC 2368 (Admin).

Subsequently, it is commonly accepted that the global adherence to the FATF standards remains uneven. Here, crypto providers can easily provide cross-border transactions. As a result, criminals can leverage crypto exchanges in jurisdictions with fewer levels of AML compliance or no compliance through decentralised P2P payments or other DeFi platforms, such as UniSwap. At the present, no crypto criminals have been trialled in the UK for money laundering offences. Only [1] *AA v Persons Unknown*,[608] the first landmark, confirmed cryptoassets as property capable of being the subject of a Worldwide Freezing Order; and [2] *Ion Sciences Ltd v Persons Unknown and others*,[609] the first ICO fraud case. Effectively, this provides international crypto money launders increased leverage to adopt a section 102 defence, as per the SOCPA. The Commercial Court granted a proprietary injunction,[610] coupled with a Worldwide Freezing Order against persons unknown. Thus, when the first crypto money laundering trial happens, the alleged defendant(s) can and will leverage the judicial grey area, increased by the uneven implementation of the FATF standards,[611]and if required, raise a section 102 SOCPA defence to shift the burden of proof to the lower civil standard. In practice, the alleged defendant can also prove that the relevant crypto transactions occurred abroad. For instance, Jersey is known as a low-tax, relaxed crypto and money laundering jurisdiction.[612] Unlike the UK, Jersey is a low-tax jurisdiction, and the Government of Jersey rejected "a full prudential and conduct of business regime" for cryptoassets. As a result, crypto exchanges with an annual turnover of below GBP 150,000[613] does not have to comply with AML and CTF laws nor KYC requirements, as mandated by the FATF.[614]

[608] [2019] EWHC 3556 (Comm).

[609] 21 December 2020 (Commercial Court).

[610] Re circumstances in which injunctions may be granted will be discussed in Chapter 5, titled "Process and enforcement".

[611] Magdalena Roibu, "A Bit(coin) dirty. The new means of money laundering" (*Schonherr*, 1 February 2021) <https://www.schoenherr.eu/content/a-bit-coin-dirty-the-new-means-of-money-laundering/> accessed 12 June 2021.

[612] Carey Olsen, "Jersey: Leading the way on crypto currency" (*Jersey Finance*, 3 May 2018) <https://www.jerseyfinance.je/our-work/jersey-leading-the-way-on-crypto-currency/> accessed 13 June 2021.

[613] Global Legal Insights, "Jersey blockchain and cryptocurrency regulation 2020, second edition" (Carey Olsen, 2020) <https://www.careyolsen.com/sites/default/files/CO_JSY_Blockchain-and-Cryptocurrency-Regulation-2020-2nd-Edition.pdf> accessed 12 June 2021.

[614] Clare Feikert-Ahalt, "Regulation of Cryptocurrency in Selected Jurisdictions" (The Law Library of Congress, June 2018) <https://www.loc.gov/law/help/cryptocurrency/regulation-of-cryptocurrency.pdf> accessed 12 June 2021.

In addition, the alleged defendant can also submit a section 327(A2), POCA, defence to a section 327 money laundering offence. Here, the "criminal conduct" is an offence in the UK, but the transaction occurred overseas, and the local jurisdiction views the relevant conduct as lawful. As a result, the alleged defendant can then argue that their conduct is not unlawful in Jersey. Thus, the criminal conduct alleged by the prosecution in the UK does not fit any criminal description in the statute. More importantly, the relevant transactions occurred beyond the jurisdiction of England and Wales.[615] As a result, when the first crypto-money laundering case appears in the UK. It is submitted that the alleged defendant could raise a successful section 102 defence, as per SOCPA, as well as a section 327(2A) POCA defence; unless there is an "irresistible" inference that the relevant property could only have been derived from the proceeds of crime. In these circumstances, the jury is entitled to infer that the cryptoassets derived from the proceeds of crime. Here, the accused must have known that the relevant digital property was criminal property.[616] Accordingly, the alleged defendant must not have an adequate explanation in relation to the suspicious transactions.

Notwithstanding the above, a section 327 offence has five potential methods of commission rather than five different offences. Here, the five methods are concealing, disguising, converting, transferring and removing, all relevant to crypto money laundering. Nonetheless, to be indicted of a section 327 offence, the prosecution must specify the precise method of money laundering, or it would offend the principle of duplicity.[617] According to the Crown Prosecution Service, "*…the rule was that generally no single count on an indictment should charge a defendant with two or more separate offences*".[618] As the technology is developing and rapidly changing, it is uncertain whether the crown prosecution service can precisely define and draft and indictment that avoids the principle duplicity. It will be open to the defence to arrange for the indictment to be quashed.[619] Given the complexity of the crypto-technology, there will be instances where an alleged defendant's actions will include all five of the methods of commissions as described by section 327. For example, a person transfers GBP

[615] POCA, s 327(2A).

[616] R v Otegbola [2017] EWCA Crim 1147.

[617] R v Greenfield [1973] 1 WLR 1151.

[618] Crown Prosecution Services, "Drafting the Indictment: Legal Guidance" (CPS, 13 December 2018) <https://www.cps.gov.uk/legal-guidance/drafting-indictment> accessed 12 June 2021.

[619] ibid.

50,000 of stolen fiat currency to a small crypto exchange (with an annual turnover of less than GBP 150,000) based in Jersey, which does not comply with AML and CTF laws or KYC requirements then converts the fiat to Ethereum. The same person then uses the Ethereum to purchase CryptoKitties; they then collect and breed the digital cats on the Ethereum platform. Over the same time, they sold the virtual cats then transferred the relevant tokens to a crypto account based in Jersey. The anonymous user then converts the cryptoasset to US dollars they then transfer the proceeds to a bank account held in the Cayman Islands. In short, it can be argued that the alleged defendant committed all five methods of commission (i.e. conceal, convert, transfer and removing criminal property from the UK).

Following the above assertion, section 327 of POCA defines *concealing or disguising* cryptoassets as "concealing or disguising its nature, source, location, disposition, movement, ownership or any rights with respect to it". This essentially outlines a section 327(3) count concerning the "concealing or disguising" of the criminal property. A typical example of *concealing or disguising* would be inserting illicit cash into a Bitcoin ATM to purchase Bitcoins,[620] later declaring that the relevant property derived from a legitimate cash business. By contrast, the notion of "converting" the proceeds of crime was discussed in *R v Fazal*.[621] Here, the count of converting criminal property revolves around the actus reus of taking or receiving or retaining or parting with someone else's property. Here, the most common conversion method involves accepting or transferring illicit funds to a digital wallet, subsequently withdrawing the amount later via Bitcoin ATM, and giving the agreed "clean" cash to the criminal.

Finally, the 4th and 5th methods of commission are more commonly known as "transferring and removing". An example of "transferring and removing" criminal property involves transferring and removing illicit funds from the UK. In this vein, a person guilty of an offence under section 327 of the POCA will be liable on a summary or a conviction on indictment. The former underlines a summary conviction and imprisonment for a term of not exceeding six years, a fine not exceeding the statutory maximum, or both; whilst the latter

[620] Chainbytes, "How to use Bitcoin ATM" (*Chainbytes*, 2021) <https://www.chainbytes.com/how-to-use-bitcoin-atm/> accessed 13 June 2021.

[621] [2009] EWCA Crim 1697.

prescribes a conviction through an indictment, thus imprisonment for a term not exceeding 14 years, coupled with a fine, or both.[622] Finally, a crypto firm or corporate entity convicted of a money laundering offence is liable to an unlimited fine.[623]

Arranging offence: POCA, section 328

"*Section 328 Arrangement [Offence]*
(1) 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.
(2) But a person does not commit such an offence if—

> *(a) he makes an authorised disclosure under section 338 and (if the disclosure is made before he does the act mentioned in subsection (1)) he has the appropriate consent;*
> *(b) he intended to make such a disclosure but had a reasonable excuse for not doing so;*
> *(c) the act he does is done in carrying out a function he has relating to the enforcement of any provision of this Act or of any other enactment relating to criminal conduct or benefit from criminal conduct*".[624]

This section will examine the offence of entering into an arrangement to launder the proceeds of crime, as per section 328 of the POCA, coupled with potential defences available to a (scenarios) crypto-money laundering offence. Here, a crypto user commits a crime if they enter into, or becomes involved in, a crypto money laundering arrangement where they know *or suspects* the relevant property purchased, used or control of criminal property by another counterpart, or by or on behalf of another person.[625] Following this statutory definition, a section 328 offence can potentially be a very wide offence, involves the "arrangement" thus in the scope of 'facilitation' of a money laundering offence on behalf of another counterpart. Here, this could include transferring fiat money to a personal digital wallet or keeping cryptoassets or

[622] POCA, s 334(1)(a).

[623] ICLG.com "UK: Anti-Money Laundering Laws and Regulations 2021" (ICLG.com, 2021) <https://iclg.com/practice-areas/anti-money-laundering-laws-and-regulations/united-kingdom> accessed 31 August 2021.

[624] POCA, s 238(1)-(2).

[625] POCA, s 328.

other digital property for another person. Unlike the POCA section 327 concealing offence, the arranging offence, as per section 328 the POCA, the latter is deemed the most likely offence committed by a crypto-firm or financial institution regulated by the FCA. By contrast, according to section 327 of the POCA, the concealing offence is most likely to be committed by a natural person, for instance a frontline criminal or an international criminal organisation.

As discussed in the previous section, the prosecution must first prove that the relevant property derived from the proceeds of crime, and thus, criminal property.[626] After that, similar to a section 327 offence, the alleged defendant must know or suspect that the property is criminal property. Following *AA v Persons Unknown,*[627] cryptoassets falls within the definition of "property" as prescribed by section 340(3) of the POCA. Here, the classical legal test applies: an alleged defendant obtains the property at the point in which they have an interest in it.[628] In addition, as mentioned in the previous section, there are two ways in which the prosecution must prove the relevant property derived from the proceeds of crime. On the one hand, the prosecution may seek to establish the relevant property derived from a specific kind of conduct that was unlawful. Alternatively, the prosecution may show circumstances in which the relevant digital asset was handled, giving rise to an irresistible inference that the relevant property could only be derived from crime.[629] In short, the former links the relevant property directly to unlawful conduct, thus underlining primary evidence of wrongdoing; whilst the latter pertains to circumstantial evidence that depends on the unlikelihood of coincidence that the defendant's guilt can rationally explain.

To illustrate the above, the first limb captures examples derived from conduct that can only be criminal. For instance, the alleged defendant is a known drug or human trafficker. Whilst moving the drugs and illegal immigrants from her property, the defendant was seen by a neighbour who called the police. When the police arrived at the defendant's house, she has multiple USB keys containing several crypto accounts with large sums of cryptoassets and fiat currencies. This is a classic case of crypto-money laundering, with direct evidence of the

[626] POCA, s 340(3).
[627] [2019] EWHC 3556 (Comm).
[628] R v Anwoir and others [2008] EWCA Crim 1354.
[629] ibid.

defendant being in the property, coupled with the large sums of cash and digital assets, which undoubtedly derived from her criminal activities. Subsequently, the second limb captures examples where circumstances are such that an irresistible inference of crime can be drawn. For instance, a fraudster creates a website that falsely purports to sell Bitcoin to retail investors. The fraudster recruited a consultant who opened two crypto accounts into which customers from the website transferred fiat currency for Bitcoins. However, upon purchase, the customers never received the agreed Bitcoins. In this case, the fraudster would be liable for a section 327, the POCA offence, whilst the crypto consultant, based on the circumstance described, must have known, or at least suspected, that the fraudster had some illegal purpose. For instance, how did the fraudster come into possession of such large sums of money, which was substantial when compared to the net income of the fraudster's employment. Here, there is no direct evidence that the consultant knew of the fraudster's unlawful purpose. However, given the usual transactions, coupled with the ambiguous arrangement, there is strong circumstantial evidence that the consultant must have known or suspected that the investments derived from criminal proceeds, thus liable for a section 328, the POCA offence. Here, the prosecution must seek to prove a series of events and circumstances that can be explained rationally, only by the defendant's guilt.[630] The prosecution must prove circumstances that give rise to the irresistible inference that the relevant asset could only be derived from crime.

As previously stated, section 328, the POCA offence, is the primary offence committed by crypto-professionals, crypto firms, or professionals regulated by the FCA. A section 327, the POCA offence intends to capture front line criminals and non-regulated professionals within the crypto space. Thus, similar to the second scenario stated above, in *R v GH,*[631] the defendant allowed his bank account to be used for fraud. Here, the primary fraudster transferred its customers' deposits and payments for a non-existent insurance cover. The Supreme Court held that the defendant had committed a section 328, the POCA offence. As a result, the lawful deposits and payments became criminal property as soon as the relevant property was transferred into the bank account.[632] Allen Overy published an article submitting that the Supreme Court had provided a narrow interpretation of what is considered "…*'criminal*

[630] McGreevy v DPP [1973] 1 WLR 276.
[631] [2015] UKSC 26.
[632] ibid.

property' as being property that is already 'criminal' by reason of criminal conduct which is separate from the conduct alleged to constitute the money laundering (a section 328) offence itself".[633] Here, the Supreme Court asserted that the rationale behind this interpretation rests upon the potential consequences for third parties, such as crypto firms, banks, and other financial institutions regulated by the FCA. As demonstrated in Chapter 2, crypto firms regulated by the FCA have an onerous reporting obligations. Thus, if they know or suspect, or have reasonable grounds for knowing or suspecting, that their client is engaged in money laundering, the crypto firm must report the suspicious transaction.

Subsequently, there are essential distinctions between money laundering and handling stolen goods. On the one hand, the former provides that an alleged offender can only be guilty of section 22, Theft Act 1968 if she "knew and believe" that the goods are stolen and acts "dishonestly". On the other hand, sections 327-329 money laundering offences as per, POCA, do not require any dishonest act and adopts a lower standard, namely "suspects" rather than "believes", as per section 22, Theft Act 1968. Accordingly, the Supreme Court in *R v GH*[634] cautioned that "*the courts should be able to use their powers to discourage the inappropriate use of the provisions of POCA to prosecute conduct which is sufficiently covered by substantive offence, as they have done in relation to handling stolen property*".[635] Thus, as mentioned in the previous section, the prosecution should avoid duplicity in relation to additional counts under sections 327-329 money laundering offences, unless there is a '*proper public purpose in doing so*",[636] or risk the money laundering indictment being quashed by the courts. For clarity, the prosecution should include a count, if and when it can be proved that "…*a thief concealed what he must have known or suspected was stolen property, but there is doubt as to whether the prosecution can prove that he was the thief himself*".[637] In practice, the Supreme Court's judgement in *R v GH* is unlikely to affect regulated crypto firms, banks or other financial institutions under section 330 reporting obligations as per the POCA. This will be examined in

[633] Allen Overy, "Supreme Court considers the constituent element of an offence under section 328 of POCA" (*Allen Overy*, 22 May 2015) <https://www.allenovery.com/en-gb/global/news-and-insights/publications/supreme-court-considers> accessed 14 June 2021.

[634] [2015] UKSC 26.

[635] Supra (n 630).

[636] ibid.

[637] ibid.

more detail in Chapter 5, titled "Process and enforcement". Here, in scenarios where a regulated crypto firm suspects that a crypto account is being opened in which proceeds of crime are being deposited and transferred, the crypto firm's AML/KYC framework should, in theory, preclude the crypto account from being opened. Thus, it is unlikely crypto firms will be captured by section 328 of the POCA offence (provided they have an AML/KYC framework in place).

In short, the *actus reus* of a section 328 POCA offence is entering or being concerned in an arrangement that facilitates the acquisition of criminal property, whilst the *mens rea* required is knowledge or suspicion. Unlike the section 327 POCA offence, an offence under section 328 underlines a two-limb test to establish the mental element of the offence created by section 328(1), as per POCA. On the one hand, the defendant must *intentionally or recklessly* enter into an arrangement that facilities the buying, holding, selling or control of criminal property by other counterparts or on behalf of another individual. On the other hand, the defendant must *know or suspect* that the arrangement would be used for money laundering purposes. For instance, a crypto investor agrees to invest GBP 50,000 in Ethereum on behalf of another individual without further inquiry concerning the source or origin of the relevant funds. Over the same period, the crypto investor receives more than GBP 1 million from his counterpart. This scenario demonstrates the relevance of the two-limb test. The crypto investor recklessly entered into an arrangement without much forethought. Subsequently, he must have suspected that the arrangement was used for illicit purposes, given the substantial sum he had received from his counterpart (and without further inquiry).

Notwithstanding the above, there are several statutory defences available to section 328, POCA offence; and as discussed in the previous section, if the defendant raises a statutory defence, the evidential burden shifts to the defendant to prove the defence to the civil standard, also known as the 51% test or on the balance of probabilities test. Here, section 328(2A) creates a statutory defence to section 328, the POCA, when the "criminal conduct" as per section 340, POCA is an offence in the UK. However, the relevant conduct occurred overseas, and the local Court permitted it in the host jurisdiction. Here, the issue of overseas transactions and enforcing English orders abroad will be examined in the Chapter 5. Thus, an individual guilty of an offence under section 328 of POCA is liable on a summary conviction or a conviction on indictment. The former outlines a summary conviction, thus imprisonment for a term of not

exceeding six years, or a fine not exceeding the statutory maximum, or both; whilst the latter prescribes a conviction through an indictment, imprisonment for a term not exceeding 14 years, or an unlimited fine, or both.[638] Finally, a crypto firm or corporate entity convicted of a money laundering offence is liable to an unlimited fine.[639] In short, on the same terms as a section 327 offence.

Acquisition, use and possession offence: POCA, section 329

"*Section 329 Acquisition, use and possession [Offence]*

(1) A person commits an offence if he—

(a) acquires criminal property;

(b) uses criminal property;

(c) has possession of criminal property.

(2) But a person does not commit such an offence if—

(a) he makes an authorised disclosure under section 338 and (if the disclosure is made before he does the act mentioned in subsection (1)) he has the appropriate consent;

(b) he intended to make such a disclosure but had a reasonable excuse for not doing so;

(c) he acquired or used or had possession of the property for adequate consideration;

(d) the act he does is done in carrying out a function he has relating to the enforcement of any provision of this Act or of any other enactment relating to criminal conduct or benefit from criminal conduct".[640]

This section will examine the acquisition, use and possession offence, as per section 329 of the POCA, coupled with potential defences available and possible scenarios concerning crypto-money laundering offences. Here, the elements of section 329, the POCA, requires the prosecution to prove beyond a reasonable doubt that the alleged defendant had: [1] acquired criminal property, [2] used the relevant property, and [3] was in possession of the relevant

[638] POCA, s 334(1)(a).

[639] Sentencing Council, "Corporate offenders: fraud, bribery and money laundering" (Sentencing, 1 October 2014) <https://www.sentencingcouncil.org.uk/offences/magistrates-court/item/corporate-offenders-fraud-bribery-and-money-laundering/> accessed 31 August 2021.

[640] POCA, s 329(1)-(2).

property.[641] Here, the latter notion of possession is not subject to any legal notion of acquisition. Thus, a section 329 offence is similar to the offence of handling stolen goods. As a result, the alleged defendant does not have to be involved in the underlying criminal conduct or the actual process concerning the money laundering scheme but enjoys the benefits of the illicit proceeds, are guilty of a section 329 offence. Here, a section 329 offence usually captures the primary criminal offender's family member or associates. In this vein, this offence is used to prosecute the family of criminals. For instance, a family member enjoyed a lavish lifestyle when compared to the net income of the individual's salary or occupation and no obvious explanation of how the relevant income might have come about.

Following the requirements of a section 329 offence, the prosecution must prove the alleged defendant had *knowledge or suspicion* of the primary offender's unlawful conduct. In the landmark case, *Hogan v Directors of Public Prosecutions*,[642] the alleged defendant purchased the relevant property for an 'adequate consideration'.[643] Here, an alleged defendant who purchased the relevant property for an 'adequate consideration' cannot be guilty of a section 329, POCA offence, even if the suspected defendant knows the goods being purchased may be criminal property. Notwithstanding this assertion, the alleged defendant must address the charge of handling stolen goods, as per section 22 of the Theft Act 1968. Nonetheless, the aforementioned 'adequate consideration' defence is only available to a section 329, POCA charge, thus not open to 327-328 offences. In *Hogan*, the defence of adequate consideration is a question of fact and must be answered separately concerning whether the relevant property constitutes criminal property.[644] For example, an unrecorded payment for a USB key containing 100 Bitcoins, and the payment was made in cash. Here, the cash payment represented less than 10% of the market value of the Bitcoins held in the USB key. The circumstances indicated a strong inference and evidence that the alleged defendant *knew or suspected* that the relevant Bitcoins were derived from illicit means. *Why sell Bitcoins at a 90% discount?* Subsequently, as prescribed by section 340 of the POCA, the notion of criminal property underlines the requirement to assess the state of mind of the alleged defendant. The suspected defendant must

[641] POCA, s 329(1).
[642] [2007] EWHC 978.
[643] POCA, s 329(2)(c).
[644] [2007] EWHC 978.

know or suspect that the relevant property was stolen since the cryptoasset was purchased at a 90% discount. There would be strong evidence that the relevant property would be criminal property. Nonetheless, an alleged defendant who purchases a relevant property for adequate consideration (for instance, 10% discount instead of 90% discount) cannot be guilty of an offence under section 329 of the POCA.[645] Thus, once the Court concludes that adequate consideration was given to purchase the relevant property, no crime was committed under section 329 of the POCA, even if the alleged defendant had known or suspected that the relevant property had been stolen.

If and when an alleged defendant raises an adequate consideration defence, the burden of proof does not shift. As a result, the prosecution must prove whether the requirement for adequate consideration requirement are met.[646] Following *Hogan v Directors of Public Prosecutions*,[647] the question of adequate consideration was deemed to be a separate issue from the state of mind requirement as prescribed by the POCA. It required an independent analysis from the Court. However, whether an alleged defendant reached the adequate threshold must be determined by the Court on a case-by-case basis. The Court must examine all relevant facts and circumstances concerning the alleged claim to determine whether the threshold has been met.[648] In *R v Haque*,[649] the Court provided some guidance concerning the question of adequate consideration. Following section 329(1)(a), POCA, it was held that the alleged defendants had not "acquired" criminal property by receiving automatic transfers from victims of fraud. In this case, the fraudsters instructed the victims to transfer large sums of money into bank accounts held by a syndicate of conspirators. Here, money from two of the victims was subsequently transferred into an account held in the joint names of the defendants (husband and wife). As a result, the defendants appealed against their conviction for acquiring criminal property, as per section 329(1)(a), POCA.

[645] POCA, s 329(2)(c).
[646] R v Haque [2019] EWCA Crim 1028.
[647] [2007] EWHC 978.
[648] ibid.
[649] [2019] EWCA Crim 1028.

It was submitted that there was no case to answer relating to the count of acquiring criminal property, on the grounds that, at the time when the money was transferred into the defendant's account, it was not criminal property,[650] thus not meeting the requirement, as prescribed by section 329(1)(a), POCA.[651] However, had the charge been framed under a different count, such as a section 328, POCA offence (as discussed in the previous section) relating to the retention, use or control of criminal property, once the money was transferred into the account, it became criminal property. This case stood as an illustration on the part of the prosecution when formulating and drafting the indictment against the defendant since failure to formulate the correct charge could have serious consequences, as seen in *R v Haque*.[652]

Crypto Money Laundering

In summary, crypto money laundering structures are a realistic money laundering tool, which can be integrated with current-day money laundering schemes. As demonstrated in this Chapter, although the technology used in crypto money laundering does not conform to existing case law, the criminal conduct concerning the schemes' arrangement and behaviours are contended to be the same. This chapter concludes with the following questions. First, the question arises concerning how English Courts should deal with this new money laundering technique. It is submitted that the start and endpoint of crypto money laundering often includes a crypto exchange. Only five crypto firms have received the appropriate AML/KYC designation from the FCA to operate in the UK.[653] Nonetheless, whether an English order or judgment can be enforced abroad will depend on the law of that particular country. Thus, domestically, English law enforcement must be able to seize and analyse the relevant crypto accounts of identified criminals to identify the crypto accounts to trace the illicit assets.

Second, the question arises on how cryptoassets should be treated from a legal perspective. At present, the case law concerning cryptoassets is still developing. Decisions,

[650] ibid.
[651] R v GH [2015] UKSC.
[652] [2019] EWCA Crim 1028.
[653] Supra (n 66) Oliver.

such as *AA v Persons Unknown*[654] and *Ion Science Ltd v Persons Unknown,*[655] are critical *interim* decisions transforming the law within the crypto space. More importantly, interim judgments are granted at an early stage in the proceedings; thus, the crypto community awaits the final decision in order to establish a consistent legal principal for future case law. Nonetheless, *Ion Science Ltd v Persons Unknown Others*,[656] is an important decision concerning the emerging case law on cryptoassets. Here, the applicants believed that they had been victims of ICO fraud. The first applicant is a company registered in England and Wales and the second applicant is a natural person domiciled in the UK. The Commercial Court at the Royal Courts of Justice had granted a proprietary injunction, coupled with a worldwide freezing order concerning a cryptoasset ICO fraud claim. The judgement follows *AA v Persons Unknown*,[657] an earlier decision concluding that cryptoassets comes within the common law definition of property.[658] As a result, cryptoassets in the UK are no longer in the twilight zone. Although the technology does not conform to existing case law, the criminal conduct surrounding the three primary money laundering offences, as per the POCA, are viewed to be the same.

Section 327 of POCA defines *concealing or disguising* cryptoassets as "concealing or disguising its nature, source, location, disposition, movement, ownership or any rights with respect to it". A typical example of *concealing or disguising* would be inserting illicit cash into a Bitcoin ATM to purchase Bitcoins,[659] later declaring the digital asset as legitimate property. Alternatively, the alleged defendant can convert illicit funds by transferring the digital asset to a digital wallet. After an agreed amount of time, the alleged defendant withdraws the appropriate amount via crypto exchange service and then gives the principal criminal the "clean" cash. Unlike section 327, a section 328 arranging offence is likely to capture crypto firms or financial institutions regulated by the FCA than front line criminals. Here, a crypto firm commits a crime if they enter into, or becomes involved in, a crypto money laundering

[654] [2019] EWHC 3556 (Comm).

[655] (unreported), 21 December 2020 (Commercial Court).

[656] 21 December 2020 (Commercial Court).

[657] [2019] EWHC 3556 (Comm).

[658] The same conclusion was also reached in New Zealand in the case of Ruscoe v Cryptopia Ltd (in Liquidation) [2020] NZHC 783.

[659] Chainbytes, "How to use Bitcoin ATM" (*Chainbytes*, 2021) <https://www.chainbytes.com/how-to-use-bitcoin-atm/> accessed 13 June 2021.

arrangement where they know *or suspects* the relevant property purchased, used or controlled is criminal property.[660] For instance, a crypto firm agrees to invest GBP 500,000 in Bitcoins on behalf of its client without further inquiry concerning the source of the relevant funds. Over a period, the crypto firm receives more than GBP 10 million. However, due to the firm's lack of due diligence, the crypto firm recklessly entered an arrangement without much forethought. The crypto firm must have suspected that the arrangement was used for illicit purposes, and given the substantial sum received, the company acted recklessly. Finally, a section 329 offence usually captures the primary offender's family or associates. In this vein, this offence is used to prosecute the family of criminals. This research provides a limited overview of criminals using crypto for money laundering purposes.

Finally, this chapter concludes that crypto money laundering is a conceivable concept. Nonetheless, further research concerning the process and enforcement (domestically and abroad) of the POCA offences are necessary to understand crypto money laundering to its fullest extent. From this research, it is submitted that the law can intervene via the POCA framework since the case law presented in this chapter provides sufficient means for the Courts of England and Wales to enforce AML rules and regulations. In short, cryptoassets in the UK are no longer in the twilight zone since the criminal conduct surrounding the three primary money laundering offences under the POCA are found to be the same.

[660] POCA, s 328.

Chapter 5: Process and Enforcement

This chapter will examine Part 5 of the POCA. As a result, this chapter will set out the challenges surrounding the enforcement and seizure of illegal assets. Recently, HM government published a policy statement in relation to the UK's Economic Crime Plan. The UK observed how the Covid-19 pandemic has shifted how criminals operate, leading to increased use of cryptoassets in money laundering across various serious organised crime groups,[661] The policy statement notes, "…*the possibility of hundreds of billions being laundered within and through the UK every year*".[662] As a result of local lockdowns, cash-based money laundering, such as money mules or low-level money laundering schemes, have stalled.[663] Nevertheless, the laundering of proceeds of crime is a crucial enabler of organised crime, and the threat is evolving due to the emergence of cryptoassets.[664] Here, substantial illicit funds are laundered through crypto-based money laundering, reflecting the use of complex high-end money laundering schemes coupled with the misuse of cryptoasset platforms to obscure the ownership of illegal assets. Following the confiscation of around 250 million worth of cryptoassets, Deputy Assistant Commissioner Graham McNulty observed that "organised criminals are increasing using cryptoasset to launder their dirty money. However, cash remains king in the criminal world".[665]

Accordingly, the Courts of England and Wales considers both Bitcoin and Ether to be property and is subject to its jurisdiction. However, the case law in relation to crypto money laundering is underdeveloped. Nonetheless, the FCA must clarify its position on the treatment

[661] HM Government, "Economic Crime Plan 2019 to 2022" (UK Finance, 4 May 2021) <https://www.gov.uk/government/publications/economic-crime-plan-2019-to-2022> accessed 31 August 2021.

[662] HM Government, "Economic Crime Plan: statement of progress" (UK Finance, 4 May 2021) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/983251/Economic_Crime_Plan_Statement_of_Progress_May_2021.pdf> accessed 31 August 2021.

[663] Eleanor Sly, "Leeds woman jailed after trying to smuggle £5.5m from UK to Dubai" (The Independent, 28 July 2021) <https://www.independent.co.uk/news/uk/crime/money-laundering-leeds-tara-hanlon-b1891152.html> accessed 31 August 2021.

[664] Robert Hart, "British Police Seize $250 Million of Cryptocurrency in International Crackdown" (Forbes, 13 July 2021) <https://www.forbes.com/sites/roberthart/2021/07/13/british-police-seize-250-million-of-cryptocurrency-in-international-money-laundering-crackdown/> accessed 31 August 2021.

[665] ibid.

of other cryptoassets, such as DeFi tokens[666] or non-fungible tokens.[667] More importantly, the lack of a consistent global regulatory framework creates uncertainty and increases the potential for market abuse, financial crime, and high-end money laundering schemes, increased with the misuse of cryptoasset platforms to obscure ownership of illicit assets. By design, cryptoassets offer a degree of anonymity and thus present a higher risk in relation to money laundering and sanctions violation. For instance, a cryptoasset held in an "unhosted wallet" reside in the user's computer or offline, thus evading proper KYC or AML checks. In addition, anonymity can be further through mixing or tumbler[668]services that anonymise or obfuscate the source of the crypto transactions.[669] Here, a mixer or tumbler service essentially combines different streams of potentially identifiable cryptoassets, which improves the anonymity of transactions, thus making the cryptoasset harder to trace.[670]

Subsequently, El Salvador recently passed the Bitcoin Law in a global first, which created a new legal framework designed to integrate Bitcoin into everything from the local banking and financial systems to everyday economic transactions.[671] President Nayib Bukele sponsored the law. The move sets the framework for a nation to create a bimonetary system using Bitcoin,[672] which all sectors in El Salvador must accept. Here, the rationale behind the adoption of Bitcoin is two-fold: firstly, only 30% of the adult population has access to a bank

[666] Vildana Hajric, "DeFi Crash Accelerates With Some Once-Hot Investments Losing 50%" (Bloomberg, 18 June 2021) <https://www.bloomberg.com/news/articles/2021-06-18/defi-crash-accelerates-with-some-once-hot-investments-losing-50> accessed 31 August 2021.

[667] Clifford Chance, "Non-fungible Tokens: The Global Legal Impact" (Clifford Chance, June 2021) <https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2021/06/non-fungible-tokens-the-global-legal-impact.pdf> accessed 31 August 2021.

[668] MyCryptoMixer, "Bitcoin Mixer" (MyCryptoMixer, 2021) <https://mycryptomixer.com/> accessed 24 June 2021.

[669] Ethereum, "Is there any Ether mixer / tumbler available?" (Ethereum, 8 September 2016) <https://ethereum.stackexchange.com/questions/2699/is-there-any-ether-mixer-tumbler-available> accessed 24 June 2021.

[670] MyCryptoMixer, "MyCryptoMixer.com: How to mix your coins using the best bitcoin mixer (tumbler) in 2020" (Bitcoin Magazine, 3 August 2020) <https://bitcoinmagazine.com/culture/mycryptomixer-com-how-to-mix-your-coins-using-the-best-bitcoin-mixer-tumbler-in-2020> accessed 31 August 2021.

[671] Neal Freyman, "El Salvador moves to make bitcoin legal tender. It would become the first country to formally adopt the cryptocurrency as part of its economy" (Business Insider, 7 June 2021) <https://www.businessinsider.com/el-salvador-moves-to-adopt-bitcoin-as-legal-tender-2021-6?utm_campaign=sf-bi-finance&utm_source=facebook.com&utm_medium=social&fbclid=IwAR03qy2-DLfupuDFFGRK5zA5swEJq8XSWFTVtpyF0-uPKeU4-VcIKdDyUvQ&r=US&IR=T?utm_source=copy-link&utm_medium=referral&utm_content=topbar> accessed 31 August 2021..

[672] The US dollar will remain the primary currency, whilst Bitcoin will be the secondary currency.

account; and secondly, the remittance rate from El Salvadorean national living abroad account for roughly 25% of GDP.[673] What does this mean for crypto money laundering? Here, the implementation and enforcement remain an open question, as there will be certain risks surrounding the use of Bitcoin by criminal actors, and whether El Salvador's Bitcoinisation will become a broader trend? It is submitted that this trend is unlikely to prompt large economies to consider adding cryptoassets as a legal tender seriously; nonetheless, as more such examples arise, the more complex the potential impact, especially concerning money laundering and terrorist financing. Notwithstanding El Salvador's recent adoption of Bitcoin as a legal tender, there is still a lively debate on whether cryptoassets can constitute "money" alongside recognised national currencies.[674]

Thus, the FCA should provide more guidance in relation to oversee transactions, sanctions screening, and its reporting requirements (similar to reporting requirements for cash transactions or cross-border transactions).[675] An AML/KYC compliant firm would reduce crypto money laundering risks by minimising the ability to transact anonymously, and in turn, assist law enforcement in their investigations. However, the case law in relation to crypto money laundering is underdeveloped.

A review of the relevant case law:

Following *AA v Persons Unknown*,[676] the Commercial Court has allowed a hearing of a UK insurance company's (the Insurer) application for an urgent injunction relief concerning an incident following a cyberattack, which prevented a Canadian company (the policyholder) from accessing its IT systems. The hackers demanded 109.25 Bitcoin in ransom, and in exchange,

[673] Michael McDonald and Matthew Bristow, "El Salvador's Bitcoin Bombshell: What does it mean?" (Bloomberg News, 9 June 2021) <https://www.bloomberg.com/news/articles/2021-06-09/el-salvador-s-bitcoin-bombshell-what-does-it-mean-quicktake> accessed 31 August 2021.

[674] Sarah Green, "It's virtually money" in David Fox and Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (Oxford University Press 2019).

[675] Adam Samson and Philip Stafford, "Financial watchdog bans crypto exchange Binance from UK" (Financial Times, 27 June 2021) <https://www.ft.com/content/8bc0e5e0-2705-496d-a265-acccaffaee87> accessed 31 August 2021.

[676] [2019] EWHC 3556 (Comm).

the company will regain access to its IT system .[677] After the ransom had been transferred to the digital wallet, the insurance company hired consultants who traced the Bitcoin transfer to a crypto account linked to an exchange called Bitfinex, a company based in Hong Kong and registered in the British Virgin Islands.[678] Whilst 13.25 Bitcoins dissipated, 96 Bitcoins remained in the account, which prompted the insurance company to seek a proprietary injunction to recover the Bitcoins. The hackers had demanded and subsequently held and controlled the Bitcoins. In short, the hackers were in possession of property belonging to the applicants or for wrongfully extorting it. However, in order to grant the proprietary injunction, the court had to consider whether cryptoasset constituted a form of property capable of being the subject of such an injunction. Previously, the court has already considered cryptoassets as 'property' by granting a worldwide freezing order[679] as well as an asset preservation order. However, until *AA v Persons Unknown*,[680] the court had not considered the issue in depth, thus following the UK's Jurisdictional Taskforce's Legal Statement on Cryptoassets and Smart Contracts.[681] The Commercial Court granted a proprietary injunction concerning the relevant Bitcoin property and permitted service out of the jurisdiction to reclaim the 96 Bitcoins which remained in the account. The court provided the following rationale: the Insurer had paid out the sum of $950,00, which was used to purchase the Bitcoin, and this property belonged to the Insurer.[682] Subsequently, the proceeds of that money can be traced into the account held with Bitfinex. As a result, those Bitcoins are being stored by Bitfinex as a constructive trustee on behalf of the Insurer or the Insurer has a restitutionary claim against the defendants who are in possession of the property which belongs to the Insurer.[683] Here, the defendants, who are the account holders of the crypto account, have wrongfully extorted that money from the Insurer, thus have no rights over the relevant property.[684]

---

[677] Jenna Rennie and Gwen Wackwitz, "Recovering the ransom: High Court confirms Bitcoin status as property" (White and Case, 10 February 2020) <https://www.whitecase.com/publications/alert/recovering-ransom-high-court-confirms-bitcoin-status-property> accessed 31 August 2021.

[678] John Metais, "Profile: Bitfinex" (Coindesk, 2021) <https://www.coindesk.com/company/bitfinex> accessed 31 August 2021.

[679] Vorotyntseva v Money-4 Limited [2018] EWHC 2596.

[680] [2019] EWHC 3556 (Comm).

[681] Supra (n 6) UK Jurisdictional Taskforce.

[682] AA v Persons Unknown [2020] CLY 236 (Final Judgment).

[683] ibid.

[684] ibid.

The court deliberated on the reasonable cause of action concerning the precise terms of the Insurer's claim are being sought under restitution or as a constructive trustee to recover and take a proprietary claim over the relevant property in the crypto account held by the defendants.[685] However, the court noted that on '*prima facie*', there is difficulty treating cryptoasset as a form of property since they are neither chose in possession nor chose in action. English law only views property as being only two kinds. On the one hand, the former underlines the premise that cryptoassets are not choses in possession because they are virtual assets, thus not tangible and cannot be possessed.[686] On the other hand, the latter prescribes that cryptoassets do not embody any right capable of being enforced by action, hence not choses in action.[687] In *Colonial Bank v Whinney*,[688] Lord Justice Fry underlines: "*all personal things are either possession or action. The law knows no tertium quid between the two*".[689] Following traditional English law, cryptoassets could not be classified as a form of property, subject to a proprietary injunction or a worldwide freezing injunction. However, following recent judgments in *Vorotyntseva v Money-4 Limited*[690] and *Robertson v Persons Unknown,*[691] coupled with the detailed consideration by the UK Jurisdictional Task Force concerning the proprietary status of cryptoassets. In *AA v Persons Unknown*, the court held that[692] it considered the statement provided by the UK Jurisdictional Task Force, thus the proprietary status of cryptoassets is compelling and should be established by English Courts. Nonetheless, cryptoassets do not sit neatly within the existing categories following traditional property law principles; however, *AA v Persons Unknown* showed the ability of the common law to stretch traditional definitions and legal principles to include new technologies. For instance, in *Armstrong DLW GmbH v Winnington Networks Ltd*,[693] the court held that an EU carbon emissions allowance can be classified as intangible property (even though it was neither a thing in possession nor a thing in action) and could be subject to a tracing claim under English law.

[685] ibid.
[686] ibid.
[687] ibid.
[688] [1885] 30 Ch.D 261.
[689] ibid.
[690] [2018] EWHC 2596.
[691] (unreported).
[692] [2019] EWHC 3556 (Common); [2020] C.L.Y. 362 (Final Judgment).
[693] [2012] EWHC 10.

More importantly, several important statutes in the UK, such as the Law of Property Act 1925, the POCA, the Theft Act 1968 and the Fraud Act 2006, all assume intangible property are not limited to things in action, and thus, include "other intangible property". In this vein, these statutes essentially extend the traditional definition of property to adopt new business practices and show no conceptual or legal difficulty in treating intangible things as property even when the object is not a thing in action. In addition, the Patents Act 1977, section 30 underlines that a patent or patent application "is a personal property (without a thing in action)". The statute essentially recognised that personal property could include things other than possessions and things in action. As a result, *AA v Persons Unknown* concluded that a "*…cryptoasset might not be a thing in action on the narrower definition of that term does not in itself mean that it cannot be treated as property*".[694] Hence, the Courts will have no difficulty in treating cryptoassets, a novel kind of intangible assets, as property as per English law. Subsequently, the court confirmed that a cryptoasset, such as Bitcoin, can meet the four criteria set out in Lord Wilberforce's classic property definition. Thus, following *National Provincial Bank v Ainsworth,*[695] the property must be: [1] definable, [2] identifiable by third parties, [3] capable of assumption by third parties, and [4] having some degree of permanence. In support of this test, other common jurisdictions, such as the Singapore International Commercial Court, have confirmed that cryptoassets are be treated as property, can be the subject of a trust. [696] In other words, cryptoassets have satisfied the three elements of a trust: certainty of intention, the certainty of subject matter, and certainty of objects.[697] In this case, the Singapore International Commercial Court was satisfied that cryptoassets had met all the requirements of a property right. In *Ainsworth*, it was held that: "*[c]rypto[assets] are not legal tender in the sense of being a regulated currency issued by a government but do have the fundamental characteristic of intangible property as being an identifiable thing of value*".[698] A newsletter published by Norton Rose Fulbright, states that, *"[c]ourts from Ohio to California to South Korea have handed down decisions finding crypto[assets] to be property. In China, despite a ban on initial*

[694] AA v Persons Unknown [2020] C.L.Y. 362 (Final Judgment).
[695] [1965] 1 AC 1175.
[696] B2C2 Limited v Quoine PTE Limited [2019] SGHC (I) 3.
[697] ibid.
[698] ibid.

coin offers, crypto exchanges and Bitcoin mining, some courts and tribunals have held crypto[assets] to be property".[699]

Moreover, *AA v Persons Unknown* underlined the applicable principles concerning the concept of proprietary injunction regarding stolen cryptoassets. When the relevant crypto-property is obtained by fraud, equity imposes a constructive trust on the fraudster's crypto account;[700] and in turn, the relevant cryptoasset will be traceable in equity.[701] As a result, a serious crime must be tried; subsequently, the court must consider whether damages are an adequate remedy concerning the merits of the proposed claim, and more importantly, to the level required for a proprietary injunction over the relevant cryptoasset. Here, the appropriate Bitcoin was paid as part of a ransom following a cyberattack on an insurance company. As a result, a claim was made for an injunction order in terms of a constructive trust and restitutionary claims concerning the loss in money used to purchase the Bitcoin, which was subsequently traced to a digital account kept by Bitfinex. Unfortunately, Bitfinex does not know the identity of its account holders.

Nonetheless, it was asserted that it was essential to assist those who had suffered blackmail and extortion and not deter from the court. More importantly, extortion, as well as blackmail, was essentially a misuse of free speech, as outlined in *LJY v Persons Unknown*,[702] which tempered the interests of justice and freedom of expression, as per section 12 of the Human Rights Act 1998.[703]As a result, Mr Justice Bryan, in *AA v Persons Unknown*, was satisfied that the application regarding the possession of property belonging to the Insurer and wrongfully extorting it was property made. Mr Justice Bryan accepted the Insurer's submissions and granted proprietary injunctions against all defendants concerning the relevant cryptoasset. Here, he considered a cryptoasset such as Bitcoin, a form of property capable of being subject

[699] Norton Rose Fulbright, "Singapore court's cryptocurrency decision: Implications for cryptocurrency trading, smart contracts and AI" (Norton Rose Fulbright, September 2019) <https://www.nortonrosefulbright.com/en-nl/knowledge/publications/6a118f69/singapore-courts-cryptocurrency-decision-implications-for-trading-smart-contracts-and-ai> accessed 31 August 2021.

[700] Westdeutsche Landesbank v Islington LBC [1996 AC 669.

[701] Poly Peck International PLC v Nadir (No. 2) [1992] 4 All ER 769.

[702] [2017] EWHC 3230 (QB).

[703] PML v Persons Unknown [2018] EWHC 838 (QB).

to a proprietary injunction, thus reconfirming the UK Jurisdictional Taskforce's Legal Statement on Cryptoassets and Smart Contracts.

In order to address the challenges concerning the increased use of cryptoassets in high-end money laundering, the Fifth Money Laundering Directive included cryptoassets providers and other crypto firms under the Money Laundering Regulation by introducing a national register of bank account ownership.[704] The FCA are the official AML/CFT supervisor of crypto firms by which to present the implementation of the travel rule and KYC/AML compliance in the UK for relevant crypto firms. It is submitted that the strict regulatory approach or "robust" assessment, as adopted by the FCA, is counterproductive as substantial funds may continue to be laundered through unregulated platforms and foreign crypto companies illegally operating the UK. Here, crypto firms cannot operate in the UK unless the business falls within the scope of the "Temporary Registration Regime" (TRR) or received full approval from the FCA. As of June 2021, only 5 crypto firms received this designation. Due to slow registration rates, the FCA announced an extension to the TRR, from the 9th of July 2021 to the 31st of March 2022.[705] Thus, as of March 2022, crypto exchanges and wallet providers will not be permitted to undertake any regulated activity in the UK, unless it receives approval from the FCA to engage in regulated activities. As a result, crypto exchanges and wallet providers will fall within the scope of Schedule 9 of the POCA, since the business is in a regulated sector, supervised by the FCA.

Money laundering regulation: Implications for Crypto firms

Following the implementation of the Fifth Money Laundering Directive, crypto-exchange providers, as well as custodian wallet providers, have specific disclosure as well as reporting obligations. The MLR essentially backs up the money laundering and terrorist financing provisions in the POCA and the Terrorism Act 2000. As examined in Chapter 4, titled: "Criminal Prescription", the POCA criminalises both the active money laundering offences, as per section 327 "*Concealing offence*", section 328 "*Arranging offence*" and section

[704] Supra (n 663) HM Government.

[705] Financial Conduct Authority, "Temporary Registration Regime extended for cryptoasset businesses" (FCA, 3 June 2021) <https://www.fca.org.uk/news/press-releases/temporary-registration-regime-extended-cryptoasset-businesses> accessed 31 August 2021.

329, "*Acquisition, use and possession offence*" of the POCA, failing to report or disclose its knowledge or suspicion of money launderings to the relevant authorities,[706] such as the crypto firm's internal money laundering reporting officer or the NCA or the FCA. Section 330 of the POCA outlines criminal and civil penalties regarding the failure to disclose or report their knowledge or suspicion of money laundering concerning a customer's activities or account transactions. To prove an offence under section 330, the prosecution must demonstrate: [1] that the property was criminal property; and [2] that the firm either: a) knew or suspected the relevant property was criminal property; or b) ought to have a reasonable suspicion that the relevant property was criminal property. It is important to note, the threshold required for "reasonable suspicion" as per section 330 is different from active money laundering offences (sections 327-329, POCA). The common law concepts concerning "know and suspect" was covered in detail in Chapter 4. However, section 330 of the POCA introduces the element of "having reasonable grounds for suspecting", which underlines a negligence standard; thus, different from active money laundering offences. In other words, the standard is higher for a section 330 offence than the "know and suspect" requirement as prescribed in active money laundering offences, as per sections 327-329 of the POCA.

Following the above, a crypto firm or employee can commit a section 330 offence despite not personally knowing or suspecting any wrongdoing, but simply because the crypto firm was negligent by not suspecting and reporting the alleged laundering. The reason for this negligence standard is due to the assertion that a business in the regulated sector, following Schedule 9 of the POCA, are deemed to be "crypto" professionals and are expected to exercise a higher degree of care and diligence when carrying out their day-to-day activities, than for instance an ordinary person or a front-line criminal. More importantly, there are no safe harbour examples in the common law concerning what is considered "reasonable grounds for suspecting" within the crypto context. As indicated in the previous section, as of March 2022 crypto exchanges and wallet providers must be approved by the FCA, in order to undertake its regulated activity in the UK. Thus, drawing on a legal sector example, *SRA v Olayemi Daniel*[707] and *SRA v Tidd.*[708] The Solicitors Disciplinary Tribunal views money laundering as a serious

[706] POCA, s 330.
[707] [2015] 11343-2015.
[708] [2013] 11178-2013.

crime resulting in severe penalties (suspension or strike-off), even when the individuals within the regulated sector were naïve and received no personal gain.[709] Within the crypto context, the FCA is the supervisory authority, and the FCA has a statutory duty under the MLR to effectively monitor crypto firms. Thus, it is prudent for a crypto firm to ensure employees receive AML training. Following Schedule 9, the POCA, crypto firms and its employees are the gatekeepers of the market and must prevent the crypto sector from being used as a vehicle for crime.

A crypto-firm or employee will commit on an offence under section 330 of the POCA if the employee has reasonable grounds for suspecting that a client is involved in money laundering and the employee does not make disclosure under the POCA to the nominated officer or the NCA or the FCA. All the evidence must be presented to the criminal standard, and the burden of proof rest with the prosecution. As mentioned in the previous paragraph, "having reasonable grounds for suspecting" presents a negligence standard, which differs from the active money laundering offences, as outlined in sections 327-329. Subsequently, to commit an offence, the information must derive from the day-to-day activities of the crypto firm, thus not through the employee's private capacity. In practical terms, due to the negligence standard, it is prudent for an employee to report any suspicious behaviour because simply relying on the defence of "lack of knowledge" might seem a risky option since, as a regulated firm, crypto employees are deemed to be "crypto" professionals and are expected to exercise a higher degree of care and diligence in carrying out their day-to-day activities. However, as a new sector, crypto firms must create its own AML system, and are thus, inexperience on how the law should be applied, whilst the financial sector understand the law and its experience derived from decisions issued by the Court on how banking regulations should be applied.[710] For the crypto sector, the consequence for its inexperience are immense; for instance, if the crypto firm or its employee fails to report a suspicious transaction, as per the POCA, to the nominated officer or the NCA or the FCA; the maximum sentence following a conviction under section 330 is five years imprisonment. In addition, civil penalties are also available under the MLR, such as [1]

[709] Solicitors Regulation Authority, "Anti Money Laundering Report" (Solicitor Regulation Authority, May 2016) <https://www.sra.org.uk/globalassets/documents/sra/research/anti-money-laundering-report.pdf?version=4a1ab0> accessed 31 August 2021.

[710] MLR 2017, Regulation 24.

fines,[711] [2] suspension and removal of authorisation,[712] [3] prohibition on senior managers,[713] and [4] injunctions.[714]

Following MLR, injunctions, as mentioned above (such as Freezing Orders (domestic freezing order) or Worldwide Freezing Orders), are discretionary and may be granted as an interim or final remedy. As a result, an exhaustive list concerning the circumstances in which an English court may grant an injunctive relief would be extensive given the breadth of the court's discretionary powers.[715] In this vein, a freezing order is normally an interim injunction that prevents the defendant(s) (or respondent(s)) from disposing of or dealing with the alleged criminal property. As per section 37 of the Senior Courts Act 1981, injunctions may be granted "*in all cases in which it appears to the Court to be just and convenient to do so*". [716] Subsequently, section 25 of the Civil Jurisdiction and Judgments Act 1982 also empowers English courts to grant interim injunctions, such as a Worldwide Freezing Orders, concerning assets held abroad. In short, injunctions may be granted as either [1] a final relief, awarded at the conclusion of a trial; or [2] an interim relief, granted prior to the commencement of or during a proceeding.[717] Subsequently, the foundation for an interim relief remains whether the grant of the injunction would be considered "just and convenient", and more importantly, the court must maintain a fair balance between the untested rights of the parties pending trial.[718] Here, the case of *American Cyanamid Co (No 1) v Ethicon Ltd*[719] provides an essential test in relation to the threshold[720] in which an interim injunction would be granted. In this vein, the court must establish that there is a serious question to be tried, and if so, it must consider the balance of convenience. The former underlines whether there is an issue for which there is sufficient evidence establishing a case.[721] The latter emphasises that the court must consider the particular

[711] MLR 2017, Regulation 76.

[712] MLR 2017, Regulation 77.

[713] MLR 2017, Regulation 78.

[714] MLR 2017, Regulation 80.

[715] Examples of injunctions: freezing injunctions, disclosure orders, search orders, proprietary injunctions, etc.

[716] Senior Courts Act 1981, s 37

[717] John Sorabji, "Interim relief: National report for England and Wales" (2018) 20 Flinders Law Journal 1.

[718] Senior Courts Act 1981, s 37.

[719] [1975] UKHL 1.

[720] In short, the threshold qualifications to American Cyanamid are essentially that the interim injunction must not dispose of the final proceedings.

[721] Cayne v Global Natural Resources Plc [1984] 1 All ER 225.

factual circumstances in which the interim injunction is being sought. Here, the court must consider the merits of the case then assess what measures are required to preserve the status quo.[722] For instance, in *Ion Science Ltd v Persons Unknown,*[723] Mr Justice Butcher was satisfied that there was a serious issue to be tried. Subsequently, he considered the balance of convenience was in favour of granting an interim injunction since there was a prima facie case of wrongdoing. As a result, the court in *Ion Science Ltd* applied the principles set out in *American Cyanamid* since it was just and convenient to grant the injunction as it appeared that the applicant had been the victim of fraud.

Criminal Property

Here, if the relevant property is deemed to be criminal property, deriving from the proceeds of crime, Part 5 of POCA sets out freezing orders and outlines the process in which the court can administer the recovery of criminal property, through mechanisms such as recover orders, interim receiving orders, and prohibitory orders. More importantly, recovery orders can be sought concerning any property, whether or not criminal proceedings have been commenced.[724] Although this seems straightforward, the 'recoverable property' must derive from unlawful conduct. For instance, a token has been disposed of or sent to another digital wallet. Traditionally, law enforcement would follow the relevant property and recover it from that person. The difficulty here is that if, for instance, the client sends the relevant digital asset to an unhosted wallet or a bitcoin mixer, then the token may not be identifiable, and the applicable property cannot be followed by law enforcement. Subsequently, the recovery will depend on whether the property continues to be identifiable. Thus, if the token exchanges hands and is traced to a DeFi protocol with no identifiable host or creator, it will be questionable whether the relevant property continues to be identifiable. More importantly, it is questionable whether law enforcement can retrieve the applicable property from a computer code with no human agency.

[722] Series 5 Software Ltd v Clarke [1996] 1 ALL ER 853.

[723] Rahman Ravelli, "Cryptocurrency Fraud: A Significant Judgment" (Legal 500, 9 February 2021) <https://www.legal500.com/developments/thought-leadership/cryptocurrency-fraud-a-significant-judgement/> accessed 31 August 2021.

[724] POCA, s240(1)(a).

Following *Serious Organised Crime Agency v Perry,*[725] recovery orders could only be made in relation to property based within the UK. As seen in *AA v Persons Unknown,* the court can make orders in circumstances where the relevant property is based abroad. However, there must be an established connection between the relevant property and the UK. The court can grant international recovery orders.[726] For crypto-firms, law enforcement may also serve a property freezing order to freeze the relevant property held in a client's account before any conviction is secured and the subsequent forfeiture of cryptoassets held in a client account recoverable.[727] After that, depending on whether the criminal property is identifiable, law enforcement can seek all or part of the relevant cryptoassets held in the account.[728] However, there must be reasonable grounds for the court to make an order for suspecting that the relevant cryptoasset in the account is intended for unlawful use or that the criminal property is identifiable and thus recoverable property. More troubling is that an account forfeiture notice must be given to the interested parties, such as the account holder, the crypto exchange, or the wallet provider.[729] However, for instance, UniSwap, a peer-to-peer protocol, the creators of the platform are anonymous. How will law enforcement serve an account forfeiture note to the interested parties when the host is unknown and the relevant cryptoassets are held via smart contract.

For instance, in *AA v Persons Unknown,* the 96 Bitcoin were sent to an account linked to an exchange known as Bitfinex; the exchange might have the information concerning the identity of the defendants via the company's KYC anti-money laundering requirement. Here, the application for a POCA, s241, and s304 to s310 freezing injunction, over the 96 Bitcoins, the application is made ex parte on notice,[730] and Bitfinex, the exchange was notified of this application. In this case, the exchange became the holders of the Insurer's property. As a result, there are claims against the exchange for restitution or constructive trustees to the criminal property. However, as the law within the crypto space is still developing, it is uncertain whether the claims against the exchange can be deemed a Bankers Trust order or a Norwich Pharmacal

[725] [2012] UKSC 350.
[726] POCA, 282A.
[727] POCA, s241, 304 to 310.
[728] POCA, s303Z1(5).
[729] POCA 303z10, POCA.
[730] POCA 303z10, POCA.

order ("NPO") requiring the Exchange to provide specified information concerning an account held by the hackers. A Norwich Pharmacal order was established in the House of Lords' decision in *Norwich Pharmacal v Commissioner of Customs & Excise,*[731] which is essentially a disclosure order where wrongdoing has occurred, and a third party has information concerning the identity of the wrongdoer.[732] In *AA v Persons Unknown,* the court acknowledged that a Bankers Trust or a Norwich Pharmacal order must be served to the Exchange to provide the specific information concerning the crypto account held by the hackers. An NPO can obtain information to enable the Insurer to plead its case against the hackers and thus bring a proprietary claim regarding Bitcoins held in the account. The Insurer must prove a good arguable case concerning the hackers' wrongdoing. The order must be deemed necessary in the interest of justice, thus not sought for an improper purpose. However, it is unclear whether an NPO can be obtained against a third party in a foreign jurisdiction. For instance, it is uncertain whether Bitfinex, a company registered in Hong Kong, has to disclose information to applicants based in the UK.

The crypto disruption is a global issue because the technology is borderless and does not respect domestic or international AML laws, nor does it have to accept the rules surrounding jurisdiction. For instance, El Salvador became the first country to officially recognise bitcoin as a legal tender primary because of the borderless nature of cryptoassets. The remittance rate from El Salvadorean national living abroad accounts for roughly 25% of GDP.[733] Due to this international element, UK applicants, as per an NPO or Bankers Trust order, may face potential difficulties obtaining a disclosure order when the third-party respondent(s) are based outside of the jurisdiction of the UK. Nonetheless, as seen in *AA v Persons Unknown,* the court has exercised its discretion to grant permission to serve an NPO outside the jurisdiction of the UK. Subsequently, *Ion Science Ltd v Persons Unknown* granted the UK's first extraterritorial Bankers Trust Order against Binance Holdings Limited.[734] However, there is considerable

[731] [1974] UKHL 6.

[732] In Norwich Pharmacal v Commissioner of Customs & Excise, Lord Reid stated the following in relation to the jurisdiction of NPOs "*...that if through no fault of his own a person gets mixed up in the tortious acts of others so as to facilitate their wrongdoing he may incur no personal liability but he comes under a duty to assist the person who has been wronged by giving him full information and disclosing the identity of the wrongdoers*".

[733] Supra (n 675) McDonald and Bristow

[734] Supra (n 725) Ravelli.

scepticism about whether UK applicants can serve a successful NPO or Bankers Trust Order to a foreign third party, as seen in *AB Bank Ltd v Abu Commercial Bank PJSC.*[735] Thus, the law in this area remains unclear. As a general rule, English Courts must not make an order for disclosure (Bankers Trust order or a NPO) in relation to foreign respondents when doing so oversteps or infringes on the sovereignty of another state. For instance, Bitfinex in *AA v Persons Unknown,* have not yet had an opportunity to address the court, thus whether the Bitfinex will comply with the UK disclosure orders and whether the Bitfinex will allow UK law enforcement to freeze and demand forfeiture of the cryptoassets held in the foreign crypto account, remains unclear.[736] For instance, in *McKinnon v Donaldson Lufkin and Jenrette Securities Corp,*[737] the court discharged an NPO on the basis that the relevant third party respondent was a foreign bank, and underling that "*save in exceptional circumstances, the court should not require a foreigner who was not a party to an action, and in particular, a foreign bank which would owe a duty of confidence to its customers regulated by the law of the country where the customer's account was kept, to produce documents outside the jurisdiction concerning business transacted outside the jurisdiction*".

As a result, the law in this area remains unclear. More importantly, whether a non-UK company will comply with a foreign disclosure order and/or a worldwide freezing order will depend on the company and the jurisdiction in which the relevant exchange or wallet provider is located. For instance, in *Sabados v Facebook Ireland,*[738] the High Court granted an NPO requiring Facebook Ireland to disclose the appropriate identification of the person unknown who had requested the deletion of the deceased's Facebook profile. Following *Bacon v Automattic Inc,*[739] the court acknowledged that the basis of distress took place in the UK concerning Facebook Ireland's deletion of a deceased's Facebook profile. Here, High Court held that there was an arguable case, and the courts of England and Wales had jurisdiction to make the NPO since the alleged damage was primarily suffered in the UK.[740] However, Facebook did not acknowledge the NPO, and thus, were not present at the hearing. In theory,

[735] [2016] EWHC 2082.
[736] POCA, s 241 and s304-310.
[737] [1986] Ch 484.
[738] [2018] EWHC 2369.
[739] [2011] EWHC 1072 (QB).
[740] Lockton Companies International v Persons Unknown [2009] EWHC 3423.

the court can serve NPO to foreign respondents purely because the alleged unlawful conduct occurred in the UK. In practice, the foreign third-party respondent(s) are more likely to be based in a crypto-friendly jurisdiction with no connection to the UK. As a result, following the Facebook Ireland case, a foreign crypto exchange or wallet provider may decide not to acknowledge the High Court's NPO. More importantly, since Facebook Ireland was foreign third-party respondent thus not held in contempt of court. As such, not observe the court's proprietary or freezing injunction over the relevant criminal property. It is submitted that UK courts must have real grounds to exercise their exorbitant jurisdiction on foreign third-party respondents. Thus, a foreign crypto firm must voluntarily decide whether it would accept the UK court's jurisdiction. Nonetheless, an NPO is essential because it allows law enforcement to obtain information concerning the digital assets held by a criminal. In turn, it will enable those assets to be traced and recovered.

Subsequently, NPOs or Bankers Trust Orders are straightforward when the applicant and the respondent(s) are based in the UK. It is generally accepted that the UK courts would not hesitate to make NPOs or Bankers Trust Orders ascertain and prevent unlawful property disposal. More importantly, the court has an equitable jurisdiction over cases involving allegations of fraud, money laundering or proprietary claims.[741] For instance, in *BDW Trading Ltd v Fitzpatrick and another,*[742] the applicant had a proprietary claim over the relevant criminal property received by the third-party respondents via fraud. The court oversaw the NPO and the freezing order, which required the third-party respondents to disclose information concerning the relevant criminal property.[743] Following *BDW Trading Ltd v Fitzpatrick and another*,[744] it is established that UK respondents must assist law enforcement on the tracing exercise, which allows the applicant to identify assets in the hands of a fraudster or a hacker (i.e. the defendant(s)) or a third party).

[741] Murphy v Murphy [1999] 1 WLR 282.
[742] [1989] WLR 656.
[743] Arab Monetary Fund v Hashim (No 8) [1989] WLR 565.
[744] [1989] WLR 656.

Crypto following and tracing rules

This section will examine the common law tracing rules and tracing in equity, allowing Banker Trust Orders or NPOs applicants to identify assets in the hands of a fraudster or a hacker (i.e. the defendant(s)) or a third party. More importantly, this section considers challenges surrounding the seizure of illegal assets within the crypto space. The technology is borderless and does not respect domestic or international AML laws, nor does it have to accept the rules surrounding jurisdiction. Notwithstanding these challenges concerning foreign respondents or defendants, the common law has long been established the following and tracing rules used to locate and identify assets that have been misappropriated.[745] The rightful claimant may assert their proprietary interest over the relevant property in the UK and seek a court-sanctioned remedy to recover the relevant property. In this vein, this section will examine the UK's common law tracing rules and the rules of following and tracing in equity. Here, following and tracing are an evidential process used to establish the legal basis for a claim over the relevant property or misappropriated property.[746] As a result, the rules of following and tracing enable the claimants to identify what happened to that relevant property, thus resolving the evidential inconsistencies that can arise concerning the relevant property, which has moved from hand to hand.[747]

The relevant authority concerning the UK's following and tracing processes was reconfirmed in *Foskett v McKeown*.[748] In this case, the fraudster took GBP 20,440 from the claimants and used it to purchase 40 per cent of his life insurance premiums, and he subsequently committed suicide. The relevant life insurance policy was approximately GBP 1 million. The claimants appealed against the initial decision, which granted a refund of GBP 20,440 plus interest. The House of Lords held that the claimants had a proprietary right to receive 40% of the life insurance policy. In this case, there was a direct link between the misappropriated funds and the insurance policy; thus, the equitable interests of the claimants

[745] Shyamkrishna Balganesh, "Common Law Property Metaphors on the Internet: The real problem with the doctrine of Cybertrespass" (2006) 12 Michigan Telecommunications and Technology Review 265.

[746] James Edelman, "Understanding Tracing Rules" (2016) 16 QUT Law review 2.

[747] Ehi Eric Esoimeme, "Institutionalising the war against corruption: new approaches to assets tracing and recovery" (2020) 27 Journal of Financial Crime 1.

[748] [2001] 1 AC 102.

were directly traceable to the insurance policy. Subsequently, by enforcing their property rights over the relevant insurance policy, the claimants received 40% of the life insurance policy. As a result, the legal concept of following and tracing was held to be distinct processes. On the one hand, following the relevant property in which the claimant has a proprietary interest, which establishes the appropriate location to reclaim the property. On the other hand, tracing goes further and undercovers where the misappropriated property has been used to purchase a new identifiable property. Here, the claimant must establish that the other identifiable asset was acquired through a series of transactional links to claim a proprietary interest over the new identifiable asset.[749] In order words, tracing essentially identifies a new asset as being the substitute for the original asset in which the claimant had a proprietary interest. As a result, it enables the claimant to assert a proprietary claim over the new asset.

Within the crypto context, the traditional legal rules concerning following and tracing can be used to establish a proprietary interest over a relevant cryptoasset that has been misappropriated or derived from proceeds of crime.[750] For instance, following and tracing can be used to evidence the proprietary interest as the misappropriated property moves from hand to hand. However, a claimant cannot follow an asset if that original asset no longer exists because the original property has been destroyed, dissipated, or mixed with other assets.[751] In the context of crypto, a property is deemed to have been destroyed when the original token has lost its identity or is combined with another asset. For instance, a misappropriated Ether may be used to create a decentralised protocol; as a result, the original Ether may be destroyed or dissipated or mixed with other assets locked into the new decentralised platform. However, if the use of the Ether can be identified in and shown to form a substantial part of the new decentralised platform, and the protocol is indivisible, the claimant can follow into and recover the new asset. In practice, it is unlikely that a decentralised platform will be identifiable since the original Ether has been consumed, thus destroyed or dissipated or mixed with other assets to create the new decentralised platform.[752]

[749] OJSC Oil Company Yugraneft v Abramovich [2008] EWHC 2613 (Comm).

[750] Supra (n 79) Fox.

[751] Borden (UK) Ltd v Scottish Timber Products Ltd [1981] Ch 25.

[752] Doug Shipp, "Blockchain & Ethereum: Welcome to the Decentralised Internet" (Atomic Ojbect, 12 December 2020) <https://spin.atomicobject.com/2020/12/12/blockchain-ethereum-decentralized/> accessed 31 August 2021.

For instance, two misappropriated CryptoKitties was then used to breed a new offspring, essentially a new CryptoKitty token.[753] The original owner of the misappropriated tokens will be entitled to recover the original tokens and *perhaps* the new token,[754] created via breeding. Here, the claimant may be permitted to follow her property into a new digital asset; however, this assertion has not been tested.[755] As a result, it will not always be easy to determine whether a relevant cryptoasset can be followed or traced. The law in this space is still developing, and everyday new cryptoassets are being created with different functionalities that do not fit into traditional property assumptions. Thus, it is not always easy to determine whether a misappropriated cryptoasset has ceased to exist when mixed with other assets, thus losing its original identity. Nonetheless, established legal rules can be used as guidance, and in general, a claimant must establish a proprietary interest over the relevant cryptoasset when the defendant misappropriated the token. In other words, "…*the claimant succeeds at all by virtue of his own title and not reverse unjust enrichment. Property rights are determined by fixed rules and settled principles. They are not discretionary*".[756] In short, a successful claimant must establish that they had a proprietary interest in the relevant cryptoasset at the time of it was transferred or received by the defendant.

Conceptually, English Courts have the equitable jurisdiction to make a Banker Trust Orders or NPO for disclosure to be mandated in order to assist a claimant in tracing and to protect the claimant's proprietary interest in the relevant cryptoasset.[757] Nonetheless, there are separate rules for tracing at common law and in equity. Here, the latter rules are generally more flexible and favourable to a claimant if the claimant is entitled to rely on equitable rules. Thus, equitable tracing is generally more favourable to a claimant than common law tracing (as discussed in the previous section). In equity, the claimant can trace through a mixed fund; however, there must be a fiduciary relationship (between the claimant and defendant) in order

[753] CryptoKitties, "Getting Started: Breeding" (CryptoKittes, 2021) <https://guide.cryptokitties.co/guide/getting-started> accessed 31 August 2021.

[754] Foskett v McKeown [2001] 1 AC 102.

[755] Glencore International AG v Metro Trading Inc (No 2) [2001] 1 Lloyd's Rep 284.

[756] Foskett v McKeown [2001] 1 AC 102 at 127.

[757] Cpod SA v de Holanda Jr [2020] EWHC 1247 (Ch).

to commence the equitable tracing process.[758] In short, equitable rules only apply when the claimant's proprietary interest over the relevant property is equitable. By contrast, the common law tracing rules applies when the claimant has legal title over the relevant asset.[759] In short, the legal title carries all the rights concerning the claimant's proprietary interest over the relevant property. However, the common law cannot trace through a mixed substitution. In order words, the common law can only trace into substitution, whereby the original property was used exclusively to acquire the substituted property. For instance, if GBP 10,000 was misappropriated and used to purchase GBP 10,000 worth of Ether, the GBP 10,000 can be traced directly to the Ether.[760]

Following the above, the common law rules enable a claimant to trace into and through a crypto account provided that there was no mixing of another cryptoasset in the account, and no other digital asset had been transferred into the crypto account.[761] In order words, the common law cannot assert its proprietary claim if the original asset loses its identity and cannot be separated from the substituted asset. It is mixed because the original asset cannot be identified, and the claimant loses its proprietary interest. For instance, if a cryptoasset is viewed as "money" and the relevant money is not "earmarked", and thus, mixed with other money, it is treated as unidentifiable following the common law approach, as per *Re Diplock*.[762] However, in the UK, cryptoassets are not viewed as money but as "property", whilst other jurisdictions, such as El Salvador, have deemed Bitcoin a legal tender. The law in this area is still developing. However, it is unlikely the UK will follow this assumption. As a result, a cryptoasset can *prima facie* be followed into and out of the crypto account and into the hands of a subsequent transferee, provided that the cryptoasset does not cease to be identifiable.[763] However, if the cryptoasset is paid through a clearing system or a crypto mixer, and the relevant cryptoasset is mixed with other cryptoassets, it is unclear whether it is possible to trace the relevant

[758] EI Ajou v Dollar Land Holdings plc [1993] EWCA Civ 4.
[759] Westdeutsche Landesbank Girozentrale v Islington LBC [1996] AC 669.
[760] Lipkin Gorman v Karpnale Ltd [1988] UKHL 12.
[761] Banque Belge Pour I'Etranger v Hambrouck [1921] 1 KB 321.
[762] [1948] Ch 465.
[763] Agip (Africa) Ltd v Jackson [1990] Ch 265.

cryptoasset into a mixed fund.[764] In *Armstrong DLW GmbH v Winnington Networks Ltd,*[765] it was held that the fraudulent transfer of carbon emissions allowances (a chose in action or intangible property) by a defendant, the claimant was entitled to compensation in order to vindicate its original property rights. However, this is unclear whether *Armstrong* will be applicable within the crypto context.

Equitable tracing

Both *AA v Persons Unknown* and *Ion Science Ltd v Persons Unknown* are important decisions in the emerging case law concerning cryptoassets; in particular, the court's guidance on its jurisdiction pertaining to worldwide freezing orders of cryptoassets held in another jurisdiction. As discussed in Chapter 4, the *lex situs* of a cryptoasset is where the claimant is domiciled. Andrew Dickinson supported this assertion in David Fox and Sarah Green's book, Cryptocurrencies in Public and Private Law.[766] As a result, the final issue to discuss is the validity of equitable tracing and claiming an equitable proprietary interest over cryptoassets obtained by fraud and whether the relevant property can be held on a constructive or resulting trust for the claimant(s). In general, a trust is a fiduciary relationship where the relevant assets are placed under the control of a trustee for the benefit of a beneficiary.[767] In short, the legal ownership and the beneficial interest are separate since the trustee(s) are the legal owner(s) of the relevant property on behalf of the beneficial owner(s). The trustees must hold and manage the appropriate property for the benefit of the customers. For instance, Coinbase is an "e-money" institution regulated by the FCA.[768] Following Coinbase's legal document titled "Coinbase User Agreement",[769] all fiat currencies, as well as cryptoassets[770] held on the

[764] ibid.

[765] [2012] EWHC 10 (Ch).

[766] Andrew Dickinson, "Cryptocurrencies and the Conflict of Laws" in David Fox and Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (Oxford University Press 2019).

[767] Julia Kagan, "Trust" (Investopedia, 19 October 2020) <https://www.investopedia.com/terms/t/trust.asp> accessed 31 August 2021.

[768] Coinbase, "E-money Licence" (Coinbase, 2021) <https://help.coinbase.com/en/coinbase/other-topics/legal-policies/e-money-license> accessed 31 August 2021.

[769] Coinbase, "Coinbase User Agreement" (Coinbase, 2021) <https://www.coinbase.com/legal/user_agreement/payments_europe> accessed 31 August 2021.

[770] Coinbase User Agreement, 2.2(B), "Digital currencies are cryptoassets like Bitcoin or Ethereum.

customer's behalf, are kept separate from company accounts.[771] As a result, the fiat currencies and cryptoassets held in the customer's digital wallet are assets held by the company for the benefit of its customer(s) on a custodial basis.[772] In other words, Coinbase is the custodian of the customer's fiat currency and cryptoassets. As a result, the company has the power and the duty to manage the relevant assets according to Coinbase's User Agreement. Here, the legal title to the relevant assets remains with the customer.[773] However, in the event of fraud or unlawful conduct, the property in question may be crystalised into a constructive or resulting trust by the operation of law or imposed by the court. As noted by Coinbase, "*[w]e reserve the right at all times to monitor, review, retain or disclose any information as necessary to satisfy any applicable law, regulation, sanctions program, legal process or government request*".[774]

Following the above, in *Ion Science Ltd v Persons Unknown,* the applicants alleged that they had been victims of initial coin offering fraud. They were induced by *Persons Unknown*, linked to a Swiss company called Neo Capital, to transfer 64.35 Bitcoins to accounts held by Binance and Kraken. The applicants believed that they were investing in real crypto projects, Uvexo and Oileum. It was later discovered that Neo Capital was not a real company,[775] and subsequently, the Swiss regulator had issued a warning against Neo Capital for carrying out unauthorised financial services.[776] Unfortunately, persons unknown disappeared with the 64.35 Bitcoins. As a result, the misappropriated funds or the traceable proceeds are alleged to be in accounts held by Binance and Kraken (innocent third party exchange service providers), who are most likely to hold the information concerning the identity of the account holder(s). Therefore, relying on *MacKinnon v Donaldson,*[777] the court granted an international Bankers Trust Order against the two crypto exchanges in order to facilitate the disclosure of information as to the identity of the alleged fraudsters. As *Ion Science Ltd v Persons Unknown* unfolds, this section explores the traditional concept of equitable tracing and applicable concerning this ICO

[771] Coinbase User Agreement, 5.16(D).

[772] Coinbase User Agreement, 5.18(A)-(D).

[773] Coinbase User Agreement, 5.18(A).

[774] Coinbase User Agreement, 13.3

[775] FINMA, "Neo Capital Group Ltd" (FINMA, 2021) <https://www.finma.ch/en/finma-public/warning-list/neo-capital-group-ltd/> accessed 31 August 2021.

[776] FINMA, "Public warning: is this provider authorised? (FINMA, 2021) < https://www.finma.ch/en/finma-public/warning-list/> accessed 31 August 2021.

[777] 1986] Ch 482.

fraud case. Following *Re Diplock*, the fraudsters are in breach of their fiduciary duty owed to the claimant since Persons Unknown claimed to be crypto professionals. This subsequently induced the applicants to transfer 64.35 Bitcoins on the premise that they were investing in a real crypto project. The assumption here is that Persons Unknown are "quasi trustees" since the applicants had entrusted to Persons Unknown Bitcoins to be dealt with for a specific purpose.[778] It is thus submitted that, in the case of ICO fraud, the requirement of "custodial fiduciaries" or "quasi trustee" can generally be satisfied as to the misappropriation of investment funds. However, it remains to be seen whether "crypto professionals" will hold the same weight as "accountant" or "lawyer" or "CFA professional" whilst assuming a fiduciary relationship against a defendant. In other words, it was establishing a fiduciary duty and the subsequent wrongdoing of the trustee, namely Persons Unknown.

Once the above is satisfied, a constructive trust may arise by operation of law as a means to commence the equitable tracing of the misappropriated funds or the traceable proceeds to the relevant crypto accounts held by Persons Unknown.[779] Following this assertion, the Court will recognise that a constructive trust has arisen and thus notify the exchange service providers, Binance and Kraken. In *Ion Science Ltd v Persons Unknown,* a constructive trust was created over the fraudster's crypto account due to the unlawful conduct committed by Persons Unknown.[780] It is important to note, a constructive trust arises due to the unconscionable conduct of Persons Unknown as a means to deprive the defendant of the profits from their wrongdoing. However, suppose the claimants and Persons Unknown relationship did not establish a "formal" fiduciary relationship. In that case, circumstances, such as fraud or theft, namely the misappropriation or misapplication of the relevant Bitcoins, may essentially give rise to the creation of a constructive trust. Here, the constructive trust had arisen through the misappropriation or the subsequent theft of the relevant Bitcoins. As a result, this "artificial" fiduciary relationship will enable the applicants to trace their stolen property to the appropriate accounts held by *Persons Unknown*.[781]

[778] Reading v Attorney General [1949] 2 KB 232.

[779] Carn ME, "Williams v Central Bank of Nigeria: constructive trusts and the law of limitation" (2014) 28 Trust Law International 1, 3.

[780] Westdeutsche Landesbank Girozentrale v Islington LBC [1996] UKHL 12.

[781] Williams v Central Bank of Nigeria [2014] UK SC 10.

In short, constructive trusts can provide a proprietary base to commence equitable tracing and, after that, a proprietary claim concerning the relevant property in order to recover the misappropriated or misapplied property derived from wrongdoing or unlawful conduct. However, not every "wrongdoing or unlawful conduct" gives rise to a constructive trust. Nonetheless, it is submitted that in *Ion Science Ltd v Persons Unknown,* there was sufficient "wrongdoing or unlawful conduct" to create a constructive trust, namely the misappropriation of stolen bitcoins derived through the fraudulent misrepresentations via *Persons Unknown*. More importantly, due to the misappropriated and/or stolen Bitcoins, *Persons Unknown* had not acquired the rightful title to the relevant Bitcoins; thus, the applicants will most likely retain the legal and beneficial ownership, and therefore, they can rely upon common law tracing as well as equitable tracing. However, as stated in the previous section, common law tracing cannot trace into a mixed fund. In order words, once the misappropriated funds are combined with other funds, they would cease to be traceable. Nonetheless, as cemented by *Westdeutsche Landesbank*, equitable tracing rules note that stolen assets are traceable in equity because the misappropriated Bitcoins are held by *Persons Unknown* under a constructive trust.[782] In order words, when the relevant is obtained by fraud, a constructive trust arises and is imposed on the *Persons Unknown.*[783] In short, equitable tracing enables the applicant to trace into the mixed or substituted property, namely when the value of the original property can be indemnified in the mixed or substituted property.[784] *Foskett v McKeown* demonstrated how equitable claimants could trace through mixed funds and subsequently acquire into a substituted property (namely the insurance).

As demonstrated throughout this chapter, the crypto disruption is transforming traditional notions of property law and the UK court's jurisdiction over foreign third-party respondents. To some extent, the case law presented here must be used to theorise the *possible* future positions of the court and the government since both the law and the technology are still developing, thus in their infancy. Nonetheless, the recent Bankers Trust Order against *Binance Holdings Limited and Payward Limited*,[785] both foreign respondents; this case provides an

[782] Commerzbank v IMB Morgan plc [2004] EWHC 2771 (Ch).

[783] Bank of Ireland v Pexxnett Ltd and others [2010[EWHC 1872.

[784] Foskett v Mckeown [2000] UKHL 29.

[785] Ion Science Ltd and Duncan Johns v Persons Unknown, Binance Holdings Limited and Payward Limited (Unreported), 21 December 2020 (Commercial Court).

exciting insight into the UK court's extraterritorial jurisdiction concerning foreign third-party respondents. The general rule is that if the respondents are based outside of the UK, the Court will not have jurisdiction over the claim. As a result, the claimant must seek permission from the court to serve the injunction and any disclosure orders outside the jurisdiction.[786] Here, the Court must decide whether the subject matter of the dispute has a sufficient connection with the UK; after that, the Court must decide whether to exercise jurisdiction over the foreign respondent(s). Interestingly, an extraterritorial claim must be made against the defendant(s)s as a constructive trustee or as a trustee of a resulting trust. Consequently, the applicants must prove that the primary subjective matter of the dispute derived from unlawful act committed (or events) in the UK or related to UK assets.

Following the above, when a claimant seeks to invoke the Court's jurisdictions over defendants or respondents based outside of the UK,[787] the claimant must prove that the claim has sufficient connection with the UK and must show: [1] there is the good arguable case;[788] [2] the claim has a reasonable prospect of success;[789] and [3] the UK is the proper place to bring the claim.[790] Following *Ion Science Ltd v Persons Unknown,* the Commercial Court permitted extraterritorial jurisdiction of a claim for Bankers Trust order against *Binance Holdings Limited and Payward Limited,*[791] even when no remedy is sought other than disclosure. Here, a Bankers Trust Order, similar to NPO, is a third-party disclosure order granted in circumstances where there is an arguable cause of fraud. The claimant only seeks to disclose the relevant identity of the account holder and the crypto exchange to disclose confidential information concerning the transaction(s) on an appropriate account to support a proprietary claim to trace the assets. By contrast, an NPO may be applicable where a Bankers Trust Order criteria do not apply, as the threshold is lower than a Bankers Trust Order. Here, an NPO does not require a direct fraudulent correlation. However, an NPO enables the claimants to identify the proper defendant(s) in relation to a claim. However, a Bankers Trust Order essentially allows the claimant to obtain more than the identity. The claimant can then request the crypto Exchange to disclose

[786] Civil Procedure Rules, 6.36.
[787] VTB Capital plc v Nutritek International Corp and others [2013] UKSC 5.
[788] Practice Direction, 6B.3.1.
[789] Civil Procedure Rules, 6.37(1)(b).
[790] Civil Procedure Rules, 6.37(3)
[791] Practice Direction, 6B.3.1(3)

confidential information concerning the defendant to support a proprietary claim to trace the assets into the defendant's crypto account.

Similarly, in *AA v Persons Unknown,*[792] the Court granted a worldwide freezing order because it was not known where persons unknown resided; thus, following *Derby v Weldon*.[793] Here, the Court's jurisdiction enabled applicants in *AA v Persons Unknown* and *Ion Science Ltd v Persons Unknown,* to obtain a freezing injunction in respect of overseas assets. However, the respondents may face the prospect of having to defend multiple proceedings in several jurisdictions. For instance, in the crypto cases mentioned earlier, the Exchange would owe a duty of confidence to its customers, following the laws of the country where the costumer's crypto account(s) are kept, whilst simultaneously having to produce confidential documents outside the jurisdiction, upon receiving an NPO or a Bankers Trust Order.[794] Thus, the approach to be taken by foreign crypto exchanges are still unclear, accordingly depending on the local laws of the country where the crypto-accounts are kept and its local crypto AML/KYC regulation. It remains to be seen how the local courts will deal with attempts to enforce locally English worldwide freezing orders.

It is important to note, worldwide freezing injunctions are not binding on foreign respondents unless the order has been recognised and enforced in the local court.[795] For instance, the Commercial Court could grant a worldwide freezing order concerning a crypto account held in North Korea. It is unlikely the local court would recognise and enforce the English freezing order. By contrast, a crypto exchange or wallet provider based in the UK, are in possession of assets that are subject to a freezing order, the crypto firm will owe a duty of care to the Court to take reasonable care to ensure compliance. Here, the crypto firm must comply with the injunction and not permit the defendant to breach the injunction, i.e. withdraw the relevant assets from the crypto account held by the firm. Thus, where a freezing order extends to assets held in a crypto account, it overrides the Exchange's contractual obligations to its customer. However, following *HM Commissioners of Customs and Excise v Barclays*

[792] [2019] EWHC 3556 (Comm).
[793] [1990] 1 WLR 1139.
[794] Dadourian Group v Simms [2006] EWCA Civ 399.
[795] ibid.

Bank plc,[796] a bank does not owe a duty of care to the claimants of the freezing order, only to the court. As a result, the third-party respondent must take reasonable care to ensure compliance with the freezing order.[797] In other words, this eliminates the risk of liability from the claimants for damages regarding a bank's inadvertent failure to comply with a freezing order. However, suppose a crypto exchange or wallet provider based in the UK, knowingly assist the defendant or allow a breach of the freezing order. In that case, the relevant crypto firm may be found guilty of contempt of court.[798] The penalties for contempt of court will be a maximum of two years imprisonment[799] or liable to a fine[800] or the seizure of assets.[801]

However, as mentioned previously, worldwide freezing orders or disclosure orders are not binding on third parties, such as foreign crypto exchanges or wallet providers, based outside the UK's jurisdiction, unless the worldwide freezing order or disclosure order has been recognised and enforced by the local jurisdiction. In the UK, third parties, such as exchange or wallet providers, are not obligated to disclose the account holder's identity or information about a defendant's asset unless the court grants an NPO or Bankers Trust Order. In other words, any disclosure by an exchange or wallet provider in the absence of an NPO or Bankers Trust Order would, for instance, breach the exchange's duty of customer confidentiality. Whilst internationally, it is uncertain how different courts would approach and enforce English orders is an obvious issue. Nonetheless, reliance on *MacKinnon v Donaldson*[802] enables English Courts to grant a Bankers Trust Order or an NPO on crypto exchanges outside the jurisdiction. However, the question of how and whether courts of a given jurisdiction will grant an English order to preserve assets within their jurisdiction, whilst pending the outcome of the main proceedings in the UK, remains uncertain. Notwithstanding these practical hardships concerning an English worldwide freezing order, the jurisdiction of the UK courts to grant worldwide freezing orders in respect of overseas assets was recognised in *Derby & Co v*

[796] [2006] UKHL 28.
[797] JSC BTA Bank v Ablyazov and another [2016] EWHC 230 (Comm).
[798] ibid.
[799] Contempt of Court Act 1981, s 14(1)
[800] Contempt of Court Act 1981, s 14(2)
[801] Civil Procedure Rules, 81.9(1).
[802] [1986] Ch 482.

Weldon.[803] Nonetheless, an English worldwide freezing order may not be the best strategy, where the relevant assets are in a jurisdiction where permission to enforce an English order may be refused.[804]

In short, the High Court has jurisdiction to make an enforcement and a recovery order concerning any criminal property transferred abroad.[805] The presumption is that the High Court's POCA orders may be made regarding criminal property based abroad and in respect of a person or persons unknown wherever domiciled.[806] However, the High Court may not make an enforcement order regarding any criminal property based outside the UK unless there is or has been a connection between the criminal conduct and the UK.[807] Notwithstanding this presumption, international law plays a critical role in determining whether claimants in the UK can obtain private redress in the local courts, as seen in the decision of the Luxembourg District Court concerning the case of the *National Crime Agency v Azam*.[808] The High Court granted enforcement and civil recovery orders against the defendant, a convicted international drug trafficker. The Luxembourg District Court recognised and enforced the UK's civil recovery order obtained by the NCA. Whist this decision only applies to assets held in Luxembourg, this case made it easier for claimants in the UK to recover assets held overseas. More importantly, this opens the door to the possibility that other foreign states will follow suit in circumstances when national courts are faced with an application to recognise enforcement, or a civil recovery order made by the UK courts. For this reason, supranational instruments such as FATF, the Rome Convention, the Hague Convention, and other EU documents are created to enhance the harmonisation and mutual recognition of legal proceedings on an international level. In this vein, UK claimants may rely on the doctrine of *res judicata* ("a matter judged"), which prevents counterparts from re-opening any claim, defence or issue, thus ensuring the finality of

[803] [1990] 1 WLR 1139.
[804] Arcadia Petroleum Ltd and others v Bosworth and others [2015] EWHC 3700.
[805] POCA 2002, s 282A.
[806] POCA 2002, s 282A(1).
[807] POCA 2002, s 282A(3).
[808] [2014] EWHC 4742 (QB).

international judgments.[809] However, enforcing English judgments in another jurisdiction requires the local court to recognise and enforce the English judgment. In other words, no English judgments will not be enforced *unless* the local court recognises and enforce the English order. Thus, whether an English judgment can be enforced in a foreign country will depend on the private law and public policy of that particular country.

Following the UK's departure from the EU, it is uncertain whether member states will adhere to the mutual recognition of English orders.[810] In short, the rules for enforcing English judgments in the EU has profoundly changed after Brexit. Previously, the UK was a party to a framework of EU Regulations and procedural rules implementing judicial cooperation. For instance, the Recast Brussels Regulation[811] or the EU Directive on the cooperation between courts of the member states in taking evidence in civil or commercial matters.[812] Under Article 67 of the withdrawal agreement, national courts of member states will continue to enforce English judgments given before the 31st of December 2020. Traditionally, the EU and the European Free Trade Association are all subject to enforcement decisions from other national courts as outlined in the Recast Brussels Regulation and the 2007 Lugano Convention.[813] However, even under the EU framework, the process in relation to the enforcement of a foreign judgment is still determined by the national laws of the enforcing member state.

Nonetheless, the UK government announced in its 2020 White Paper that it is keen to work with the EU concerning the mutual recognition of national court orders, as contained in

[809] Addleshaw Goddard, "Secretary of State for Health and Social Care and the NHS Business Services Authority v Servier Laboratories LTD and Others" (*Addleshaw Goddard*, 2020) <https://www.addleshawgoddard.com/en/insights/insights-briefings/2020/litigation/-supreme-court-provides-clarity-application-res-judicata/> accessed 31 August 2021.

[810] For instance, the Brussels Regulation (Council Regulation EC 44/2001), the 1968 Brussels Convention, etc provides for the enforcement of foreign judgments. Here, judgment is defined as interim or final decision of a recognised court.

[811] EC 1215/2012: Recast regulation on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

[812] EC 1206/2001: Regulation on co-operation between the courts of the member states in the taking of evidence in civil or commercial matters.

[813] Ministry of Justice, "News Story: Support for the UK's intent to accede to the Lugano Convention 2007" (*GOV.UK*, 28 January 2020) <https://www.gov.uk/government/news/support-for-the-uks-intent-to-accede-to-the-lugano-convention-2007> accessed 31 August 2021.

the 2007 Lugano Convention.[814] Thus, until the EU and the UK agree on a new arrangement, claimants must rely on [1] the Hague Convention, or [2] the non-EU reciprocal enforcement regime, or [3] enforcement under national law as avenues to enforce English judgments in other jurisdictions.

The Hague Convention

The Hague Convention on Choice of Court Agreements was concluded on the 30th of June 2005. The UK ratified this international arrangement through the Private International Law (Implementation of Agreements) Act 2020.[815] Here, the EU, Denmark, Montenegro, Mexico and Singapore are parties.[816] The Hague Convention requires contracting states to recognise and enforce foreign judgments in civil or commercial matters between contracting states.[817] As a result, only civil and commercial matters are covered by the Hague Convention. Article 4(1) defines "judgment" as "*any decision on the merits given by a court, whatever it may be called, including a decree or order, and a determination of costs or expenses by the court (including an officer of the court), provided that the determination relates to a decision on the merits which may be recognised or enforced under this Convention. An interim measure of protection is not a judgment*". In other words, "judgment" means any final decision is given by a court (such as default judgment, cost determination, final injunctions, etc.).[818] However, interim protective measures and procedural rulings will not be covered under the Hague Convention.

[814] HM Government, *The Future Relationship with the EU: The UK's approach to Negotiations* (White Paper, CP 211, 2020) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/868874/The_Future_Relationship_with_the_EU.pdf> accessed 31 August 2021.

[815] Edward Attenborough, "Dispute Resolution Post-Brexit Transition Period" (*White & Case*, 6 January 2021) <https://www.whitecase.com/publications/alert/dispute-resolution-post-brexit-transition-period> accessed 18 July 2021.

[816] HCCH, "Status Table: Convention of 30 June 2005 on Choice of Court Agreement" (*Hague Conference on Private International Law*, 2021) <https://www.hcch.net/en/instruments/conventions/status-table/?cid=98> accessed 31 August 2021.

[817] The Law Society, "Choice of court agreements after Brexit" (*The Law Society*, 10 February 2021) <https://www.lawsociety.org.uk/en/topics/brexit/choice-of-court-agreements-after-brexit> accessed 31 August 2021.

[818] Joint Stock Company Aeroflot-Russian Airlines v Berezovsky and Glushkov [2014] EWCA Civ 20.

In summary, the available judicial orders and measures an English court might award to support the FCA or the NCA's AML efforts, includes civil recovery order, freezing order, worldwide freezing order, Bankers Trust order, Norwich Pharmacal order, etc. (as discussed above). Here, the issue depends on whether these orders would fall within the definition of Article 4(1) of the Hague Convention on Choice of Court Agreements. Previously, Article 35 of the Recast Brussel Regulation allowed English courts to grant interim relief in relation to proceedings in another Member State. Thus, after the end of the transition period, Article 4(1) of the Hague Convention provides that a final judgment, such as a final injunction (and not interim judgments, such as interim injunctions) will be recognised and enforced in other contracting states ("Hague Convention 2005 states").[819] However, contracting states may refuse recognition or enforcement if [1] the judgment is considered null or void under the domestic law of the contracting state;[820] [2] the contracting party lacks the capacity to enforce the English judgment;[821] [3] the claimant does not provide sufficient notice of the original English proceedings;[822] [4] the English judgment was obtained by fraud;[823] [5] the recognition or enforcement would be incompatible with the procedural fairness or public policy of the requested state;[824] [6] the English judgment is inconsistent with a judgment given in the requested state concerning a dispute between the same parties,[825] or [7] the English judgment is inconsistent with an earlier judgment given in another state between the same parties.[826] As a result, the enforcing court is not allowed to review the merits of the English judgment. However, it is not obliged to enforce English judgments if it satisfies the requirements mentioned earlier.

Notwithstanding the above, an English judgment must be recognised by the local court. In other words, no English decision will be enforced unless it is recognised. Thus, whether or

[819] Hague Convention, Article 8.
[820] Hague Convention, Article 9(a).
[821] Hague Convention, Article 9(b).
[822] Hague Convention, Article 9(c).
[823] Hague Convention, Article 9(d).
[824] Hague Convention, Article 9(e).
[825] Hague Convention, Article 9(f).
[826] Hague Convention, Article 9(g).

not the Hague Convention applies will depend on the private international law of that specific country.

The reciprocal enforcement regime

The reciprocal enforcement regime allows the enforcement of judgments from most commonwealth countries and British Overseas Territories,[827] cemented in the Administration of Justice Act 1920 and the Foreign Judgment (Reciprocal Enforcement) Act 1933.[828] In addition, the UK is also party to several bilateral treaties with individual countries[829] on the reciprocal recognition and enforcement of English judgments.[830] Here, bilateral treaties provide a framework for English claimants to obtain a declaration of enforceability of the English judgment from the court in the country where enforcement is recognised; thus, an injunction order made by an English court may not be enforceable unless the local courts have formally recognised the English Order.[831] In order words, if the relevant cryptoassets are in a jurisdiction that will not allow enforcement, a Worldwide Freezing Order will have no material effect. For instance, in *YS GM Marfin II LLC & Ors v Muhammad Ali Lakhani & Ors*,[832] the High Court confirmed that it is not an abuse of process for English claimants to notify third parties outside the jurisdiction of the UK concerning an English Worldwide Freezing Order obtained against the defendant. However, claimants must not mispresent that "*it is a contempt of Court for any third party knowingly to assist in or to permit a breach of the Worldwide Freezing Order*",[833] because third parties outside the UK are unlikely to be held in contempt since such parties are unlikely to be bound by the Worldwide Freezing Order.[834] It is important to note that, although a Worldwide Freezing Order is not enforced in a given jurisdiction, a reputable crypto exchange

[827] Such as Australia, Canada, India, Israel, Pakistan, Guernsey, Jersey, Isle of Man, Bahamas, Barbados, Bermuda, British Virgin Islands, Cayman Islands, Jamaica, Malaysia, New Zealand, Nigeria, Singapore, Sri Lanka, etc.

[828] Oliver Browne and Tom Watret, "Enforcement of Foreign Judgment 2021" (Latham & Watkins, 2021) <https://www.lw.com/thoughtLeadership/enforcement-of-foreign-judgments-2021> accessed 31 August 2021.

[829] Such as Austria, Belgium, France, Germany, Italy, the Netherlands, Norway, etc.

[830] ibid.

[831] Stephenson Harwood, "Worldwide freezing orders and third parties: practical steps for claimants and third parties" (Stephenson Harwood, 8 February 2021) <https://www.shlegal.com/news/worldwide-freezing-orders-and-third-parties-practical-steps-for-claimants-and-third-parties> accessed 31 August 2021.

[832] [2020] EWHC 2629.

[833] ibid.

[834] Euroil Ltd v Cameroon Offshore Petroleum SARL [2014] EWHC 52.

may be unwilling to help its client to breach an English Order even if the order has no legal effect on the third party and within the relevant jurisdiction. However, the point remains uncertain whether a third-party crypto firm will recognise and enforce a Worldwide Freezing Order and may have to be decided by the court in the country concerned. In short, an English judgment is only enforceable under a reciprocal regime if the English Court was granted jurisdiction on a territorial (i.e. commonwealth) or consensual basis (i.e. individual treaties).

However, following the UK's withdrawal from the EU, the essential question arises as to whether the reciprocal regime will enable the enforcement of UK judgments in the relevant member states when the EU framework ceases to cover it. Many commentators[835] believe that the English order, which might have been enforceable under the EU framework, will no longer be enforceable.[836] Thus, the point concerning the enforcement of an English Worldwide Freezing Order or English judgments remains unclear. As a result, it depends on whether the reciprocal arrangement is in force in the relevant jurisdiction. After that, which English orders or judgments are recognised by local courts, and subsequently, the local procedure must be followed.

Enforcement under national law

As demonstrated above, the enforcement of English orders and judgments will be a matter of national law in accordance with the relevant jurisdiction in which the claimant is seeking redress.[837] Thus, English judgments could be enforced under national law via judicial precedent if none of the above frameworks applies.[838] As a result, depending on the country in question, English claimants must follow the national rules whilst seeking the enforcement of English orders and judgments. As demonstrated in Vitol SA v Capri Marine Ltd,[839] once the

[835] Oriol Sapar and Jesús Castell, "Choice of law and jurisdiction in banking and finance contracts after Brexit: a perspective from Europe" (2020) 14 Law and Financial Markets Review 2, 121.

[836] Martyna Kulińska, "Cross-Border Commercial Disputes: Jurisdiction, Recognition and Enforcement of Judgments After Brexit" (2020) 16 Croatian Yearbook of European Law & Policy 1, 279.

[837] For instance, claimant must follow the national law in the enforcing state, for instance in the United States, Russia and China, and as such, consideration must be given to the appropriate local law whilst seeking redress.

[838] This covers the USA, Hong Kong as well as judgments from the EU and EFTA states.

[839] [2010] EWHC 458.

English claimant obtains a Worldwide Freezing order in the UK, the claimant can use the English order to "assist" in their application abroad. Nevertheless, the national court can also make an independent order for or against the English judgment depending on the enforcing jurisdiction. Thus, it is essential to instruct local lawyers before attempting to enforce English judgments abroad.

Are Smart Contracts the Future?

In assessing whether an English order or judgment can be enforced abroad will depend on the law of that particular country. As a result, English claimants must seek local law advice in the country of enforcement. Nonetheless, as mentioned in the previous section, the Hague Conference on Private International Law's Convention on the Recognition and Enforcement of Foreign Judgements enables contracting states to recognise and enforce civil and commercial judgments from other contracting states. Thus, providing more scope with regards to the civil recovery of the criminal property. Here, any country may become a party to the Hague's Convention on the Recognition and Enforcement of Foreign Judgments (however, only the European Union, Denmark, Montenegro, Mexico and Singapore are parties), this may make English judgments more widely enforceable within the international community.

International cooperation is critical due to the global nature of the crypto technology, making cryptoassets well suited for carrying out money laundering and facilitating crimes at an international scale. Thus, law enforcement must work closely with its foreign partners to conduct investigations, make arrests, and seize criminal assets in cases involving cryptoassets. However, authors such as Dmitri Trenin and Pavel Koshkin notes that the international community after Brexit will move from globalisation to fragmentation.[840] From this perspective, it is unlikely more countries will sign and ratify the Hague Convention on the Recognition and Enforcement of Foreign Judgments.

[840] Dmitri Trenin and Pavel Koshkin, "The world after Brexit: From globalisation to fragmentation" (Carngie Moscow Center, 17 August 2016) <https://carnegie.ru/2016/08/17/world-after-brexit-from-globalization-to-fragmentation-pub-64355> accessed 31 August 2021.

As a potential solution, Parliament can mandate the use of a FCA approved smart contract for every crypto transaction transacted in the UK, and effectively circumvent the potential jurisdictional disputes that may arise, if and when, the relevant asset is held abroad. In this instance, the agency relationship between the FCA and the crypto firm will be neutral since the AML enforcement will be administered by the FCA and lead to more money laundering cases being stopped, through an automated AML system governed by the state. For instance, when a client creates a crypto account in the UK, the client must adhere to a FCA approved smart contract protocol that, if they are suspected or deemed to hold criminal property, the cryptoassets held in the relevant account will automatically transfer to a FCA "holding" account. In other words, the asset will be frozen pending further FCA investigations and/or final judgment from the court. In addition, the FCA approved smart contract can be used to protect counterparts from fraud or force majeure. For instance, if and when a crypto transaction fails to settle, the relevant collateral or the original sum, as agreed by the parties, will automatically transfer to the non-defaulting party. Thus, in addition to the AML/KYC requirements, the FCA should recommend the use of a FCA approved smart contract to protect UK counterparts and investors.

The aforementioned is a potential solution, since the end objective of crypto money laundering is to re-integrate the illicit funds back into the mainstream economy as a legitimate transaction. For that reason, for every step or potential solution, there will be a counter step or reaction by criminal clients thus understanding the inadequacies of a potential solution is equally as important as simply developing and imposing new AML regulations. It is viewed that, when a criminal wants to spend the proceeds of their crime, the criminal face a dilemma: how can they spend large sums of money without a legitimate source of income? In order to spend the criminal income, the criminal must ensure there is no direct link between the relevant asset and the actual criminal activity. As a result, the illicit funds must be funnelled through a web of crypto accounts in "crypto friendly" jurisdictions with little or no AML laws, then placed in various crypto marketplaces to disguise its criminal origin. Thus, once the relevant property has been sufficiently "cleaned", the criminals must then transfer the relevant cryptoasset to an UK account, in order to spend the proceeds of their crime openly in the UK.

It is submitted that the smart contract model can be used by the FCA as social leverage, since in the long term, this automated AML system will be more cost effective for crypto firms. In short, the smart contract model can encourage crypto firms to be more vigilant whilst reducing the costs of regulation and fees associated with non-compliance. It is viewed that future research surrounding the process and enforcement (domestically and internationally) of the POCA offences must be examined through established crypto principles and case law. As noted previously, in the absence of leading crypto case law and consistent legal principles, it remains uncertain as to how the FCA guidelines will be applied to a crypto firm with a particular set of facts in Court. As a consequence, this adds further pressure to the already fragile agency relationship between crypto firms and the FCA.

As a result, this research has explored the regulatory issues surrounding crypto AML compliance and considered this from an agency theory perspective. As a consequence, a number of practical implications were examined, including whether an English worldwide freezing order can be enforced abroad. Thus, rather than being a simple relationship between the FCA and the crypto firm, the smart contract model acknowledges the complex hub of relationships that are involved in crypto money laundering. It is submitted that the smart contract model can be used by the FCA as social leverage, since it is viewed as being more proactive in dealing with crypto money laundering risks, and then in the long term, this will be more cost effective and more manageable for the crypto community since unexpected regulatory costs will be avoided. In short, the smart contract model can encourage crypto firms to be more vigilant whilst reducing the high costs of regulation and fees associated with non-compliance.

Accordingly, this section sets out a framework for the recognition and the legal enforcement of smart contracts, coupled with reasons as to why the FCA should recommend the use of a FCA approved smart contract when engaging in crypto related tranactions. Here, a smart contract is defined as a computer code that runs alongside decentralised blockchain platforms, such as Ethereum 2.0. As mentioned in Chapter 2, a smart contract is a computer code programmed to execute predefined logic that automatically transacts in response to an agreed input or output; thus, the computer code is self-executing when triggered by pre-agreed instructions. Accordingly, the International Swaps and Derivatives Association (“ISDA”) authored a Whitepaper concerning the implementation of Smart Contracts and Distributed

Ledger, which highlights the distinction between "Smart Legal Contract" and "Smart Contract Code".[841] The former refers to a binding legal contract or operational provisions of a legal contract, being represented and executed by a computer programmed.[842] The latter refers to the computer code designed to execute pre-agreed instructions if predefined conditions are met.[843] It is submitted that, for a Smart Legal Contract to be executed, it will need to use a Smart Contract Code. Thus, the definitions mentioned earlier are interconnected, and the overall relationship creates a legally enforceable contract. Clack, Bakshi and Braine, asserts that "*a smart contract is an automatable and enforceable agreement. Automatable by computer, although some parts may require human input and control. Enforceable either by legal enforcement of rights and obligations or via tamper-proof execution of computer code*".[844]

Accordingly, Akber Datoo and Jeffrey Golden argue that *The Satanita*[845] has cemented the legal paradigm in support of smart contracts, which may, in turn, give rise to the status of a legal contract.[846] Here, the authors contend that *"The Satanita"* established four legal principles which will reinforce the notion of smart contracts as legal contracts. Firstly, the legal principle that contractual relations may arise between counterparties, even when the parties do not know the other party's identity when they agree to be bound by the rules.[847] Secondly, the principles cemented in *"The Satanita"* has been fundamental to the international rollout of the ISDA Master Agreements.[848] Here, the ISDA protocol is essentially the common rulebook that industry participants are able to enter into a pre-agreed derivative contract. In short, the authors argue that the legal principles in *"The Satanita"* enabled the international recognition of the

[841] International Swaps and Derivatives Association, *Smart Contracts and Distributed Ledger – A legal Perspective* (White Paper, August 2017) <https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf> accessed 31 August 2021.

[842] ibid.

[843] ibid.

[844] Christopher Clack, Vikran Bakshi and Lee Braine, "Smart Contract Templates: foundations, design landscape and research directions" (ResearchGate, August 2016) <https://www.researchgate.net/publication/305779577_Smart_Contract_Templates_foundations_design_landscape_and_research_directions_CDClack_VABakshi_and_LBraine_arxiv160800771_2016> accessed 31 August 2021.

[845] [1897] AC 59.

[846] Akber Datoo and Jeffrey Golden, "Sailing into the rules of smart contracts" (2021) 6 Journal of International Banking and Financial law 387.

[847] ibid.

[848] ibid

ISDA protocol, which will legitimise the use of smart contracts. Thirdly, "The Satanita" was deemed significant in determining when and whether transactions deployed by a smart contract will give rise to a legal contract.[849] Finally, the authors conclude that is a strong presumption that smart contracts will give rise to a legal contract, even if there is no traditional written arrangement in natural language.[850]

Although Datoo and Golden rightfully outlined the relevance of *"The Satanita"* in relation to the adoption of smart contracts; however, the presumption that a smart contract written entirely in code will give rise to a legal contract is a subject matter yet to be decided by the courts. It is viewed that the courts will require additional evidence to determine whether the legal character of the arrangement met the established contractual formalities, thus giving rise to a legally binding contract. However, the authors assumed that the computer code would provide the required legal certainty concerning the terms of the contract. Here, the authors illustrate that "*once a proposed smart contract is posed on a distributed ledger and fulfils the "offer" requirement, it is capable of acceptance by the offeree. This acceptance can be by performance, for example, by transferring control of a digital asset to the smart contract (including a digital representation of an offline asset). The action of uploading assets to the smart contract should be provide an unequivocal communication of acceptance*".[851] In order words, the authors reinforce the notion that when a user interacts with the smart contract platform, and as a result, that interaction is deemed to represent acceptance of an offer. Here, according to Datoo and Golden, the interaction mentioned above means accepting an offer. As a result, the users are deemed to have intended to form legal relations, thus creating an agreement in relation to the terms of the computer code. However, the UK Jurisdictional Taskforce underlined the following scenario:

"*It is where Alice and Bob do not have a natural language contract at all so that the supposed agreement exists solely in code that the contractual position moves furthest from familiar territory. Here, there should be no difficulty in identifying terms (they will comprise the source code). There should also be no difficulty in identifying consideration—it will often be readily*

[849] ibid.
[850] ibid.
[851] ibid.

identifiable from examination of the code or even merely of the code's behaviour. ***Where the code itself will not assist is with the question of whether an agreement has been reached at all (as the mere existence of code capable of executing contractual promises reveals nothing about whether Alice and Bob actually agreed to contract on the basis of such code) and whether they intended to create legal relations. Those questions will need to be answered by reference to evidence extrinsic to the code itself***".[852]

It is submitted that the mere interaction with the smart contract platform cannot give rise to a legally binding contract. In addition, Sarwar Sayeed, Hector Marco-Gisbert and Tom Caira examined the vulnerabilities surrounding smart contracts and reveal that the smart contract technology provides a false sense of security.[853] Here, the authors identified the following vulnerabilities: [1] **malicious acts** via the spreading malware to deceive users or to conduct fraud; [2] **weak protocol** via weak or flaws in the consensus protocols thus compromising the blockchain network; [3] **defraud** via exploitation tricks to take advantage of participants, i.e. trick the relevant counterpart to release the cryptoasset prior to a transaction being fully confirmed; and [4] **application bugs**, for instance, DAO was able to raise $150m, however, due to an application bug the hacker was able to steal $60m.[854]

As a result, the smart contract enables crypto users to form a digital agreement without a third party. However, as this technology expands, it contains inherent vulnerabilities that may challenge the sustainability of this technology. As mentioned above, it is unlikely that a smart contract written entirely in code will give rise to a legally binding contract due to established principles of English contract law, namely the certainty of terms and the intention to form legal relations. More importantly, the UK Jurisdictional Taskforce's legal statement underlines the assumption that for a Smart Legal Contract to be executed, it will need to use a Smart Contract Code, coupled with additional extrinsic evidence outlining the rights and remedies of the parties, thus adhering to established principles of English contract law.

---

[852] Supra (n 6) UK Jurisdictional Taskforce.

[853] Sarwar Sayeed, Hector Marco-Gisbert and Tom Caira, "Smart Contract: Attacks and Protections" (2020) 8 IEEE Access 1. <https://research-portal.uws.ac.uk/files/14463317/2020_01_17_Sayeed_et_al_Smart_final.pdf> accessed 31 August 2021.

[854] ibid.

Notwithstanding the above vulnerabilities, the adoption of smart contracts will enable crypto firms and crypto users to minimise transactional risks and circumvent jurisdictional disputes pertaining to the enforcement of English orders abroad or seizing illicit assets from another jurisdiction. Here, the FCA can recommend that when a client creates a crypto account in the UK, the client must adhere to the pre-agreed conditions governed by the FCA approved smart contract code. For instance, in the event of money laundering, the relevant funds held in the client's crypto account will automatically transfer to a FCA "holding" account. Thus, the FCA will hold the relevant funds until the client is cleared of money laundering. Subsequently, the implementation of smart contracts in crypto transactions will minimise counterparty risks associated with crypto transactions. As mentioned previously, fraudsters tend to trick potential investors or platform users to release funds prior to a transaction being fully confirmed. Here, the FCA approved smart contract can be deployed to protect investors from fraud. For instance, in a relevant crypto transaction or an ICO, if a crypto transaction fails to settle or the ICO turns out to be fraudulent, the smart contract will hold the pre-agreed collateral, and in the event of default, the computer code will automatically transfer the relevant sum to the non-defaulting party.

However, for a smart contract to be enforceable in the UK, parties must agree on the choice of law and jurisdiction. Without a clearly defined governing law clause, it may be challenging to claim jurisdiction based on the platform's location. More importantly, if counterparties do not intend for their smart contract arrangement to be enforceable in a court of law, no legal contract may have been formed. As a result, the UK government can essentially ensure the UK remains a competitive choice for crypto users seeking redress and enforcement of crypto transactions. Thus, instead of following the traditional route of bilateral treaties and international conventions, the UK should develop a legally binding framework for smart contracts. The UK is one of the first jurisdictions in the world to clarify that smart contracts can be enforced in England and Wales. The UK Jurisdictional Taskforce advocates that "smart contracts should be capable of satisfying the requirements for a binding contract in English law and are thus enforceable by the court".[855] As a result, Parliament can essentially ensure the UK

[855] White & Case, "Status of cryptoassets and smart contracts under English law" (White & Case, 28 November 2019) <https://www.whitecase.com/publications/alert/status-cryptoassets-and-smart-contracts-under-english-law> accessed 21 August 2021.

remains a competitive choice for crypto users seeking redress and enforcement of crypto transactions. More importantly, the UK government will have control over anti-money laundering. Once the UK's framework for smart contracts is recognised internationally, more countries will recognise smart contracts, which will essentially resolve the issue of jurisdiction. In short, The UK should seek to set a gold standard and ideally achieve some degree of mutual recognition of smart contract standards to enable cross-border interoperability.

Chapter 6: Going forward

There is an international battle commencing at the moment in relation to future of the global financial system. In one corner, the US, which has been the leader of the global monetary system, in another corner, the Chinese government, launched the Digital Yuan, a cryptoasset 'with Chinese characteristics' which could be used to reinforce the government's surveillance and censorship capabilities at both micro and macroeconomic levels.[856] In the third corner, the challenge of a private crypto currency created by Facebook, which could pose a threat to national sovereignty and the international monetary system.[857] Finally, in the fourth corner are the Cypherpunks, who want to overthrow the global financial system by "*using cryptographic technology to build communities invisible to the state and multinational corporations*".[858] As a result, the geopolitical risk associated with crypto money laundering is creating tension around the world, with many countries concerned that the underlying technology could undermine the global financial system, and more importantly, proliferate crime.

This thesis has explored the regulatory influences in relation to the crypto sector's AML compliance and considered it from an agency theory perspective. A number of practical implications were considered in this research, including the different levels of agency relationships that are affected each time new crypto laws are implemented in the UK. As submitted in Chapter 3, this thesis acknowledged the complex hubs of agency relationships that are involved in crypto money laundering: [1] the crypto firm, [2] the FCA and [3] the criminal, seeking to spend the proceeds of their crime openly in the UK. The conflicting nature of this agency model is used to understand the influences that affect the crypto sector and its decision-making process, since AML compliance is implemented through the crypto firm. On the one hand, it is not apparent from an agency perspective where the advantage to the crypto firm lies in supporting the FCA as a principal. On the other hand, the FCA views the crypto sector as

[856] Alice Ekman, *China's Blockchain and Cryptocurrency Ambitions* (Brief, European Union Institute for Security Studies, 2021)

[857] Jahja Rrustemi and Nils Tuchschmid, "Facebook's Digital currency venture "Diem": the new Frontier…or a Galaxy far, far away?" (*Technology Innovation Management Review*, December 2020) <https://timreview.ca/article/1407> accessed 28 August 2021.

[858] Brady Dale, "Cypherpunk, Crypto Anarchy and How Bitcoin Lost the Narrative" (*CoinDesk*, 24 November 2020) <https://www.coindesk.com/tech/2020/11/24/cypherpunk-crypto-anarchy-and-how-bitcoin-lost-the-narrative/> accessed 28 August 2021.

being part of the state and simply an arm of law enforcement. This is a dangerous assumption because ultimately crypto firms operate through an economic business model that is geared toward financial profits, and not social development. As a result, agency model was used to study the possible impact(s) as to how the criminal, the crypto sector and the FCA, would respond to certain pressures such as increased regulation and control. Moreover, this research indicates that it is not just the agency relationship between the crypto firm and the client that can determine the money laundering risk, but equally the agency relationships between the client, the FCA and the firm's employees. Thus, it is a complex web of agency relationships that determine criminal behaviour and money laundering. In crypto money laundering, there are two sides working with AML regulation: [1] the crypto sector and the FCA, trying to manage crypto transaction and prevent potential criminals from circumventing the system and [2] the criminals and programmers trying to outsmart the current AML framework. As a result, this theory explored the human response underpinning money laundering and its response to regulation.

This research considered a number of practical approaches and agency theory was used as the base theory because it identified the core relationships between the crypto firm, the FCA and the criminal clients. It is viewed that the agent does not work for the principal thus by increasing the regulatory threat towards crypto firms, this agency relationship could backfire on the FCA. Ultimately, the agent and the principal must be in a mutually agreeable relationship since both parties need to derive some benefit from the contract. If these conditions are not met, increasing AML obligations would not in the long term address the money laundering problem; since it is hard to identify where the advantage to the crypto firm lies in supporting the FCA, as a principal. As a result, this will incentive the agent to completely sabotage the relationship and may, in turn, provoke extreme reactions from the crypto community. For instance, the development of DeFi has generally been a known side effect of trying to control the crypto community. Thus, as the cost of regulation becomes too high for the crypto sector to deal with, programmers will be rewarded more lucratively for developing new protocols that are harder to detect, and in turn, outsmart the current AML framework. It is submitted that money laundering is a multiplier of criminal conduct, and more importantly, the underlying technology allows the reinvestment of laundered funds to enter the mainstream economy as legitimate

transactions. It is viewed that the FCA's tolerance towards the damages caused by crypto money laundering and the cost of regulations determines the strictness of crypto laws and AML rules.

Nonetheless, the FCA should not impede on the legitimate and innovative growth of the crypto sector. Thus, international regulators should work together to develop a coordinate international response to protect crypto investors and businesses from fraudulent and manipulative money laundering schemes that threaten the integrity of the crypto market. As demonstrated in this thesis, in order to effectively address the crypto money laundering issue, the regulatory response must transcend national borders. However, as mentioned in Chapters 2 and 3, once the agency paradigm is applied; it is argued that, as soon as the costs of regulation to the crypto sector becomes higher than the penalties of non-compliance, then the crypto regulation is no longer efficient. It is viewed that, the rapid growth of DeFi protocols and decentralised exchanges (such as Uniswap)[859] without a readily identifiable intermediary (unlike Coinbase)[860] adhering to AML/CFT/KYC compliance obligations, has caught the FCA off guard and is the result of its attempt to control the crypto community. Reactionary responses such as this are convenient and practical for crypto programmers, especially when a position is reached that adhering to the new crypto AML laws are considered to be too costly or too burdensome. As a result, DeFi is considered an option especially when crypto programmers feel that they do not have the expertise to deal with AML/CTF/KYC compliance and sees that failing to implement the regulation would result in unwanted court and legal costs as well as hefty fines. Unfortunately, reactionary responses such as this opens the door for criminal crypto services to operate because a decentralised protocol is now available.

Crypto money laundering structures are a more than plausible money laundering tool, which can be integrated with current-day money laundering schemes. As demonstrated in this Chapter 4, although the technology used in crypto money laundering does not conform to the existing case law, the criminal conduct concerning the schemes' arrangement and behaviours are the same. Subsequently, all money laundering offences require the 'actus reus' concerning the facilitation of the criminal property and the 'mens rea' element as the requisite knowledge or suspicion. As a result, the latter element, as noted in Chapter 4, on the knowledge or suspicion

[859] Supra (n 464) Uniswap.

[860] As examined in Chapters 2 and 3.

is read vaguely so that it catches both 'front line' criminals as well as those facilitating or benefiting from crime; for instance, individuals or otherwise legitimate crypto firms, who knows or suspects that they are laundering for a criminal, as well as family members living a lavish lifestyle deriving from a life of crime. Here, the question arises on how cryptoassets should be treated from a legal perspective. At present, the case law concerning cryptoassets is still developing. Decisions, such as *AA v Persons Unknown*[861] and *Ion Science Ltd v Persons Unknown,*[862] are critical interim decisions transforming the law within the crypto space. Nonetheless, although the technology does not conform to existing case law, the criminal conduct surrounding the three primary money laundering offences, as per the POCA, is viewed as the same.

This thesis concludes that crypto money laundering is a realistic possibility and one that rightfully worries international regulators. As a potential solution, Parliament must mandate the use of a FCA approved smart contract protocol for every crypto transaction transacted in the UK, and effectively circumvent the potential jurisdictional disputes that may arise, if and when, the relevant asset is held abroad. More importantly, the smart contract model will be more cost effective, and thus more manageable for the crypto sector since unexpected regulatory costs will be avoided. In short, the smart contract model can encourage crypto firms to be more vigilant whilst reducing the high costs of regulation and fees associated with non-compliance. In this instance, the agency relationship between the FCA and the crypto firm will be neutral since AML enforcement will be administered by the FCA, and as a result, lead to more suspicious transactions being stopped by an automated protocol.

A criminal's decision to engage in crime are governed by the probability of apprehended and conviction (the "crime risk"), and the financial return it offers. William Viscusi found empirical evidence to suggest that there is a positive corelation between the crime income levels and the risk of being apprehended.[863] This finding suggests that an increased threat of criminal sanctions will determine the value of a launder's crime income; in order words, risky crimes

[861] [2019] EWHC 3556 (Comm).

[862] (unreported), 21 December 2020 (Commercial Court).

[863] William Viscusi, "The risk and rewards of criminal activity: a comprehensive test of criminal deterrence" [1986] 4 Journal of Labour Economics 3.

will command wage premiums.[864] As a consequence, the primary concern of a criminal is not the crime risk but the rewards the crime risk offers and the potential crime income. It is submitted that, a criminal's willingness to launder its assets in UK, are governed by the perceived value of the benefit and the crime income, irrespective of the potential drawbacks, for instance a FCA smart contract in order to enter the UK's mainstream economy. As demonstrated through this thesis, the end objective of money laundering is to re-integrate the illicit funds back into the mainstream economy as a legitimate transaction. For that reason, when a criminal wants to spend the proceeds of their crime, the criminal face a dilemma: how can they spend large sums of money without a legitimate source of income? Thus, in order to be able to spend the money in the UK, the criminal must ensure there is no direct link between the relevant asset and the actual criminal activity. As a result, the illicit funds are funnelled through a web of crypto accounts based in "crypto friendly" jurisdictions with little or no AML laws, then placed in various crypto marketplaces to disguise its criminal origin. Thus, once the relevant property has been sufficiently "cleaned", the criminal must then transfer the relevant cryptoasset to an UK account, in order to spend the proceeds of their crime openly in the UK.

It is submitted that the smart contract model can be used by the FCA as social leverage, since in the long term, this automated AML model will be more cost effective for crypto firms. In short, the smart contract model can encourage crypto firms to be more vigilant whilst reducing the costs of regulation and fees associated with non-compliance. It is viewed that future research surrounding the process and enforcement (domestically and internationally) of the POCA offences must be examined through established crypto principles and case law. As noted previously, in the absence of leading crypto case law and consistent legal principles, it remains uncertain as to how the FCA guidelines will be applied to a crypto firm with a particular set of facts in Court. As a consequence, this adds further pressure to the already fragile agency relationship between crypto firms and the FCA.

[864] ibid.

Research question

The FCA banned Binance Markets Limited from carrying out regulated activities in the UK because it refused to provide information about the wider Binance Group, [865] thus breaching section 165(1) of FSMA.[866] It is viewed that the FCA will continue leverage its punitive powers over a crypto firm in order to incentivise the disclosure of a firm's offshore related business. Nonetheless, whether an English order or judgment can be enforced abroad will depend on the law of that particular country. In order words, law enforcement must be able to seize and analyse foreign accounts of identified criminals to identify the crypto addresses in order to trace the illicit transfers. As a summary, *crypto-money laundering can be defined as the process by which the proceeds of crime are dealt with and transferred into the crypto space. Here, the illicit funds are funnelled through a web of shell companies and then placed in various crypto marketplaces to disguise their criminal origins. Generally, criminals tend to seek out crypto exchanges domiciled in countries with a low risk of detection due to weak or ineffective AML adherence. The end objective is to re-integrate the illicit funds back into the mainstream economy as a legitimate transaction*. As a result, the overarching research question is: *How will the AMLD5 and amendments to the MLR influence the crypto sector in the UK.* The purpose of this thesis is to provide a comprehensive AML framework that can be applied to the enforcement of the AML regulations within the crypto sector in the UK. At the start of this research, cryptoassets were unregulated, however, as mentioned in Chapter 2, the FCA became the AML/CTF supervisor of crypto firms in the UK. Notwithstanding these developments, a significant number of crypto firms still do not meet the required standard under the MLR, thus only five crypto firms have received the appropriate AML/KYC designation from the FCA to operate in the UK. As a result, the FCA had to extend the end date of the Temporary Registration Regime for existing crypto firms, from the 9 July 2012 to the 3 March 2022.[867] It is submitted that the UK is at a critical juncture in developing its regulatory approach for cryptoassets, and as a result, has a valuable opportunity to position the UK's crypto sector at the forefront of

[865] See Chapter 2, section "The FCA's jurisdiction over crypto businesses".

[866] FSMA, s 165(2) requiring the production of information the FCA. In addition, there may be criminal liability in relation to a s165(2) breach, as per s 177 of the FSMA.

[867] Financial Conduct Authority, "Cryptoassets: AML/CTF regime" (FCA, 16 August 2021) <https://www.fca.org.uk/firms/financial-crime/cryptoassets-aml-ctf-regime> accessed 29th August 2021.

innovation. Nonetheless, cryptoassets, by their nature and technology, require regulatory coherence with other international jurisdictions to ensure cross-border interoperability, legal clarity as well as certainty. How do issuers and users of crypto exploit cryptoassets to bypass the MLRs? For instance, the rapid growth of DeFi protocols and decentralised exchanges without a readily identifiable intermediary adhering to AML/CFT/KYC compliance obligations has caught international regulators off guard.[868]

Finally, can the AMLD5 and the MLRs help manage the risks associated with cryptoassets? Cryptoassets are unlikely to disappear and will survive in various forms and shapes among different market participants, from those who desire greater decentralisation, peer-to-peer networks and anonymity, to central bankers who desire centralisation, close networks and KYC compliance. As a result, cryptoassets will test traditional civil as well as criminal laws pertaining to the concealment of anonymous transactions, the end use of the underlying commodity or service being transacted, and more importantly, the origins of client funds. Nonetheless, at the heart of the UK's MLR framework is the creation of a crypto authority, the FCA, which seeks to transform AML/CTF supervision in the UK. At the present, as noted in Chapter 2, only certain categories of crypto firms are included in the scope of the UK's AML/CTF rules. For a more comprehensive AML framework, the UK government should propose to extend these rules to the entire crypto sector, obliging all service providers to conduct due diligence on their customers. As introduced in Chapter 1, the FCA should ensure the full traceability of crypto transfers via the Travel Rule, or alternatively, as submitted in Chapter 5, the FCA should advocate for the implementation of a FCA approved smart contract template for all crypto transactions transacted in the UK. This is a potential solution since the end objective of crypto money laundering is to re-integrate the illicit funds back into the mainstream economy as a legitimate transaction. For that reason, for every step or potential solution, there will be a counter step or reaction by criminals thus understanding the inadequacies of a potential solution is equally as important as simply developing and imposing new AML regulations. As a result, this research has explored the regulatory issues surrounding crypto AML compliance and considered this from an agency theory perspective. As a consequence, a number of practical implications were examined, including whether an English

[868] DeFi will be further discussed in the "Future Research" section.

order or judgment can be enforced abroad. Thus, rather than being a simple relationship between the FCA and the crypto firm, the FCA approved smart contract model acknowledges the complex hub of relationships that are involved in crypto money laundering. It is submitted that the smart contract model can be used by the FCA as social leverage, since the FCA is viewed as being more proactive in dealing with money laundering risks, and in the long term, this will be more cost effective thus more manageable for the crypto sector since unexpected regulatory costs will be avoided. In short, the smart contract model can encourage crypto firms to be more vigilant whilst reducing the high costs of regulation and fees associated with non-compliance.

The main finding to arise from this research is that international cooperation is critical due to the global nature of the crypto technology, making cryptoassets well suited for carrying out money laundering and facilitating crimes at an international scale. Parliament has confirmed that it will follow the FATF's recommendations in relation to the country's risk assessments, and as a result, the government will implement proportionate measures in response to the risks posed by crypto money laundering. Notwithstanding this assertion, reactionary responses such as Defi are convenient and practical for crypto believers, especially when adhering to AML/CTF laws are too costly or burdensome on an innovate crypto firm. Unfortunately, a natural response to burdensome AML compliance leads to the establishment of new technologies, such as DeFi. Such platforms can give rise to an opportunity for crypto criminals to continue to operate with fair ease. As a result, the UK's crypto AML framework must include the mutual recognition of freezing and confiscation orders implemented through a FCA approved smart contract protocol, as presented in Chapters 4 and 5.

Thus, whether the AMLD5 and the MLR can help mitigate the risks associated with cryptoassets, remains untested and unclear. As mentioned in Chapter 5, Binance Market Limited, a UK subsidiary of the wider Binance Group,[869] was banned from operating in the UK because the FCA alleged that the company is not capable of being adequately supervised since

[869] See Chapter 5, the process and enforcement.

it refused to provide the information in relation to the wider Binance Group.[870] In short, the regulator considered it inappropriate for a FCA authorised firm to refuse cooperation thus hindering the provision of adequate and reliable information to the FCA. However, it is viewed that, this is an artificial response and will not address the underlying issue. For instance, in October 2020 the FCA banned the sale of crypto derivatives to retail consumers, whilst many overseas exchanges state no retail investors use their platform, there are allegations that some UK investors are using virtual private networks (also known as VPNs) to trade crypto derivatives abroad. Thus, whilst the FCA is the central authority supervising UK crypto firms, crypto money laundering is a global phenomenon that requires strong international cooperation.

Future Research

The UK aims to future-proof sterling against unregulated cryptoassets since the underlying technology pose a challenge in relation to the everyday usability and increases the country's ML/TF risks. The Bank of England set out recommendations to boost the UK's FinTech sector by creating a central bank digital currency to improve its internal payment systems.[871] Other governments around the world are also laying the groundwork for a central bank-run digital currency whilst simultaneously threatening to clamp down on any rival cryptos.[872] In the US, Coinbase's recent IPO[873] is a lamentable disappointment for crypto believers;[874] however, investors in both crypto and Coinbase must reconcile the environmental damage caused by crypto miners and the fact that the US government will never allow a digital currency to challenge the dollar.[875] In the Middle East, Turkey bans crypto payments for goods

[870] Adam Samson, Philip Stafford and Eva Szalay, "UK's FCA says it is not capable of supervising crypto exchange Binance" (Financial Times, 25 August 2021) <https://www.ft.com/content/17620a3b-b82d-4b85-aa85-4cf2793b7a02> accessed 31 August 2021.

[871] Chris Giles, "UK considers creating central bank digital currency" (*Financial Times*, 19 April 2021) <https://www.ft.com/content/b39d663a-5082-42cb-ab9b-7b91e4ee1d19> accessed 31 August 2021.

[872] Benjamin Parkin, "India's digital currency plans put pressure on crypto industry" (*Financial Times*, 12 April 2021) <https://www.ft.com/content/a6767184-d216-4582-aa74-c25cb418802e> accessed 31 August 2021.

[873] Eric Platt, "Netscape 2.0: Coinbase stock debut rekindles memories of web breakthrough" (Financial Times, 16 April 2021) <https://www.ft.com/content/cbd46d95-6866-4c32-b7af-51b1772e388d> accessed 31 August 2021.

[874] Elaine Moore, "Coinbase adds sheen to cryptocurrencies but does not eliminate the risks (*Financial Times*, 16 April 2021) <https://www.ft.com/content/abb1504f-b5f4-4d93-bdf6-ed992a03b0e8> accessed 31 August 2021.

[875] Izabella Kaminska, "Coinbase listing is a lament for some bitcoin believers" (*Financial Times*, 18 April 2021) <https://www.ft.com/content/ba47468b-ddb8-4740-af63-d5629ca8364e> accessed 31 August 2021.

and services; the country's central bank notes that anonymity and the lack of regulation pose 'significant risk' for consumers.[876] Nonetheless, due to economic uncertainties and inflation risks, Turkey has the largest volume of crypto transactions in the Middle East.[877] However, following a bullish crypto quarter, coupled with government crackdowns, two Turkish crypto exchanges have collapsed.[878]

As introduced in Chapter 4, the Financial Stability Institute of the Bank for International Settlements published a report on supervising cryptoassets for anti-money laundering.[879] The report notes that supervision of cryptoasset service providers is only just beginning to be implemented around the world, with only a few countries performing more active supervision, such as conducting consultations and taking enforcement actions.[880] The report asserts that much work remains in relation to the implementation of AML/CFT/KYC standards.[881] Nonetheless, the report notes that most jurisdictions have implemented or are in the process of implementing FATF's AML/CFT national risk assessments for cryptoassets and its service providers.[882] The question posed here depends on the outcome of national authorities' assessment of cryptoassets and whether those risks are captured by existing regulation or whether there is a gap in existing laws that need to be addressed.[883] It is asserted that "*for gaps in AML/CFT regulation, implementing standards, particularly those issued by the Financial Action Task Force, should provide a solid basis for effective AML/CFT compliance and guidance*". However, challenges remain when crypto instruments and operating models do not conform to existing regulatory frameworks. On the one hand, centralised crypto exchanges, such as Coinbase and Binance,[884] its related activities would fall into the regulatory scope, and

[876] Ayla Jean Yackley, "Turkey bans crypto payments for goods and services" (*Financial Times*, 16 April 2021) <https://www.ft.com/content/449f8ac5-be7b-4d50-b01d-fe5314109d6f> accessed 31 August 2021.

[877] ibid.

[878] Ryan Browne, "A second bitcoin exchange collapses in Turkey amid crackdown on cryptocurrencies" (*CNBC*, 26 April 2021) <https://www.cnbc.com/2021/04/26/turkish-bitcoin-exchange-vebitcoin-collapses-amid-crypto-crackdown.html> accessed 31 August 2021.

[879] Supra (n 453) Coelho.

[880] ibid.

[881] ibid.

[882] ibid.

[883] ibid.

[884] Supra (n 459) Conway.

regulators can easily apply the basic principle of "***same business, same risks, same rules***".[885] Here, these exchanges are essentially private companies that offer a platform for their customers to trade cryptoassets. The regulatory treatment of centralised crypto exchanges is akin to those of financial institutions or in the UK e-money institutions; as a result, regulatory compliance measures are adhered to, namely the registration and identification of its customers. In this vein, centralised crypto exchanges are not in line with the Libertarian philosophy of Bitcoin, as advocated by the cypherpunk movement,[886] as discussed in Chapter 2. On the other hand, decentralised crypto exchanges, such as Uniswap,[887] is an automated liquidity protocol that is used to exchange cryptoassets using smart contracts powered through the Ethereum platform.[888] Here, as compared to Coinbase, Uniswap is a publicly owned and self-sustainable protocol.[889] The founder is anonymous, and the users of the platform are anonymous. In this context, KYC is not required as trading is done directly from the user's digital wallet.[890] In such cases, the regulatory identification of such novel instruments as well as operating models will not be as straightforward because they do not conform to existing regulatory definitions, especially in relation to effective AML/CFT compliance.

As mentioned in Chapter 3, in 2021, the FATF published a draft guidance in relation to entities engaged in activities as well as transactions involving cryptoassets.[891] Here, the FATF draft has broadened the scope in relation to the named entities to include [1] traditional financial institutions as well as [2] crypto service providers. Interestingly, the 2019 FATF guidance explicitly placed AML/CFT obligations on crypto service providers.[892] However, the definition

[885] Supra (n 453) Coelho.

[886] Kiran Vaidya, "Origins and Philosophical ideology behind Bitcoin" (Medium, 11 November 2016) <https://medium.com/all-things-ledger/origins-and-philosophical-ideology-behind-bitcoin-680f09a6a063> accessed 31 August 2021.

[887] Supra (n 461) Vermaak

[888] Supra (n 462) Uniswap.

[889] Supra (n 463) Uniswap.

[890] Daniel Lesnick, "Crypto AM: Definitively DeFi's guide to using Uniswap" (CityAM, 26 Setpember 2020) <https://www.cityam.com/crypto-am-definitively-defis-guide-to-using-uniswap/> accessed 31 August 2021.

[891] Financial Action Task Force, "Draft updated guidance for a risk-based approach to virtual assets and VASPs" (FATF, 19 March 2021) <https://www.fatf-gafi.org/media/fatf/documents/recommendations/March%202021%20-%20VA%20Guidance%20update%20-%20Sixth%20draft%20-%20Public%20consultation.pdf> accessed 31 August 2021.

[892] Financial Action Task Force, "Virtual Assets and Virtual Asset Service Providers" (FATF, June 2019) <https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 31 August 2021.

of crypto service providers focused on entities, such as centralised crypto exchanges operating through a custodial model (i.e. Coinbase), whereby the business held the cryptoasset on behalf of its customers. In this context, the knowledge of the private key is required to move the cryptoasset from one blockchain address to another user. Alternatively, providers of a non-custodial service, such as UniSwap, allowing users to control their private keys whilst interacting with other users without reliance on a third party, known as 'decentralised exchanges', were not considered in the FATF's original guidance, published in June 2019. As a result, the 2021 draft guidance significantly expands on the 2019 FATF guidance. From an analysis of the 2019 and the 2021 FATF guidance, some notable points: [1] a reassessment of the FATF's risk-based approach in relation to 'stable coins'; [2] additional guidance concerning the risks as well as the potential risk posed in peer-to-peer transactions; [3] updated guidance pertaining to the licensing as well as registration of crypto firms; [4] the implementation the KYC 'travel rule' in relation to crypto transactions; and [5] guidance in relation to the information-sharing and cooperation amongst international regulators.[893]

More importantly, the FATF notes that monitoring new and emerging risks requires a broadening of the "crypto" definition. As a result, it clarifies that the taxonomy must extend well beyond what was suggested in 2019. In recent years, the crypto-space has seen the rise of anonymity-enhanced cryptoassets, coupled with decentralised platforms and exchanges that enables or allows for reduced transparency and increased obfuscation of financial transactions.[894] In particular, the emergence of initial coin offerings (ICOs) that present money laundering and terrorist financing, fraud as well as market manipulation risks. Here, new illicit financing methods continue to emerge, more notably, the increasing use of crypto-to-crypto layering schemes that obfuscate illegal transactions in an easy, cheap, and secure manner via decentralised applications.

Given the development of additional illicit methods and services through the introduction of new types of decentralised providers in this space, the FATF recognised the need for further clarification in relation to the application of FATF guidance to decentralised

[893] Supra (n 453) Coelho.
[894] ibid.

technologies and crypto providers.[895] Thus, the most critical aspect of the draft guidance underlines that the definition of "virtual asset service providers" extends well beyond the definition submitted in the 2019 guidance. Here, the draft guidance clarifies that the definitions should be read expansively by national regulators. There should not be a case where a financial asset is not covered by the FATF standards, either under domestic cryptoasset legislation or as a traditional financial asset.[896] The 2021 draft explicitly mentions the rapidly growing area of DeFi, whereby the crypto service provider does not have a centralised developer nor a centralised governance body.[897] Here, the FATF notes that without an identifiable central body may carry greater money laundering as well as terrorist financing risks due to their decentralised business model; however, the lack of a central body may also reduce the likelihood of mass adoption.[898] It is submitted that more research should be conducted in relation to DeFi and its implications for money laundering.

The term DeFi refers to financial tools and operating models that do not conform to the existing AML/KYC/CF regulatory framework. Here, the financial tools are built on an open and permissionless blockchain-based network (i.e. Ethereum), known as decentralised applications ("DApps"), powered by smart contracts. Decentralised applications utilise cryptoassets, such as Bitcoin or Ether or other cryptoassets that are compatible with the "Ethereum Request for Comment" protocol ("ERC-20"). ERC-20 is used for all smart contracts and provides a list of rules that DApps must follow to use the open blockchain platform.[899] Following the ERC-20 ensures compatibility between the different types of cryptoassets issued on the Ethereum platform. Accordingly, DeFi does not require a custodial relationship amongst its users nor its corresponding digital assets. Here, the relevant digital asset is sent directly to the address of a smart contract (the code is stored directly on the blockchain network). The cryptoasset will remain locked until a user or the relevant code unlocks and sends the asset to

[895] ibid.

[896] ibid.

[897] ibid.

[898] ibid.

[899] Nathan Reiff, "What is ERC-20 and what does it mean for Ethereum" (Investopedia, 6 September 2020) <https://www.investopedia.com/news/what-erc20-and-what-does-it-mean-ethereum/> accessed 31 August 2021.

another address.[900] The scale of DeFi grew significantly; data provided by DeFi Pulse shows that the total value locked in DApps via smart contracts soared to over USD $50 billion.[901]

Subsequently, almost all DeFi products and services are automated through DApps. Once a transaction is initiated by a user, the smart contract (the computer code) will carry out the transaction (thus, no centralised body required).[902] Here, the smart contract will automatically carry out the transaction, therefore, without intermediary entities. As such, it does not involve a crypto exchange or a financial institution "holding" these assets (no custodial relationship required).[903] More importantly, all transactions are recorded on the open blockchain; thus, anyone with access to the internet can confirm the transaction's outcome. Notwithstanding this fact, users are anonymous because users are only identifiable through their public key used to execute the transaction. In order words, the users' real identities remain anonymous.[904]

In this vein, the reason DeFi can function without intermediaries are due to the following unique features: [1] all DeFi transactions must be over collateralised; as a result, the total value of the asset exceeds the value of the loan, or the transaction must be pre-funded by the borrower.[905] [2] Here, transactions are conducted through a DApp; thus, transactions are automated through a smart contract protocol. For instance, following a remedial action, such as margin calls or when an event of default occurs, the smart contract will automatically transfer the pre-agreed sum to the counterpart without using any time consuming nor costly legal processes.[906] [3] At the present, all DeFi cryptoassets have incredibly high levels of liquidity, and more importantly, the liquidity provision is embedded within smart contract protocol.[907] In

[900] ibid.

[901] Crypti, 'DeFi Grows as Total Value locked Tops $50 Billion" (Crypti, 9 April 2021) <https://crypti.io/defi-grows-as-total-value-locked-tops-50-billion> accessed 31 August 2021.

[902] Alyssa Hertig, "DeFi is short for "decentralised finance", an umbrella term for a variety of financial applications in cryptocurrency or blockchain geared towards disrupting financial intermediaries" (CoinDesk, 17 December 2020) <https://www.coindesk.com/what-is-defi> accessed 31 August 2021.

[903] ibid.

[904] ibid.

[905] ibid.

[906] Rigway Barker, "DeFi: Decentralised finance is on the rise" (WithersWorldWide, 7 August 2020) <https://www.withersworldwide.com/en-gb/insight/defi-decentralized-finance-is-on-the-rise> accessed 31 August 2021.

[907] ibid.

other words, the pledged assets are locked in and can be disposed of automatically and instantaneously when a pre-agreed contractual event occurs without the need for human intervention. [4] Here, the distinguishing factor in relation to DeFi platforms that do not exist in traditional financial markets, are the issuance of governance tokens that allow the owners of the cryptoasset to vote on certain platform upgrades, governance matters, and potentially, receive a portion of the fees paid by customers of the platform.[908]

Interestingly, when the 2019 FATF guidance was published, DeFi was barely on the radar. However, the ERC-20 technical standard's standardisation led to an explosion in the use and demand for DeFi protocols.[909] During the summer of 2020, known as the 'DeFi Summer', the user base for Compound and Uniswap grew significantly,[910] which led introducing governance tokens created to promote more accessible trading and enhance liquidity. Here, DeFi governance tokens are being distributed to users who invested "based assets", such as Bitcoin or Ether, to be locked in the smart contract as a form of collateral as well as liquidity within the DeFi protocol. This over collateralisation enables new DeFi tokens to be traded on the decentralised platform.[911] This rapid growth in cryptoasset activity through DeFi protocols and decentralised exchanges (such as Uniswap) without a readily identifiable intermediary (unlike Coinbase) adhering to AML/CFT/KYC compliance obligations has caught the FATF off guard. The critical question posed here for future research: how will the FCA impose AML/CFT/KYC compliance measures on a decentralised crypto exchange without a readily identifiable founder nor corporate body?

The draft FATF guidance provides a revised position in relation to the definition of a virtual asset service provider (VASP) as an attempt to capture DeFi platforms within its guidance. Here, the FATF notes scenarios in its guidance where a client can access a crypto service (whether it is a centralised exchange like Coinbase or a decentralised exchange like Uniswap) that, regardless of the underlying technology, some entity must have provided that

[908] ibid.

[909] Brady Dale, "With COMP below $100, a look back at the 'DeFi Summer' it sparked' (Nasdaq, 20 October 2020) <https://www.nasdaq.com/articles/with-comp-below-%24100-a-look-back-at-the-defi-summer-it-sparked-2020-10-20> accessed 31 August 2021.

[910] ibid.

[911] ibid.

financial service, even if the transaction or the act of providing the service was temporary or portions of the process was automated and shared amongst multiple parties.[912] The FATF essentially reiterated the notion that DeFi service providers remain in scope and is part of the FATF's VASP recommendations. In order words, the FATF is discounting DeFi's underlying technology, and essentially, groups DeFi service providers with that of centralised crypto service providers. As a result, the FATF underlines the assertion that there is no such thing as DeFi, and although the creator(s) and the users of DeFi are anonymous, and the transactions are all automated through smart contracts. Notwithstanding this fact, the FATF views that "*the decentralisation of any individual element of operations does not eliminate VASP coverage if the elements of any part of the VASP definition remains in place*".[913] Thus, it is viewed that a natural or legal person, who launches a service that will provide DeFi products or services, does not relieve a provider of the FATF's VASP obligations, even if those functions are to be automated through smart contracts in the future. As a result, the FATF asserts that: "*the use of an automated process such as a smart contract to carry out VASP functions does not relieve the controlling party of responsibilities for VASP obligations. For purposes of determining VASP status, launching a self-propelling infrastructure to offer VASP services is the same as offering them, and similarly commissioning others to build the element of an infrastructure, is the same as building them*".[914]

The FATF's position underlines the notion that if a creator was building the codebase or a DeFi protocol or service, the natural or legal person intends to derive, directly or indirectly, profits from the relevant codebase or protocol. As a result, the natural or legal person will be considered a VASP. Thus, once a code creator is regarded as a VASP, the DeFi programmer will be subject to the same compliance obligations as a traditional financial institution (i.e. bank or broker and dealer relationship) or a centralised crypto-exchange regulated through a crypto-custodian. In other words, the DeFi programmer or DeFi institution will be deemed as the identifiable person or entity required to conduct the relevant AML/CTF/KYC compliance checks on users who interact with the DeFi platform. Hence, the DeFi programmer would be required to check each DeFi transaction in relation to whether AML/CTF/KYC compliance

[912] Supra (n 453) Coelho.
[913] ibid.
[914] ibid.

measures are met. Subsequently, when a suspicious transaction arises, the DeFi programmer must submit a report to the NCA or the FCA. In this vein, a risk-based KYC must be conducted on any user interacting with the DeFi protocol whilst observing the Travel Rule. As discussed in Chapter 1, the Travel Rule is essentially a requirement mandated by the FATF. The information concerning the sender and the recipient must be recorded by the VASP when processing a transfer. More importantly, this information must be made available to the NCA or the FCA on demand. It is therefore submitted that many of the FATF's recommendations are intended for centralised crypto service providers. For instance, compliance measures such as the Travel Rule or AML/CTF/KYC may not be relevant to DeFi providers since the creator(s) and the users are anonymous. Notwithstanding this fact, the language submitted by the FATF captures a broad audience, as evidence by the following: *"launching a self-propelling infrastructure to offer VASP services is the same as offering them".* The language submitted by the FATF could easily capture innocent third-party or non-affiliated persons or entities, as these entities may be considered a VASP.

Subsequently, before releasing the FATF draft recommendations, there was a reasonably clear distinction between the compliance responsibilities imposed on e-money institutions and those imposed on centralised crypto-services, such as Coinbase, operating in the crypto-space. As demonstrated from Coinbase's IPO, centralised crypto services can easily adopt FATF recommendations. Whilst traditional financial institutions, such as Goldman Sachs,[915] JP Morgan,[916] and Citi,[917] increase their engagement in cryptoassets,[918] it will be relatively straightforward for banks to implement their existing compliance checks in relation to their dealings in cryptoassets. However, as evidence in the above paragraphs, the same is not true for De-Fi platforms, such as the programmers or businesses that help create a De-Fi protocol, or the anonymous individuals that effectively control and benefit economically from

[915] Eva Szalay, "Goldman Sachs executes its first bitcoin derivatives trade" (Financial Times, 7 May 2021) <https://www.ft.com/content/5ec1d0aa-7992-4fb8-8011-9d7f7b44faac> accessed 31 August 2021.

[916] Danny Nelson, "JPMorgan to Let Clients invest in Bitcoin fund for first time: Sources" (Nasdaq, 26 April 2021) <https://www.nasdaq.com/articles/jpmorgan-to-let-clients-invest-in-bitcoin-fund-for-first-time%3A-sources-2021-04-26> accessed 31 August 2021.

[917] Eva Szalay, "Citi weighs launching crypto services after surge in client interest" (Financial Times, 7 May 2021) <https://www.ft.com/content/d90ed3bf-2c8d-46c9-98b7-67859f6598e5> accessed 31 August 2021.

[918] Chris Nuttal, "Big banks move into crypto services" (Financial Times, 7 May 2021) <https://www.ft.com/content/eec2ffb3-73f4-4397-b6bf-58c60fc8a8a7> accessed 31 August 2021.

De-Fi platforms, or third-party users that purchased governance tokens, will effectively be all captured by the FATF draft recommendations.

More importantly, there are many practical questions that arise when attempting to apply AML/CTF/KYC compliance measures on these otherwise unsuspecting third-parties. For instance, under the FATF draft guidance, any holder of a governance token could be captured under the FATF's VASP mandate. In this vein, when a user sells their governance token, would this mean the De-Fi user is no longer considered a VASP? Thereafter, if the same user bought all or some of the governance tokens back, would this mean the user must adhere to the FATF's VASP mandate? If so, who will adhere to AML/CTF/KYC compliance measures in relation to recordkeeping and reporting duties, when we cannot identify who or what ultimately owns and controls the De-Fi protocol?

As demonstrated through Coinbase, FATF's recommendations can be applied to crypto firms that have identifiable employees, such as the CEO or the chef compliance officer. The critical question posed here for future research: how would an individual who purchased a single governance token, comply with the FATF's AML/CTF/KYC mandates? It would be interesting to see what penalties would apply to an individual in these circumstances. The DeFi space is rapidly developing, and it is nonetheless, still in its infancy, proponents believe that the DeFi protocol is more transparent than centralised crypto service providers because the FCA can watch the transactions in real time.[919] By contrast, in the case of centralised crypto service providers, the FCA usually get the information after the transaction have occurred, thus retrospectively, whilst with the De-Fi protocol, transactions can be monitored live.[920] Notwithstanding this fact, one of the most significant disadvantage pertaining to De-Fi is that it requires overcollateralization,[921] and is thus, extremely capital intensive, even compared to traditional finance.[922]

[919] Akash Takyar, "Centralised Finance vs Decentralised Finance" (LeewayHertz, 2021) <https://www.leewayhertz.com/defi-vs-cefi/> accessed 31 August 2021.

[920] ibid.

[921] UNN Finance, "Union's Crypto Default Swap" (Medium, 5 April 2021) <https://medium.com/union-finance-updates-ideas/unions-crypto-default-swap-7a6f7467b38a> accessed 31 August 2021.

[922] Atem Tolkachev, "The DeFi market desperately needs to connect with real-world assets" (CoinTelegraph, 14 November 2020) <https://cointelegraph.com/news/the-defi-market-desperately-needs-to-connect-with-real-world-assets> accessed 31 August 2021.

Subsequently, this led to an increased demand in crypto derivatives as well as other crypto-hedging services. According to Freshfield's calculations, the crypto derivatives market reached $2.159 trillion in the second quarter of 2020.[923] Here, this represents a year-on-year increase of 165.56%,[924] this growth was proliferated by 2020's DeFi summer.[925] Nonetheless, crypto derivatives as well as DeFi applications are vulnerable to price manipulation. For instance, creators or investors may exploit flash loans by taking out an uncollateralised loan using applications like Aave or dYdX, then repay the initial loan and pocket any profits, whilst artificially inflating or deflating the market value of a cryptoasset.[926] More recently, an investor took advantage of bZx, a lending protocol, which pegged its value through Uniwap, a decentralised exchange.[927] Here, the investor identified a token with low liquidity in a particular Uniswap pool, the investor then borrowed enough through a flash loan to dump tokens on to Uniswap's decentralised exchange, which artificially forced the price down whilst a parallel trade took out a long position on the same cryptoassets.[928] Thus, through market manipulation, the trader made more than $330,000 in profit.[929]

As investors as well as developers rush to DeFi markets amid the hype, the FCA has deemed crypto derivatives as inappropriate for retail investors and effectively banned the sale, marketing and distribution of crypto derivatives as well as exchange traded notes that are based on unregulated cryptoassets.[930] Here, the FCA notes that this blanket ban was aimed at protecting customers from harm that these crypto-products may pose, namely financial loss, market manipulation, market abuse and financial crime in the crypto-market. Following this

[923] Tom Rhodes and Olga Sendetska, "The end of the wild west: FCA confirms ban on sales of cryptoasset derivatives to retail consumers" (Freshfields Bruckhaus Deringer, 16 October 2020) <https://digital.freshfields.com/post/102gid3/the-end-of-the-wild-west-fca-confirms-ban-on-sales-of-cryptoasset-derivatives-to> accessed 31 August 2021.

[924] ibid.

[925] Jennifer Spencer, "3 Lessons from the Summer of DeFi Boom" (Entrepreneur Europe, 8 November 2020) <https://www.entrepreneur.com/article/358661> accessed 31 August 2021.

[926] ibid.

[927] ibid.

[928] ibid.

[929] ibid.

[930] Financial Conduct Authority, "FCA bans the sale of crypto-derivatives to retail consumers" (FCA, 6 October 2020) <https://www.fca.org.uk/news/press-releases/fca-bans-sale-crypto-derivatives-retail-consumers> accessed 31 August 2021.

assertion, DeFi will be on the FCA's radar: "*the government does not currently propose to bring specific DeFi activities into the scope of regulation but recognises the increasingly important role played by DeFi. It will therefore keep this space under review and monitor developments closely*".[931] As a result, the key legal considerations surrounding cryptoassets is ever more important.

Theoretical framework

As a summary, this thesis explored the regulatory influences within crypto AML compliance and considered the implementation from an agency theory perspective. As outlined in Chapter 3, a number of practical implications were examined, including the different types of agency relationships that affect the crypto space, for instance, between the client, the regulator, and the crypto firm, seeking to launder money on their behalf. The main conclusion to arise from this research is that future relationship between the FCA and the crypto space will need to look at fostering co-operation rather than solely relying on aggressive control tactics, since new technologies such as DeFi will emerge. In short, regulation will always fall short of innovation. Subsequently, the agency model is the appropriate theoretical framework since ultimately the FCA is relying on crypto firms to implement the government's AML strategy on their behalf. As a result, the crypto community needs to see and experience a benefit to engaging in this work on behalf of the government. As DeFi enters the markets, this becomes especially pertinent that the FCA seeks to foster a cohesive partnership with the tech community.

Thus, it is commonly accepted that the global implementation of the FATF standards concerning money laundering remains uneven. Here, the crypto space provides easy cross-border transactions. As a result, criminals can leverage crypto exchanges in jurisdictions with fewer levels of AML compliance or no compliance through decentralised DeFi platforms, such as UniSwap. As a result, no crypto criminals have been trialled in the UK for money laundering offences. Thus, when the first crypto money laundering trial happens, the alleged defendant(s) can and will leverage the judicial grey area, increased by the uneven implementation of the

[931] HM Treasury, "UK regulatory approach to cryptoassets and stablecoins: Consultation and call for evidence" (HM Treasury, January 2021) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950206/HM_Treasury_Cryptoasset_and_Stablecoin_consultation.pdf> accessed 31 August 2021.

FATF standards,[932]and if required, raise a section 102 SOCPA defence to shift the burden of proof to the lower civil standard. In practice, the alleged criminal can also prove that the relevant crypto transactions occurred abroad. For instance, as noted in Chapter 4, Jersey is known as a low-tax, relaxed crypto and money laundering jurisdiction.[933] Unlike the UK, Jersey is a low-tax jurisdiction, and the Government of Jersey rejected "a full prudential and conduct of business regime" for cryptoassets. As a result, crypto exchanges with an annual turnover of below GBP 150,000[934] does not have to comply with AML and CTF laws nor KYC requirements, as mandated by the FATF.[935]

Notwithstanding the above, the overreaching question is: *How will the AMLD5 and amendments to the MLRs influence the crypto sector in the UK*. Nonetheless, at the start of this research, it is important to note that the crypto sector in the UK as well as abroad was essentially unregulated. As of June 2021, only five crypto firms have met the FCA's AML requirements. In addition, 51 crypto firms have withdrawn their applications for AML registration due to not meeting the required standards under the MLR and can no longer trade in the UK.[936] Subsequently, the main finding to arise from this research is that international cooperation is critical due to the global nature of the crypto ecosystem, making cryptoassets well suited for carrying out money laundering and facilitating crimes at an international scale. As a potential solution, Parliament must mandate the use of a FCA approved smart contract protocol for every crypto transaction transacted in the UK, and effectively circumvent the potential jurisdictional disputes that may arise, if and when, the relevant asset is held abroad. It is viewed that, the regulatory reforms suggested by Parliament can be characterised as short-sighted, since the agent is not an arm of law enforcement for the principal. As a consequence, by increasing the regulatory threat towards crypto firms, could in turn, backfire on the FCA. Ultimately, the agent and the principal must be in a mutually agreeable relationship; thus, both parties need to derive actual benefits from the contract. If these conditions are not met, increasing AML obligations

[932] Supra (n 611) Roibu.

[933] Supra (n 614) Olsen.

[934] Supra (n 615) Global.

[935] Clare Feikert-Ahalt, "Regulation of Cryptocurrency in Selected Jurisdictions" (The Law Library of Congress, June 2018) <https://www.loc.gov/law/help/cryptocurrency/regulation-of-cryptocurrency.pdf> accessed 31 August 2021.

[936] Joshua Oliver, "UK regulator warns on crypto industry's anti-money laundering practices" (Financial Times, 3 June 2021) <https://www.ft.com/content/5c055be1-56ce-4792-a789-d0f0259ccd1a> accessed 31 August 2021.

would not in the long term address the money laundering problem; since it is hard to identify where the advantage for the crypto space lies in supporting the FCA. In short, the crypto community can/will sabotage its relationship with the FCA or other government regulators. As seen through, the development of DeFi, a known side effect of the government trying to control the crypto space. By contrast, the implementation of a FCA approved smart contract model; here, the agency relationship between the FCA and the crypto sector will be neutral since the AML enforcement will be administered by the FCA, through an automated AML system governed by the state.

As noted in Chapter 5, for a smart contract to be enforceable in the UK, parties must agree on the choice of law and jurisdiction because, without a clearly defined governing law clause, it may be challenging to claim jurisdiction based on the platform's location. Nonetheless, the UK is one of the first jurisdictions in the world to clarify that smart contracts can be enforced in England and Wales. As a result, Parliament can essentially ensure the UK remains a competitive choice for crypto users seeking redress as well as enforcement of crypto transactions. The UK should seek to set a gold standard and ideally achieve some degree of mutual recognition of smart contract standards to enable cross-border interoperability. Finally, this thesis offers originality in providing a thorough overview of the crypto laws, regulations and the relevant case law pertaining to cryptoassets in the UK. Thus, this research extends beyond existing works that have offered insight into the broad workings of the crypto sector and its legal implications.

Bibliography

Command Papers

Alice Ekman, *China's Blockchain and Cryptocurrency Ambitions* (Brief, European Union Institute for Security Studies, July 2021).

ECB Crypto-Asset Trask Force, *Cryptoassets: Implications for financial stability, monetary policy, and payments and markets infrastructures* (Occasional Paper Series No. 223, May 2019).

FATF, *Virtual Currencies Key Definitions and Potential AML/CFT Risk* (FATF report, June 2014).

Financial Action Trask Force, *International Standards on combating money laundering and the financing of terrorism and proliferation* (FATF Recommendations, June 2021).
Financial Conduct Authority, *Guidance on Cryptoassets* (FCA Consultation Paper 19/3, 2019).

Financial Conduct Authority, *Guidance on Cryptoassets: Feedback and Final Guidance to CP 19/3* (FCA, Policy Statement PS19/22).

Financial Conduct Authority, *Prohibiting the sale to retail clients of investment products that reference cryptoassets* (CP19/22, July 2019).

Financial Conduct Authority, *Prohibiting the sale to retail clients of investment products that reference cryptoassets* (FCA Policy Statement, October 2020).

Financial Reporting Council, *The UK Corporate Governance Code* (FRC, April 2016).
HM Government, *Economic Crime Plan 2019 to 2022* (UK Finance, 4 May 2021).

HM Government, *Economic Crime Plan: statement of progress* (UK Finance, 4 May 2021).
HM Government, *The Future Relationship with the EU: The UK's approach to Negotiations* (White Paper, CP 211, 2020).

HM Treasury, *Amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (information on the Payer) regulation 2017 Statutory Instrument 2022* (HM Treasury, 22 July 2021).

HM Treasury, *Call for Evidence: Review if the UK's AML/CFT regulatory and supervisory regime* (HM Treasury, 22 July 2021).

HM Treasury, *Money Laundering and Terrorist Financing (Amendment) Regulations 2019* (Explanatory Memorandum, No. 1511, December 2019).

HM Treasury, *National risk assessment of money laundering and terrorist financing 2017* (HM Treasury, October 2017).

HM Treasury, *Transposition of the Fifth Money Laundering Directive: Consultation* (Her Majesty's Treasury, April 2019).

HM Treasury, *Transposition of the Fifth Money Laundering Directive: Response to the consultation* (HM Treasury, January 2020).

HM Treasury, *Transposition of the Firth Money Laundering Directive* (GOV.UK, 23 January 2020).

HM Treasury, *UK regulatory approach to cryptoassets and stablecoins: Consultation and call for evidenc*e (HM Treasury, January 2021).

HMRC, *Policy paper Cryptoassets for individuals* (HMRC, 19 December 2018)
International Finance Corporation, *Blockchain opportunities for private enterprises in emerging markets* (Work Bank Group, January 2019).

Rodrigo Coelho, Jonathan Fishman and Denise Garcia Ocampo, *FSI Insights on policy implementation No 31: Supervising cryptoassets for anti-money laundering* (Financial Stability Institute, No 31, 2021).

Books/Journals

Adolf Berle and Gardiner Means, *The Modern Corporation and Private Property* (1st edn, Macmillian 1932) 114.

Akber Datoo and Jeffrey Golden, "Sailing into the rules of smart contracts" (2021) 6 Journal of International Banking and Financial law 387.

Alexandre Padilla, "Can agency theory justify the regulation of insider trading" (2002) 5 The Quarterly Journal of Austrian Economics 38.

Amy YT Chen, *Corporate Governance: Shareholder Value and the Pursuit of Short-Termism* (LLM Dissertation, Lancaster University, 2013).

Andrew Dickinson, "Cryptocurrencies and the Conflict of Laws" in David Fox and Sarah Green (eds), Cryptocurrencies in Public and Private Law (Oxford University Press 2019).

Andrew L-T Choo, "Evidence" (5th edn, Oxford University Press 2018) 27.

Anthony Giddens, *Central Problems in Social Theory: Action, Structure, and Contradiction* (First published 1979, University of California Press 1983).

Ben Regnard-Weinrabe, Heenal Vasu and Hazem Danny Ai Nakib, 'Stablecoins' (7th edn, Hart Publishing 2019) 487.

Bonnie Buchanan, 'Money laundering – a global obstacle' (2004) 18 Research in International Business and Finance 1, 115.

Carn ME, "Williams v Central Bank of Nigeria: constructive trusts and the law of limitation" (2014) 28 Trust Law International 1, 3.

Charles Perrow, *Complex Organisations: A critical essay* (3rd edn, Random House 1986).

Chiara Zilioli, 'Crypto-assets: legal challenges under private law' [2020] European Law Review 45(2), 251-266.

Christina Davilas, "AML compliance for foreign correspondent accounts: a primer on beneficial ownership requirements and other challenges" (2014) 15 Journal of Investment Compliance 1.

Daniel Kahneman and Amos Tversky, "Prospect Theory: An Analysis of Decision under Risk" (1979) 47 The Econometrica Society 2.

David Campbell, 'The roles of monitoring and morality in company law: A criticism of the direction of present regulation' (1997) 7 Australian Journal of Corporate Law 343.

David Fox, Cyber-Currencies in Private Law (1st edn, Oxford University Press 2018).

Denise Vigani, 'Aristotle's Account of Courage' (2017) 34 History of Philosophy Quarterly 4, 313.

Donato Masiandaro, "Money Laundering: the Economics of Regulation" (1999) 7 European Journal of Law and Economics 3.

Ehi Eric Esoimeme, "Institutionalising the war against corruption: new approaches to assets tracing and recovery" (2020) 27 Journal of Financial Crime 1.

Előd Takáts, "Laundering Enforcement" (2011) 27 Journal of Law Economics and Organisation 1, 34.

Eugene Fama and Michael Jensen, 'Separation of ownership and control' (1983) 26 Journal of Law and Economics 301.

Eugene Fama, "Agency problems and the theory of the firm" (1980) 88 Journal of Political Economy 288, 289.

Fraklin Edwards, Kathleen Hanley, Robert Litan and Roman Weil, "Crypto Asserts require better regulation: Statement of the financial Economists Roundtable on Crypto Assets (2019) 75 Financial Analysts Journal 2, 18.

Getie Dessaiegn Mihret, "How can we explain internal auditing? The inadequacy of agency theory and a labour process alternative" (2014) 25 Critical Perspectives on Accounting 8, 771.
Ian Lee, "Efficiency and ethics in the debate about shareholder primacy" (2006) 2 Delaware Journal of Corporate Law 31, 538.

James Edelman, "Understanding Tracing Rules" (2016) 16 QUT Law review 2.
James March, "Bounded rationality, ambiguity, and the engineering of choice" (1978) 9 The Bell Journal of Economics 2, 590.

Jason Chuah, Money Laundering Considerations in Blockchain based International Commerce in Zhao, L. and Jia, S. "*Maritime and Commercial Law in China and Europe" (Informa) (Forthcoming 2022), Chapter 14.*

John Calvin Jeffries and Paul Stephen, "Defenses, Presumptions, and Burden of Proof in the Criminal Law" (1979) 88 The Yale Law Journal 7.

John Edward Parkinson, *Corporate power and responsibility: Issues in the theory of Company Law* (1st edn, Oxford University Press, 1992) 41.

John Parkinson, *Corporate power and responsibility: Issues in the theory of company law* (1st edn, Oxford University Press) 41-42.

John Sorabji, "Interim relief: National report for England and Wales" (2018) 20 Flinders Law Journal 1.

John Stuart Mill, *Utilitarianism and the 1868 Speech on Capital Punishment* (2nd edn, Hackett Publishing Company Inc 2001) 3.

Kathleen Eisenhardt, 'Agency Theory: An Assessment and Review' (1989) 14 The Academy of Management Review 1, 57.

Klaus Schwab, *The Fourth Industrial Revolution* (1st edn, Penguin Random House 2017) 7.

Lucia Pellegrina and Donato Masciandaro, "The Risk-Based Approach in the New European Ant-Money Laundering Legislation: A Law and Economics View" (2009) 5 Review of Law and Economics 2, 6.

Martyna Kulińska, "Cross-Border Commercial Disputes: Jurisdiction, Recognition and Enforcement of Judgments After Brexit" (2020) 16 Croatian Yearbook of European Law & Policy 1, 279.

Merrick Dodd, "For whom are corporate managers trustee" (1932) 45 Harvard Law Review 7, 1146.

Michael Hirst, *Jurisdiction and the Ambit of the Criminal Law* (1st edn, Oxford University Press 2003).

Michael Jenson and William Meckling, "Theory of the firm: Managerial behaviour, agency costs and ownership structure" (1976) 3 Journal of Financial Economics 4, 305.

Mohammed Ahmad Naheem, "The Agency Dilemma in Anti-Money Laundering Regulation" (2020) 23 Journal of Money Laundering Control 1, 26.

Oriol Sapar and Jesús Castell, "Choice of law and jurisdiction in banking and finance contracts after Brexit: a perspective from Europe" (2020) 14 Law and Financial Markets Review 2, 121.

Peter Wright, Ananda Mukherji and Mark Kroll, “A re-examination of agency theory assumptions: extensions and extrapolations” (2001) 30 Journal of Behavioural and Experimental Economics 5, 413.

Peter Wright, Mark Kroll, Bevalee Pray and Augustine Lado, “Strategic orientations, competitive advantage, and business performance” (1995) 33 Journal of Business Research 1, 143.

Peter Yeo, ‘Crypto-assets: Regulators’ dilemma’ [2020] 4 Journal of Business Law 265.

Rafael La Porta, Florencio Lopez-de-Silanes, Andrei Shleifer and Robert Vishny, “Law and Finance” (1998) 106 Journal of Political Economy 6.

Richard Card, Rupert Cross and Philip Asterley, *Card, Cross & Jones Criminal Law* (21st edn, Oxford University Press 2014) 10.

Robert Wiseman and Luis Gomez-Mehia, “A Behavioural Agency Model of Managerial Risk Taking” (1997) 23 The Academy of Management Review 1, 133.

Roee Sarel, “Property Rights in Cryptocurrencies: A Law and Economics Perspective” 22 North Carolina Journal of Law and Technology 3.

Roger Brownsword, Eloise Scotford and Karen Yeung, *The Oxford Handbook of Law, Regulation and Technology* (1st edn, Oxford University Press 2017).

Rold van Wegberg, Jan-Jaap Oerlemans and Oskar van Deventer, “Bitcoin money laundering: mix results? An explorative study on money laundering of cybercrime proceeds using bitcoin” (2018) 25 Journal of Financial Crime 2.

Rudi Fortson, “R v Rogers (Bradley David): Money laundering -jurisdiction – Proceeds of Crime 2002 s327(1)(c) Court of Appeal (Criminal Division): Treacy L.J. Lang J. and Judge Bevan QC: August 1, 2014; [2010] EWVA Crim 1680” (2014) 910 Criminal Law Review 12.

Sarwar Sayeed, Hector Marco-Gisbert and Tom Caira, “Smart Contract: Attacks and Protections” (2020) 8 IEEE Access 1.

Shyamkrishna Balganesh, “Common Law Property Metaphors on the Internet: The real problem with the doctrine of Cybertrespass” (2006) 12 Michigan Telecommunications and Technology Review 265.

Stephen Ross, “The Economic Theory of Agency: The Principal Problem” (1973) 63 The American Economic Review 2, 135.

Tom R Tyler, *Why people obey the law* (1st edn, Princeton University Press 2021).

Tom Tyler, Why people obey the law (Yale University Press, 1990) 19.

William Blaire, *Banks and financial crime: the International law of tainted money* (2nd edn, Oxford University Press 2017).

William Viscusi, "The risk and rewards of criminal activity: a comprehensive test of criminal deterrence" [1986] 4 Journal of Labour Economics 3.

Wim Marneffe and Lode Vereeck, "The meaning of regulatory costs" (2011) 32 European Journal of Law and Economics 3.

Online News Journals

Adam Samson and Philip Stafford, "Financial watchdog bans crypto exchange Binance from UK" (Financial Times, 27 June 2021) <https://www.ft.com/content/8bc0e5e0-2705-496d-a265-acccaffaee87> accessed 28 August 2021.

Adam Samson, "Binance customers face extensive sterling withdrawal outage" (Financial Times, 29 June 2021) <https://www.ft.com/content/2d427ed7-f9e4-46cf-a4c4-46429b19df5d> accessed 28 August 2021.

Adam Samson, Philip Stafford and Eva Szalay, "UK's FCA says it is not capable of supervising crypto exchange Binance" (Financial Times, 25 August 2021) <https://www.ft.com/content/17620a3b-b82d-4b85-aa85-4cf2793b7a02> accessed 28 August 2021.

Andy Mukherjee, 'China's Crypto is All about Tracing – and Power" (Bloomberg, 24 May 2020) <https://www.bloomberg.com/opinion/articles/2020-05-24/china-s-yuan-will-exit-covid-19-with-a-big-digital-currency-lead> accessed 31 August 2021.

Ayla Jean Yackley, "Turkey bans crypto payments for goods and services" (Financial Times, 16 April 2021) <https://www.ft.com/content/449f8ac5-be7b-4d50-b01d-fe5314109d6f> accessed 31 August 2021.

Benjamin Parkin, "India's digital currency plans put pressure on crypto industry" (Financial Times, 12 April 2021) <https://www.ft.com/content/a6767184-d216-4582-aa74-c25cb418802e> accessed 28 August 2021.

Billy Bambrough, 'As Bitcoin Smashes Through $40,000, Data Reveals What's Behind the Huge 2021 Bitcoin Price Boom' (Forbes, 6 January 2021) <https://www.forbes.com/sites/billybambrough/2021/01/08/is-this-whats-really-behind-the-huge-2021-bitcoin-price-boom/?sh=74979dda32d9> accessed 28 August 2021.

Billy Bambrough, 'PayPal just gave 346 million people a new way to buy Bitcoin – But there's a nasty catch' (Forbes, 23 October 2020) <https://www.forbes.com/sites/billybambrough/2020/10/23/paypal-just-gave-346-million-people-a-new-way-to-buy-bitcoin-but-theres-a-nasty-catch/?sh=41fd7c002b61> accessed 28 August 2021.

Billy Bambrough, 'Why this Former Billionaire and Goldman Sachs Veteran now sees Bitcoin hitting $50,000 in 2021" (Forbes, 22 December 2020)

<https://www.forbes.com/sites/billybambrough/2020/12/22/why-this-former-billionaire-and-goldman-sachs-veteran-now-sees-bitcoin-hitting-50000-in-2021/?sh=15aadfce453b> accessed 28 August 2021.

Billy Bambrough, "Radical New Bitcoin Price Model Reveals When Shock Bitcoin Rally Could Peak" (Forbes, 13 April 2021) <https://www.forbes.com/sites/billybambrough/2021/04/13/new-radical-bitcoin-price-model-reveals-when-the-shock-bitcoin-rally-could-peak/?sh=53d853cd914c> accessed 28 August 2021.

Camilla Hodgson, Hannah Murphy and Martin Coulter, 'Cryptocurrency enthusiasts hate, and love, Libra coin' (Financial Times, 19 June 2019) <https://www.ft.com/content/5cbc38e0-91d8-11e9-b7ea-60e35ef678d2> accessed 28 August 2021.

Chris Giles, "UK considers creating central bank digital currency" (Financial Times, 19 April 2021) <https://www.ft.com/content/b39d663a-5082-42cb-ab9b-7b91e4ee1d19> accessed 28 August 2021.

Chris Nuttal, "Big banks move into crypto services" (Financial Times, 7 May 2021) <https://www.ft.com/content/eec2ffb3-73f4-4397-b6bf-58c60fc8a8a7> accessed 28 August 2021.

David Voreacos, 'Cryptocurrencies U.S., South Korea Bust Giant Child Porn Site by Following a Bitcoin Trail' (Bloomberg News, 19 October 2019) <https://www.bloomberg.com/news/articles/2019-10-16/giant-child-porn-site-is-busted-as-u-s-follows-bitcoin-trail> 28 August 2021.

Economist Jobs, 'The future of Initial Coin Offerings' (*Economist Jobs*, 4 October 2017) <https://economistjobs.com/future-initial-coin-offerings/> accessed 31 August 2021.

Economist, 'The Promise of the blockchain: The trust machine" (Economist, 31 October 2015) <https://www.economist.com/leaders/2015/10/31/the-trust-machine> accessed 31 August 2021.

Elaine Moore, "Coinbase adds sheen to cryptocurrencies but does not eliminate the risks (Financial Times, 16 April 2021) <https://www.ft.com/content/abb1504f-b5f4-4d93-bdf6-ed992a03b0e8> accessed 31 August 2021.

Eleanor Sly, "Leeds woman jailed after trying to smuggle £5.5m from UK to Dubai" (The Independent, 28 July 2021) <https://www.independent.co.uk/news/uk/crime/money-laundering-leeds-tara-hanlon-b1891152.html> accessed 31 August 2021.

Eric Platt, "Netscape 2.0: Coinbase stock debut rekindles memories of web breakthrough" (Financial Times, 16 April 2021) <https://www.ft.com/content/cbd46d95-6866-4c32-b7af-51b1772e388d> accessed 31 August 2021.

Isabelle Lee, "The crypto industry has racked up $2.5 billion in fines since bitcoin was launched in 2009" (Market Insider, 21 June 2021) <https://www-businessinsider-

com.cdn.ampproject.org/c/s/www.businessinsider.com/crypto-industry-bitcoin-racked-up-25-billion-fines-penalty-sec-2021-6?amp> accessed 31 August 2021.

Izabella Kaminska, "Coinbase Listing is a lament for some bitcoin believers: Purists believe the platform has forsaken crypto's true principles" (The Financial Times, 18 April 2021) <https://www.ft.com/content/ba47468b-ddb8-4740-af63-d5629ca8364e> accessed 31 August 2021.

Izabella Kaminska, "Coinbase listing is a lament for some bitcoin believers" (Financial Times, 18 April 2021) <https://www.ft.com/content/ba47468b-ddb8-4740-af63-d5629ca8364e> accessed 31 August 2021.

Jahja Rrustemi and Nils Tuchschmid, "Facebook's Digital currency venture "Diem": the new Frontier…or a Galaxy far, far away?" (*Technology Innovation Management Review*, December 2020) <https://timreview.ca/article/1407> accessed 31 August 2021.

Jake Frankenfield, 'Data Anonymization' (Investopedia, 25 June 2018) <https://www.investopedia.com/terms/d/data-anonymization.asp> accessed 31 August 2021.

Joshua Oliver, "Barclays stops UK clients from sending funds to Binance" (Financial Times, 5 July 2021) <https://www.ft.com/content/abc04cc0-ea53-4ecb-8c1e-49c85014fa3f> accessed 31 August 2021.

Joshua Oliver, "UK regulator warns on crypto industry's anti-money laundering practices" (Financial Times, 3 June 2021) <https://www.ft.com/content/5c055be1-56ce-4792-a789-d0f0259ccd1a> accessed 31 August 2021.

JP Buntinx, "Prosecutors issue arrest warrants for 75 Thordex employees, 62 arrested so far" (CryptoMode, 23 April 2021) <https://cryptomode.com/prosecutors-issue-arrest-warrants-for-75-thodex-employees-62-arrested-so-far/> accessed 31 August 2021.

JP Morgan, 'Can stablecoin achieve global scale?' (JP Morgan Markets, 3 December 2019).
Julia Kagan, "Trust" (Investopedia, 19 October 2020) <https://www.investopedia.com/terms/t/trust.asp> accessed 31 August 2021.

Kalyeen Makortoff, 'Bitcoin: be prepared to lose all your money, FCA warns consumers' (The Guardian, 11 January 2021) <https://www.theguardian.com/business/2021/jan/11/bitcoin-be-prepared-to-lose-all-your-money-fca-warns-consumers-risk-productis-cryptoassets> accessed 31 August 2021.

Kevin Peachey, 'Pay by cash? Not for long, report warns' (BBC News, 6 March 2019) <https://www.bbc.co.uk/news/business-47456698> accessed 31 August 2021.

Laura Shin, 'How to Speculate in ICOs: 10 Practical Financial Tips' *Forbes Magazine* (London 17 July 2017) <https://www.forbes.com/sites/laurashin/2017/07/17/how-to-speculate-in-icos-10-practical-financial-tips/#55a5b12c5378> accessed 31 August 2021.

Lisa Bachelor, “HSBC accused of closing UK accounts held by Syrians” (*The Guardian*, 8 August 2014) <https://www.theguardian.com/money/2014/aug/08/hsbc-accused-closing-bank-accounts-syrians#:~:text=One%20HSBC%20customer%2C%20Majid%20Maghout,was%20swallowed%20by%20the%20ATM.> accessed 31 August 2021.

Mary Ann Russon, ‘JP Morgan creates first US bank-backed crypto-currency’ (BBC News, 14 February 2019) <https://www.bbc.co.uk/news/business-47240760> accessed 31 August 2021.
Mary-Ann Russon, “Binance: Watchdog clamps down on cryptocurrency exchange” (BBC News, 28 June 2021) <https://www.bbc.co.uk/news/business-57632831> accessed 31 August 2021.

Michael McDonald and Matthew Bristow, “El Salvador’s Bitcoin Bombshell: What does it mean?” (Bloomberg News, 9 June 2021) <https://www.bloomberg.com/news/articles/2021-06-09/el-salvador-s-bitcoin-bombshell-what-does-it-mean-quicktake> accessed 31 August 2021.

Neal Freyman, “El Salvador moves to make bitcoin legal tender. It would become the first country to formally adopt the cryptocurrency as part of its economy” (Business Insider, 7 June 2021) <https://www.businessinsider.com/el-salvador-moves-to-adopt-bitcoin-as-legal-tender-2021-6?utm_campaign=sf-bi-finance&utm_source=facebook.com&utm_medium=social&fbclid=IwAR03qy2-DLfupuDFFGRK5zA5swEJq8XSWFTVtpyF0-uPKeU4-VcIKdDyUvQ&r=US&IR=T?utm_source=copy-link&utm_medium=referral&utm_content=topbar> accessed 31 August 2021.

Olga Kharif, ‘One of the most High-Profile Initial Coin Offerings had crashed 50%’ *Bloomberg Markets* (London, 1 November 2017) <https://www.bloomberg.com/news/articles/2017-11-01/shining-star-of-initial-coin-offerings-crashing-back-to-earth> accessed 31 August 2021.

Oliver Browne and Tom Watret, “Enforcement of Foreign Judgment 2021” (Latham & Watkins, 2021) <https://www.lw.com/thoughtLeadership/enforcement-of-foreign-judgments-2021> accessed 31 August 2021.

Palash Ghosh, ‘Gabon’s Bongo Family: Living in Luxury, Paid for By Corruption and Embezzlement’ (International Business Times, 15 February 2013) <https://www.ibtimes.com/gabons-bongo-family-living-luxury-paid-corruption-embezzlement-1088930> accessed 31 August 2021.

Pawel Kuskowski, ‘The Step that would save European Banks Twenty Billion Dollars’ (Forbes, 10 September 2018) <https://www.forbes.com/sites/pawelkuskowski/2018/09/10/the-step-that-would-save-european-banks-twenty-billion-dollars/> accessed 31 August 2021.

Priscila Azevedo Rocha and Joanna Ossinger, “UK Financial Regulator bars Exchange Binance Market” (Bloomberg, 27 June 2021)

<https://www.bloomberg.com/news/articles/2021-06-27/u-k-financial-regulator-bars-crypto-exchange-binance> accessed 31 August 2021.

Robert Hart, "British Police Seize $250 Million of Cryptocurrency in International Crackdown" (Forbes, 13 July 2021) <https://www.forbes.com/sites/roberthart/2021/07/13/british-police-seize-250-million-of-cryptocurrency-in-international-money-laundering-crackdown/> accessed 31 August 2021.
Rodrigo Campos, "El Salvador bitcoin move opens banks to money laundering, terrorism financing risks – Fintech" (Reuters, 25 June 2021) <https://www.reuters.com/technology/el-salvador-bitcoin-move-opens-banks-money-laundering-terrorism-financing-risks-2021-06-25/> accessed 31 August 2021.

Ryan Browne, "A second bitcoin exchange collapses in Turkey amid crackdown on cryptocurrencies" (CNBC, 26 April 2021) <https://www.cnbc.com/2021/04/26/turkish-bitcoin-exchange-vebitcoin-collapses-amid-crypto-crackdown.html> accessed 28 April 2021.

Ryan Browne, "Turkish crypto exchange boss goes missing, reportedly taking $2 billion of investors' funds with him" (*CNBC*, 23 April 2021) <https://www.cnbc.com/2021/04/23/bitcoin-btc-ceo-of-turkish-cryptocurrency-exchange-thodex-missing.html> accessed 31 August 2021.

Taylan Bilgic and Firat Kozok, "Turks Suspect Big Crypto Losses as Exchange CEO goes Missing" (Bloomberg News, 22 April 2021) <https://www.bloomberg.com/news/articles/2021-04-22/turks-suspect-massive-crypto-losses-as-exchange-ceo-goes-missing?utm_content=business&utm_medium=social&cmpid=socialflow-facebook-business&utm_campaign=socialflow-organic&utm_source=facebook&fbclid=IwAR1Pwnub0VfdvinqeOtm5JjY9vbwT3M8VUpmkP14-Cl0mA56Gat4gGhYf3g> accessed 31 August 2021.

Taylor Tepper, "Coinbase IPO: Here's what you need to know" (Forbes Advisor, 22 March 2021) <https://www.forbes.com/advisor/investing/coinbase-ipo-direct-listing/> accessed 29 March 2021.

The Economist, 'How to put Bitcoin into Perspective' (The Economist, 30 August 2018) <https://www.economist.com/technology-quarterly/2018/08/30/how-to-put-bitcoin-into-perspective> accessed 31 August 2021.

The Economist, 'Pessimism v progress' (The Economist, 21 December 2019). <https://www.economist.com/leaders/2019/12/18/pessimism-v-progress> accessed 31 August 2021.

The Economist, 'Telecommunications: The shape of Phones to come' (The Economist, 22 March 2001) <https://www.economist.com/taxonomy/term/23/0?page=15> accessed 31 August 2021.

The Economist, 'Token Resistance: Regulators begin to tackle the craze for initial coin offering' (*Economist*, 11 November 2017) <https://www.economist.com/news/finance-and-

economics/21731157-they-raise-difficult-legal-questions-regulators-begin-tackle-craze> accessed 31 August 2021.

The Economist, 'Why bitcoin uses so much energy' (The Economist, 9 July 2018) < https://www.economist.com/the-economist-explains/2018/07/09/why-bitcoin-uses-so-much-energy> accessed 31 August 2021.

Vildana Hajric, "DeFi Crash Accelerates With Some Once-Hot Investments Losing 50%" (Bloomberg, 18 June 2021) <https://www.bloomberg.com/news/articles/2021-06-18/defi-crash-accelerates-with-some-once-hot-investments-losing-50> accessed 31 August 2021.

Online Law Firm Sources

Addleshaw Goddard, "Secretary of State for Health and Social Care and the NHS Business Services Authority v Servier Laboratories LTD and Others" (Addleshaw Goddard, 2020) <https://www.addleshawgoddard.com/en/insights/insights-briefings/2020/litigation/-supreme-court-provides-clarity-application-res-judicata/> accessed 28 August 2021.

Allen Overy, "Supreme Court considers the constituent element of an offence under section 328 of POCA" (Allen Overy, 22 May 2015) <https://www.allenovery.com/en-gb/global/news-and-insights/publications/supreme-court-considers> accessed 28 August 2021.

Ashifa Kassam, 'How criminals use Canada's casinos to launder millions' (The Guardian, 15 October 2018) <https://www.theguardian.com/world/2018/oct/15/canada-money-laundering-casino-vancouver-model> accessed 31 August 2021.

Clifford Chance, 'HM Treasury considers gold-plating 5MLD requirements for cryptos' (Clifford Chance, 8 May 2019) <https://www.cliffordchance.com/hubs/regulatory-investigations-financial-crime-insights/our-insights/hm-treasury-considers-gold-plating-5mld-requirements-for-cryptos.html> accessed 28 August 2021.

Clifford Chance, "Non-fungible Tokens: The Global Legal Impact" (Clifford Chance, June 2021) <https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2021/06/non-fungible-tokens-the-global-legal-impact.pdf> accessed 28 August 2021.

Edward Attenborough, "Dispute Resolution Post-Brexit Transition Period" (White & Case, 6 January 2021) <https://www.whitecase.com/publications/alert/dispute-resolution-post-brexit-transition-period> accessed 31 August 2021.

Eva Szalay, "Citi weighs launching crypto services after surge in client interest" (Financial Times, 7 May 2021) <https://www.ft.com/content/d90ed3bf-2c8d-46c9-98b7-67859f6598e5> accessed 31 August 2021.

Eva Szalay, "Goldman Sachs executes its first bitcoin derivatives trade" (Financial Times, 7 May 2021) <https://www.ft.com/content/5ec1d0aa-7992-4fb8-8011-9d7f7b44faac> accessed 31 August 2021.

Harry Eddis, Richard Hay and Simon Treacy, 'UK FCA spells out when cryptoassets fall within the scope of regulation' (Linklaters LLP, 1 August 2019) <https://www.linklaters.com/en/insights/blogs/fintechlinks/2019/august/uk-fca-spells-out-when-cryptoassets-fall-within-the-scope-of-regulation> accessed 31 August 2021.

Iberian Lawyer, 'Cuatrecasas issues blockchain tokens for legal services' (Iberian Lawyer, 18 February 2019) <http://www.iberianlawyer.com/news/news/8382-cuatrecasas-issues-blockchain-tokens-for-legal-services> accessed 31 August 2021.

Ioan Grillo, 'A True Tale of Drug Cartels, Money Laundering and Horse Racing' (The Ney York Times, 22 September 2017) <https://www.nytimes.com/2017/09/22/books/review/bones-joe-tone-trevino-brothers.html> accessed 31 August 2021.

Jenna Rennie and Gwen Wackwitz, "Recovering the ransom: High Court confirms Bitcoin status as property" (White and Case, 10 February 2020) <https://www.whitecase.com/publications/alert/recovering-ransom-high-court-confirms-bitcoin-status-property> accessed 31 August 2021.

John Metais, "Profile: Bitfinex" (Coindesk, 2021) <https://www.coindesk.com/company/bitfinex> accessed 17 June 2021.
John Rogerson and William Obree, "Proving Fraud in the English Courts – a higher standard?" (White & Case LLP, 2 April 2020) <https://www.whitecase.com/publications/alert/proving-fraud-english-courts-higher-standard> accessed 31 August 2021.

Linklaters LLP, 'FCA provides further clarity on UK cryptoasset regulation in new draft guidance' (Linklaters LLP, 25 January 2019)<https://www.linklaters.com/en/insights/blogs/fintechlinks/2019/fca-provides-further-clarity-on-uk-cryptoasset-regulation-in-new-draft-guidance> accessed 31 August 2021.

Linklaters, "Our Ethical Code: Delivering legal certainty in a changing world" (*Linklaters*, 2021) <https://www.linklaters.com/en/about-us/our-firm-at-a-glance/our-ethical-code> accessed 31 August 2021.

Linklaters, "Purpose and values: Delivering legal certainty in a changing world" (*Linklaters*, 2021) <https://www.linklaters.com/en/about-us/our-firm-at-a-glance/purpose-and-values> accessed 31 August 2021.

Milton Friedman, "The social responsibility of business is to increase its profits" (*The New York Times Magazine*, 13 September 1970) <http://www.colorado.edu/studentgroups/libertarians/issues/friedman-soc-resp-business.html> accessed 31 August 2021.

Norton Rose Fulbright, "Singapore court's cryptocurrency decision: Implications for cryptocurrency trading, smart contracts and AI" (Norton Rose Fulbright, September 2019)

<https://www.nortonrosefulbright.com/en-nl/knowledge/publications/6a118f69/singapore-courts-cryptocurrency-decision-implications-for-trading-smart-contracts-and-ai> accessed 31 August 2021.

Stephenson Harwood, "Worldwide freezing orders and third parties: practical steps for claimants and third parties" (Stephenson Harwood, 8 February 2021) <https://www.shlegal.com/news/worldwide-freezing-orders-and-third-parties-practical-steps-for-claimants-and-third-parties> accessed 31 August 2021.

Tom Rhodes and Olga Sendetska, "The end of the wild west: FCA confirms ban on sales of cryptoasset derivatives to retail consumers" (Freshfields Bruckhaus Deringer, 16 October 2020) <https://digital.freshfields.com/post/102gid3/the-end-of-the-wild-west-fca-confirms-ban-on-sales-of-cryptoasset-derivatives-to> accessed 31 August 2021.

White & Case, "Status of cryptoassets and smart contracts under English law" (White & Case, 28 November 2019) <https://www.whitecase.com/publications/alert/status-cryptoassets-and-smart-contracts-under-english-law> accessed 31 August 2021.

Online Government sources

Bank for International Settlements, 'Investigating the impact of global stablecoins' (BIS Committee on Payments, October 2019) <https://www.gouvernement.fr/sites/default/files/locale/piece-jointe/2019/10/1489_-_g7sc_report_on_global_stablecoins_-17_october_2019_final.pdf> accessed 31 August 2021.

Bank for International Settlements, 'The role of central bank money in payment systems' (BIS, August 2003) <https://www.bis.org/cpmi/publ/d55.pdf> accessed 31 August 2021.

Bank of England, 'Discussion Paper: Central Bank Digital Currency' (Bank of England, March 2020) <https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf> accessed 31 August 2021.

Carey Olsen, "Jersey: Leading the way on crypto currency" (Jersey Finance, 3 May 2018) <https://www.jerseyfinance.je/our-work/jersey-leading-the-way-on-crypto-currency/> accessed 28 August 2021.

Clare Feikert-Ahalt, "Regulation of Cryptocurrency in Selected Jurisdictions" (The Law Library of Congress, June 2018) <https://www.loc.gov/law/help/cryptocurrency/regulation-of-cryptocurrency.pdf> accessed 28 August 2021.

Crown Prosecution Service, "Legal Guidance, Proceeds of Crime" (*CPS*, 19 December 2021) <https://www.cps.gov.uk/legal-guidance/proceeds-crime> accessed 31 August 2021.

Crown Prosecution Services, "Drafting the Indictment: Legal Guidance" (CPS, 13 December 2018) <https://www.cps.gov.uk/legal-guidance/drafting-indictment> accessed 28 August 2021.

European Banking Authority, ‘EBA acts to improve AML/CFT supervision in Europe’ (EBA, 2 February 2020) <https://eba.europa.eu/eba-acts-improve-amlcft-supervision-europe> accessed 31 August 2021.

European Banking Authority, ‘Report with advice for the European Commission’ (EBA, 9 January 2019) <https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf> accessed 31 August 2021.

European Commission, ‘Communication from the Commission on an Action Plan for a comprehensive Union policy on prevent money laundering and terrorist financing’ (Brussels, 7 May 2020) <https://ec.europa.eu/finance/docs/law/200507-anti-money-laundering-terrorism-financing-action-plan_en.pdf> accessed 31 August 2021.

European Parliament, ‘Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion’ (TAX3 Committee, July 2018) <https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf> accessed 31 August 2021.

Europol, ‘How Covid-19-Related Crime Infected Europe During 2020’ (Europol, 12 November 2020) <https://www.europol.europa.eu/publications-documents/how-covid-19-related-crime-infected-europe-during-2020> accessed 31 August 2021.

FCA, ‘Guidance on Cryptoassets: Consultation Paper: CP19/3’ (FCA, January 2019) <https://www.fca.org.uk/publication/consultation/cp19-03.pdf> accessed 10 June 2020.

FCA, ‘Prohibiting the sale to retail clients of investment products that reference cryptoassets’ (FCA Consultation Paper CP19/22, July 2019) <https://www.fca.org.uk/publication/consultation/cp19-22.pdf> accessed 31 August 2021.

Financial Action Task Force, ‘International standards on combating money laundering and the financing of terrorism and proliferation: FATF Recommendations (FATF, June 2019) <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html> accessed 31 August 2021.

Financial Action Task Force, “Draft updated guidance for a risk-based approach to virtual assets and VASPs” (FATF, 19 March 2021) <https://www.fatf-gafi.org/media/fatf/documents/recommendations/March%202021%20-%20VA%20Guidance%20update%20-%20Sixth%20draft%20-%20Public%20consultation.pdf> accessed 31 August 2021.

Financial Action Task Force, “Glossary of the FATF Recommendations’ (FATF, 2020) <https://www.fatf-gafi.org/glossary/u-z/#:~:text=A%20virtual%20asset%20is%20a,for%20payment%20or%20investment%20purposes> accessed 31 August 2021.

Financial Action Task Force, “Guidance on the Risk-Based Approach” (*FATF*, 2007) <http://www.fatf-

gafi.org/publications/fatfrecommendations/documents/fatfguidanceontherisk-basedapproachtocombatingmoneylaunderingandterroristfinancing-highlevelprinciplesandprocedures.html#:~:text=The%20Guidance%20on%20the%20Risk,was%20published%20in%20June%202007> accessed 31 August 2021.

Financial Action Task Force, "Virtual Assets and Virtual Asset Service Providers" (FATF, June 2019) <https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 31 August 2021.

Financial Action Task Force, Guidance for a risk-based approach: virtual assets and virtual asset service providers' (FATF, June 2019) <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html> accessed 31 August 2021.

Financial Action Task Froce, 'The United Kingdom's measures to combat money laundering and terrorist financing' (FATF, December 2017) <https://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-united-kingdom-2018.html> accessed 31 August 2021.

Financial Conduct Authority, 'CP19/22: Restricting the sale to retail clients of investment products that reference cryptoassets' (FCA, 3 July 2019) <https://www.fca.org.uk/publications/consultation-papers/cp19-22-restricting-sale-retail-clients-investment-products-reference-cryptoassets> accessed 31 August 2021.

Financial Conduct Authority, 'Cryptoasset investment scams' (FCA, 2020) <https://www.fca.org.uk/scamsmart/cryptoasset-investment-scams> accessed 31 August 2021.

Financial Conduct Authority, 'Cryptoassets: AML / CFT regime' (FCA, 24 August 2020) <https://www.fca.org.uk/firms/financial-crime/cryptoassets-aml-ctf-regime> accessed 31 August 2021.

Financial Conduct Authority, 'Cryptoassets: AML/CFT regime: Register with the FCA' (FCA, 1 October 2020) <https://www.fca.org.uk/cryptoassets-aml-ctf-regime/register> accessed 2 October 2020.

Financial Conduct Authority, 'Cryptoassets: AML/CTF regime' (FCA, 25 October 2019) <https://www.fca.org.uk/firms/financial-crime/cryptoassets-aml-ctf-regime> accessed 31 August 2021.

Financial Conduct Authority, 'Dear CEO: Cryptoassets and Financial Crime' (FCA, June 2018). <https://www.fca.org.uk/publication/correspondence/dear-ceo-letter-cryptoassets-financial-crime.pdf> accessed 31 August 2021.

Financial Conduct Authority, 'FCA innovation – fintech, regtech and innovative businesses' (FCA, 2020) <https://www.fca.org.uk/firms/innovation> accessed 31 August 2021.

Financial Conduct Authority, ‘Global Financial Innovation Network (GFIN)’ (Financial Conduct Authority, 31 January 2019) <https://www.fca.org.uk/firms/global-financial-innovation-network> accessed 31 August 2021.

Financial Conduct Authority, ‘Over £27 million reported lost to crypto and forex investment scams’ (FCA, 21 May 2019) <https://www.fca.org.uk/news/press-releases/over-27-million-reported-lost-crypto-and-forex-investment-scams> accessed 31 August 2021.

Financial Conduct Authority, ‘PERG 3A.3 the definition of electronic money’ (FCA, 2013) <https://www.handbook.fca.org.uk/handbook/PERG/3A/3.html> accessed 31 August 2021.
Financial Conduct Authority, ‘Press Release: FCA established temporary registration regime for cryptoasset businesses’ (FCA, 16 December 2020) <https://www.fca.org.uk/news/press-releases/fca-establishes-temporary-registration-regime-cryptoasset-businesses> accessed 31 August 2021.

Financial Conduct Authority, ‘Prohibiting the sale to retail client of investment products that reference cryptoassets: Technical Annex’ (FCA, October 2020) <https://www.fca.org.uk/publication/policy/ps20-10-technical-annex.pdf> accessed 31 August 2021.

Financial Conduct Authority, “Consumer warning on Binance Markets Limited and the Binance Group” (FCA, 26 June 2021) <https://www.fca.org.uk/news/news-stories/consumer-warning-binance-markets-limited-and-binance-group> accessed 31 August 2021.

Financial Conduct Authority, “Consumers: Cryptoassets” (FCA, 2021) <https://www.fca.org.uk/consumers/cryptoassets> accessed 31 August 2021.

Financial Conduct Authority, “Cryptoassets: AML/CTF regime” (FCA, 16 August 2021) <https://www.fca.org.uk/firms/financial-crime/cryptoassets-aml-ctf-regime> accessed 31 August 2021.

Financial Conduct Authority, “Cryptoassets: AML/CTF regime” (FCA, 16 August 2021) <https://www.fca.org.uk/firms/financial-crime/cryptoassets-aml-ctf-regime> accessed 31 August 2021.

Financial Conduct Authority, “Cryptoassets: Find out about the regulation of cryptoassets (including “cryptocurrencies” such as Bitcoin and Litcoin) and the risks of investing and making payments using cryptoassets” (FCA, 7 March 2019) <https://www.fca.org.uk/consumers/cryptoassets> accessed 31 August 2021.

Financial Conduct Authority, “Cryptoassets: How we define cryptoassets” (FCA, 2019) <https://www.fca.org.uk/firms/cryptoassets> accessed 31 August 2021.

Financial Conduct Authority, “FCA bans the sale of crypto-derivatives to retail consumers” (FCA, 6 October 2020) <https://www.fca.org.uk/news/press-releases/fca-bans-sale-crypto-derivatives-retail-consumers> accessed 31 August 2021.

Financial Conduct Authority, “Temporary Registration Regime extended for cryptoasset businesses” (FCA, 3 June 2021) <https://www.fca.org.uk/news/press-releases/temporary-registration-regime-extended-cryptoasset-businesses> accessed 23 June 201.

Financial Reporting Council, “Corporate Governance and Stewardship” (FRC, 2021) <https://www.frc.org.uk/directors/corporate-governance-and-stewardship> accessed 31 August 2021.

Finextra, ‘European Union unsure how to regulate Facebook’s Libra’ (Finextra, 20 February 2020) <https://www.finextra.com/newsarticle/35318/european-union-unsure-how-to-regulate-facebooks-libra> accessed 31 August 2021.

FINMA, “Neo Capital Group Ltd” (FINMA, 2021) <https://www.finma.ch/en/finma-public/warning-list/neo-capital-group-ltd/> accessed 31 August 2021.

FINMA, “Public warning: is this provider authorised? (FINMA, 2021) <https://www.finma.ch/en/finma-public/warning-list/> accessed 31 August 2021.
Gavyn Davies, “Bitcoin has ambitions for gold’s role” (Financial Times, 10 January 2021) <https://www.ft.com/content/625fbd5a-d90c-434f-998d-5e0eeb4c0f71> accessed 31 August 2021.

GOV.UK, “Guidance issued under section 2a of the Proceed of Crime Act 2002” (Gov.uk, 31 January 2018) <https://www.gov.uk/government/publications/the-proceeds-of-crime-act-section-2a> accessed 31 August 2021.

HCCH, “Status Table: Convention of 30 June 2005 on Choice of Court Agreement” (Hague Conference on Private International Law, 2021) <https://www.hcch.net/en/instruments/conventions/status-table/?cid=98> accessed 31 August 2021.

International Swaps and Derivatives Association, Smart Contracts and Distributed Ledger – A legal Perspective (White Paper, August 2017) <https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf> accessed 31 August 2021.

IRS, ‘Virtual currency: IRS issues additional guidance on tax treatment and reminds taxpayers of reporting obligations’ (IRS, 9 October 2019) <https://www.irs.gov/newsroom/virtual-currency-irs-issues-additional-guidance-on-tax-treatment-and-reminds-taxpayers-of-reporting-obligations> accessed 31 August 2021.

Joint Money Laundering Steering Group, ‘Further amendments to JMLSG Guidance’ (JMLSG, 10 January 2020) <http://www.jmlsg.org.uk/industry-guidance/article/jmlsg-guidance-current> accessed 31 August 2021.

Law Commission, ‘Adapting English Law for the digital revolution’ (Law Commission, 21 September 2020) <https://www.lawcom.gov.uk/adapting-english-law-for-the-digital-revolution/> accessed 31 August 2021.

Library of Congress Law, “Regulatory Approaches to Cryptoassets: United Kingdom” (Library of Congress Law, 30 December 2020) <https://www.loc.gov/law/help/cryptoassets/uk.php> accessed 31 August 2021.

Liechtenstein Government, ‘Blockchain Act Liechtenstein’ (*Liechtenstein Government*, October 2019) <https://impuls-liechtenstein.li/en/blockchain-act-liechtenstein/> accessed 31 August 2021.

Ministry of Justice, “News Story: Support for the UK’s intent to accede to the Lugano Convention 2007” (GOV.UK, 28 January 2020) <https://www.gov.uk/government/news/support-for-the-uks-intent-to-accede-to-the-lugano-convention-2007> accessed 31 August 2021.
Robby Houben and Alexander Snyers, ‘Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion (European Parliament Special Committee on Financial Crime and Tax Avoidance, July 2018) <http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf> accessed 31 August 2021.

Sir Geoffrey Vos, ‘‘Cryptoassets as property: how can English law boost the confidence of would-be parties to smart legal contracts?’ (UK Courts and Tribunals Judiciary, May 2019) < https://www.judiciary.uk/announcements/speech-by-sir-geoffrey-vos-chancellor-of-the-high-court-cryptoassets-as-property/> accessed 31 August 2021.

Solicitors Regulation Authority, “Anti Money Laundering Report” (Solicitor Regulation Authority, May 2016) <https://www.sra.org.uk/globalassets/documents/sra/research/anti-money-laundering-report.pdf?version=4a1ab0> accessed 31 August 2021.

Steve Browning, ‘Briefing Paper: Cryptocurrencies: Bitcoin and other exchange tokens’ (House of Commons Number 8780, 19 February 2020) <https://researchbriefings.files.parliament.uk/documents/CBP-8780/CBP-8780.pdf> accessed 31 August 2021.

The Crown Prosecution Services, ‘Proceeds of Crime Act 2002 Part 7 - Money Laundering Offences’ (CPS, 1 March 2018) <https://www.cps.gov.uk/legal-guidance/proceeds-crime-act-2002-part-7-money-laundering-offences> accessed 31 August 2021.

The Global Financial Innovation Network, ‘GFiN – One year on – Report 2019’ (GFiN, January 2019) <http://dfsa.ae/Documents/Fintech/GFIN-One-year-on-FINAL-20190612.pdf> accessed 31 August 2021.

The Joint Money Laundering Steering Group, ‘Prevention of money laundering and combating terrorist financing: Part II Sectoral Guidance’ (JMLSG, June 2020) <https://secureservercdn.net/160.153.138.163/a3a.8f7.myftpupload.com/wp-content/uploads/2020/07/JMLSG-Guidance_Part-II_-July-2020.pdf> accessed 31 August 2021.

The Law Society, “Anti-money laundering after Brexit” (The Law Society, 1 April 2021) <https://www.lawsociety.org.uk/en/topics/brexit/anti-money-laundering-after-brexit> accessed 31 August 2021.

The Law Society, “Choice of court agreements after Brexit” (The Law Society, 10 February 2021) <https://www.lawsociety.org.uk/en/topics/brexit/choice-of-court-agreements-after-brexit> accessed 31 August 2021.

The UK Government, ‘Information you must send with a transfer of funds to prevent money laundering’ (GOV.UK, 25 February 2014) <https://www.gov.uk/guidance/how-to-comply-with-eu-payments-regulation#the-eu-funds-transfer-regulation> accessed 10 January 2020.

The United States Department of Justice, ‘Bitcoin dealer indicted on money laundering charges; held without bond’ (The US Department of Justice, 17 August 2018) <https://www.justice.gov/usao-sdca/pr/bitcoin-dealer-indicted-money-laundering-charges-held-without-bond> accessed 31 August 2021.

The United States Department of Justice, ‘Dark Web Vendors Pleads Guilty to Cryptocurrency Money Laundering Conspiracy’ (Department of Justice, 2 October 2019) <https://www.justice.gov/usao-sdca/pr/dark-web-vendors-plead-guilty-cryptocurrency-money-laundering-conspiracy> accessed 31 August 2021.

The US Commodity Futures Trading Commission, ‘Bitcoin Basics’ (CFTC, December 2019) <https://www.cftc.gov/sites/default/files/2019-12/oceo_bitcoinbasics0218.pdf> accessed 31 August 2021.

The US Commodity Futures Trading Commission, ‘IN CASE YOU MISSED IT: Chairman Tarbert Comments on Cryptocurrency Regulation at Yahoo! Finance All Markets Summit’ (CFTC, 10 October 2019) <https://www.cftc.gov/PressRoom/PressReleases/8051-19> accessed 31 August 2021.

The US Securities Exchange Commission, ‘SEC Halts Alleged $1.7 Billion Unregistered Digital Token Offering’ (SEC, 11 October 2019) <https://www.sec.gov/news/press-release/2019-212> accessed 31 August 2021.

The World Economic Forum, ‘The Fourth Industrial Revolution, by Klaus Schwab’ (Word Economic Forum, 2019) <https://www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab> accessed 31 August 2021.

UK Jurisdictional Taskforce, ‘Legal statement on cryptoassets and smart contracts’ (Tech Nation, November 2019) <https://technation.io/news/uk-takes-significant-step-in-legal-certainty-for-smart-contracts-and-cryptocurrencies/> accessed 31 August 2021.

United Nations Office on Drugs and Crime, “Money-Laundering and Globalisation’ (UNODC, 2020) <https://www.unodc.org/unodc/en/money-laundering/globalization.html> accessed 31 August 2021.

United Nations Office on Drugs and Crime, “The Money-Laundering Cycle’ (UNODC, 2020) <https://www.unodc.org/unodc/en/money-laundering/laundrycycle.html> accessed 31 August 2021.

Online sources

Akash Takyar, “Centralised Finance vs Decentralised Finance” (LeewayHertz, 2021) <https://www.leewayhertz.com/defi-vs-cefi/> accessed 28 August 2021.

Alyssa Hertig, “DeFi is short for “decentralised finance”, an umbrella term for a variety of financial applications in cryptocurrency or blockchain geared towards disrupting financial intermediaries” (CoinDesk, 17 December 2020) <https://www.coindesk.com/what-is-defi> accessed 28 August 2021.

Amazon, “Leadership Principles” (Amazon, 2021) <https://www.amazon.jobs/en/principles> accessed 31 August 2021.Anatol Antonovici, “Dogecoin Mining 2021: Everything you need to know” (Coindesk, 28 June 2021) <https://www.coindesk.com/dogecoin-mining-2021-everything-you-need-to-know> accessed 28 August 2021.

Andy Greenberg, ‘Prosecutors Trace $13.4M in Bitcoins from the Silk Road to Ulbricht’s Laptop’ (The Wired, 29 January 2015) <https://www.wired.com/2015/01/prosecutors-trace-13-4-million-bitcoins-silk-road-ulbrichts-laptop/> accessed 28 August 2021.

Antony Lewis, ‘A Gentle Introduction to Bitcoin’ (Bits on Blocks, 1 September 2015) <https://bitsonblocks.net/2015/09/01/gentle-introduction-bitcoin/> accessed 7 January 2019.

Atem Tolkachev, “The DeFi market desperately needs to connect with real-world assets” (CoinTelegraph, 14 November 2020) <https://cointelegraph.com/news/the-defi-market-desperately-needs-to-connect-with-real-world-assets> accessed 31 August 2021.

Binance, “Buy and sell crypto in minutes” (Binance, 2021) <https://www.binance.com/en> accessed 28 August 2021.

Bitcoin Exchange Guide, ‘Initial Coin Offering – Alternative ICO Cryptocurrency Token Guide’ (Bitcoin Exchange Guide, 2017) < https://bitcoinexchangeguide.com/initial-coin-offering/> accessed 28 August 2021.

Bitcoin Magazine, “Coincase IPO exceeds all expectations, showing more promise for Bitcoin” (*Nasdaq*, 19 April 2021) <https://www.nasdaq.com/articles/coinbase-ipo-exceeds-all-expectations-showing-more-promise-for-bitcoin-2021-04-19> accessed 28 August 2021.

Bitcoin Magazine, “The Bitcoin Magazine” (Bitcoin Magazine, 2021) <https://bitcoinmagazine.com/> accessed 28 August 2021.

Bitcoin Wiki, ‘Private Key’ (Bitcoin, 1 March 2019) <https://en.bitcoin.it/wiki/Private_key> accessed 28 August 2021.

Bitpay, “Take control of your crypto” (Bitpay, 2021) <https://bitpay.com/wallet/> accessed 28 August 2021.
Blockchain.com, “The world’s most popular crypto wallet” (Blockchain.com, 2021) <https://www.blockchain.com/wallet> accessed 31 August 2021.

Brady Dale, “Cypherpunk, Crypto Anarchy and How Bitcoin Lost the Narrative” (*CoinDesk*, 24 November 2020) <https://www.coindesk.com/tech/2020/11/24/cypherpunk-crypto-anarchy-and-how-bitcoin-lost-the-narrative/> accessed 28 August 2021.

Brady Dale, “With COMP below $100, a look back at the ‘DeFi Summer’ it sparked’ (Nasdaq, 20 October 2020) <https://www.nasdaq.com/articles/with-comp-below-%24100-a-look-back-at-the-defi-summer-it-sparked-2020-10-20> accessed 28 August 2021.

Braintree, “Braintree a PayPal Service: Boost Revenue with Global payments partner” (Braintree, 2021) <https://www.braintreepayments.com/gb> accessed 28 August 2021.

Buy Bitcoin Worldwide, ‘How to buy bitcoins with cash or cash deposits’ (Buy Bitcoin Worldwide, 2020) <https://www.buybitcoinworldwide.com/en/buy-bitcoins-with-cash/> accessed 28 August 2021.

Chainbytes, “How to use Bitcoin ATM” (Chainbytes, 2021) <https://www.chainbytes.com/how-to-use-bitcoin-atm/> accessed 28 August 2021.

Chris Hoofnagle, ‘Should regulation be ‘Technology Neutral’ (Berkeley.edu, 2 February 2018) <https://hoofnagle.berkeley.edu/2018/02/02/should-regulation-be-technology-neutral/> accessed 28 August 2021.

Chris McCoy, ‘Overview: convert cryptocurrency to fiat currency’ (BlockchainDK, 18 December 2017) <https://www.blockchaindk.com/2017/12/18/convert-cryptocurrency-to-fiat-currency/> accessed 28 August 2021.

Christopher Clack, Vikran Bakshi and Lee Braine, “Smart Contract Templates: foundations, design landscape and research directions” (ResearchGate, August 2016) <https://www.researchgate.net/publication/305779577_Smart_Contract_Templates_foundations_design_landscape_and_research_directions_CDClack_VABakshi_and_LBraine_arxiv160800771_2016> accessed 28 August 2021.

Christopher Malmo, ‘One Bitcoin Transaction Consumes As Much Energy As Your House Uses in a Week’ (Vice News, 1 November 2017) <https://www.vice.com/en_us/article/ywbbpm/bitcoin-mining-electricity-consumption-ethereum-energy-climate-change> accessed 28 August 2021.

Coinbase, “Coinbase User Agreement” (Coinbase, 2021) <https://www.coinbase.com/legal/user_agreement/payments_europe> accessed 28 August 2021.

Coinbase, “E-money Licence” (Coinbase, 2021) <https://help.coinbase.com/en/coinbase/other-topics/legal-policies/e-money-license> accessed 28 August 2021.

Coinbase, “Get direct access to Coinbase Exchange” (Coinbase, 2021) <https://www.coinbase.com/exchange> accessed 28 August 2021.

Coinbase, “SEC Form S-1 Regulation Statement under the Securities Act 1933: Coinbase Global Inc” (*SEC.Gov*, 25 February 2021) <https://www.sec.gov/Archives/edgar/data/1679788/000162828021003168/coinbaseglobalincs-1.htm> accessed 28 August 2021.

Coinbase, “Wallet” (Coinbase, 2021) <https://wallet.coinbase.com/> accessed 3 August 2021.
CoinDesk, ‘Inside the standards race for implementing FATF’s travel rule’ (Coin Desk, 4 February 2020) <https://www.coindesk.com/inside-the-standards-race-for-implementing-fatfs-travel-rule> accessed 28 August 2021.

Coindesk, “Coindesk” (Coindesk 2021) <https://www.coindesk.com/> accessed 28 August 2021.

Coinmama, “The easiest way to buy and sell cryptocurrency” (Coinmama, 2021) <https://www.coinmama.com/?locale=en> accessed 28 August 2021.

CoinMarketCap, ‘All Cryptocurrencies’ (CoinMarketCap, January 2020) <https://coinmarketcap.com/all/views/all/> accessed 28 August 2021.

Coinmarketcap, ‘Storjcoin X’ (Cryptocurrency Market Capitalizations, 21 November 2017) <https://coinmarketcap.com/currencies/storjcoin-x/#charts> accessed 28 August 2021.

CoinSutra, ‘What is cold storge in cryptocurrency’ (CoinSutra, 12 August 2019) <https://coinsutra.com/cold-storage-cryptocurrency/> accessed 28 August 2021.

Cointelegraph, “Cointelegraph: The future of money” (Cointelegraph. 2021) <https://cointelegraph.com/> accessed 28 August 2021.

Colin Schwarz, ‘Ethereum 2.0: A Complete Guide’ (Medium, 4 July 2019) <https://medium.com/chainsafe-systems/ethereum-2-0-a-complete-guide-d46d8ac914ce> accessed 28 August 2021.

Compliance Tyler, ‘Part Two — How to write a compliance monitoring programme’ (Medium, 14 September 2019) <https://medium.com/@tyler.woollard/part-two-how-to-write-a-compliance-monitoring-programme-7d054ae4c614> accessed 28 August 2021.

Craig Adeyanju, ‘What Crypto exchanges do to comply with KYC, AML and CFT regulations’ (Coin Telegraph, 17 May 2019) <https://cointelegraph.com/news/what-crypto-exchanges-do-to-comply-with-kyc-aml-and-cft-regulations> accessed 28 August 2021.

Crypti, ‘DeFi Grows as Total Value locked Tops $50 Billion” (Crypti, 9 April 2021) <https://crypti.io/defi-grows-as-total-value-locked-tops-50-billion> accessed 28 August 2021.

CryptoKitties, “Getting Started: Breeding” (CryptoKittes, 2021) <https://guide.cryptokitties.co/guide/getting-started> accessed 28 August 2021.

CryptoNews, ‘How to store cryptocurrencies safely in 2020’ (CryptoNews, 2020) <https://cryptonews.com/guides/how-to-store-cryptocurrency-safely.htm> accessed 28 August 2021.

Cynthia Ma, Giles Hawkins, ‘FCA to Supervise Cryptoasset Business under AML/CFT Regime from 10 January 2020’ (Ashfords, December 2019) <https://www.ashfords.co.uk/news-and-media/general/fca-to-supervise-cryptoasset-businesses-under-the-amlcft-regime-from-10-january-2020> accessed 28 August 2021.

Daniel Lesnick, “Crypto AM: Definitively DeFi’s guide to using Uniswap” (CityAM, 26 Setpember 2020) <https://www.cityam.com/crypto-am-definitively-defis-guide-to-using-uniswap/> accessed 28 August 2021.

Danny Nelson, “DeepDotWeb Operator Pleads guilty to laundering $8.4M in Bitcoin Kickbacks’ (*Coindesk*, 31 March 2021) <https://www.coindesk.com/deepdotweb-operator-pleads-guilty-to-laundering-8-4m-in-bitcoin-kickbacks> accessed 28 August 2021.

Danny Nelson, “JPMorgan to Let Clients invest in Bitcoin fund for first time: Sources” (Nasdaq, 26 April 2021) <https://www.nasdaq.com/articles/jpmorgan-to-let-clients-invest-in-bitcoin-fund-for-first-time%3A-sources-2021-04-26> accessed 28 August 2021.

Dmitri Trenin and Pavel Koshkin, “The world after Brexit: From globalisation to fragmentation” (Carngie Moscow Center, 17 August 2016) <https://carnegie.ru/2016/08/17/world-after-brexit-from-globalization-to-fragmentation-pub-64355> accessed 28 August 2021.

Doug Shipp, “Blockchain & Ethereum: Welcome to the Decentralised Internet” (Atomic Object, 12 December 2020) <https://spin.atomicobject.com/2020/12/12/blockchain-ethereum-decentralized/> accessed 28 August 2021.

Electrum, “Electrum Bitcoin Wallet” (Electrum, 2021) <https://electrum.org/#home> accessed 31 August 2021.

Elliptic, ‘Bitcoin money laundering: how criminals use crypto (and how MSBs can clean up their act) (Elliptic, 18 September 2020) < https://www.elliptic.co/our-thinking/bitcoin-money-laundering> accessed 31 August 2021.

Ethereum, ‘Create your own Crypto-Currency with Ethereum’ (*Ethereum*, 2017) <https://www.ethereum.org/token> accessed 31 August 2021.

Ethereum, “Is there any Ether mixer / tumbler available?” (Ethereum, 8 September 2016) <https://ethereum.stackexchange.com/questions/2699/is-there-any-ether-mixer-tumbler-available> accessed 31 August 2021.

Exodus, “Exodus Bitcoin & Crypto Wallet” (Exodus, 2021) <https://www.exodus.com/> accessed 31 August 2021.

Global Legal Insights, “Jersey blockchain and cryptocurrency regulation 2020, second edition” (Carey Olsen, 2020) <https://www.careyolsen.com/sites/default/files/CO_JSY_Blockchain-and-Cryptocurrency-Regulation-2020-2nd-Edition.pdf> accessed 31 August 2021.

Gordon Exall, “Court of Appeal overturns findings of fact: the standard of proof for dishonestly: Also delay of 22 months in giving judgment unacceptable” (Civil Litigation Brief, 18 March 2020) <https://www.civillitigationbrief.com/2020/03/18/court-of-appeal-overturns-findings-of-fact-the-standard-of-proof-for-dishonesty-also-delay-of-22-months-in-giving-judgment-unacceptable/> accessed 31 August 2021.

Gregory Elliehausen, “The cost of banking regulation: a review of the evidence” (IDEAS, 1998) <https://ideas.repec.org/p/fip/fedgss/171.html> accessed 29 August 2021.

ICIG.com, “UK: Ani- Money Laundering Laws and Regulations 2021” (ICIG.com, 25 May 2021) <https://iclg.com/practice-areas/anti-money-laundering-laws-and-regulations/united-kingdom#:~:text=As%20is%20the%20general%20rule,under%20POCA%20or%20the%20Regulations> accessed 31 August 2021.

ICLG.com “UK: Anti-Money Laundering Laws and Regulations 2021” (ICLG.com, 2021) <https://iclg.com/practice-areas/anti-money-laundering-laws-and-regulations/united-kingdom> accessed 31 August 2021.

Infinitus Tech, ‘What You Need to Know About Infinitus’ (Infinitus, 21 August 2018) <https://medium.com/infinitustoken/what-you-need-to-know-about-infinitus-b026190af597> accessed 31 August 2021.

Infinitus, ‘About’ (Infinitus, May 2019) <https://inftech.io/> accessed 9 January 2019.

Jennifer Spencer, “3 Lessons from the Summer of DeFi Boom” (Entrepreneur Europe, 8 November 2020) <https://www.entrepreneur.com/article/358661> accessed 12 May 2021.

John Biggs, ‘How to run a Token sale’ (*Tech Crunch*, 22 September 2017) <https://techcrunch.com/2017/09/22/how-to-run-a-token-sale/> accessed 31 August 2021.

Kevin Helms, “Turkish Crypto Exchange Exit Scam: CEO Flees Country, 62 People Detained, Users cannot access $2 Billion of Funds” (Bitcoin.com, 24 April 2021) <https://news.bitcoin.com/turkish-crypto-exchange-exit-scam-ceo-flees-country-people-detained-users-cannot-access-2-billion-funds/> accessed 31 August 2021.

Kevin Kelleher, ‘The gold rush days of bitcoin mining are over, and not because of the price’ (Ideas, 22 December 2014) <https://qz.com/316898/the-gold-rush-days-of-bitcoin-mining-are-over-and-not-because-of-the-price/> accessed 31 August 2021.

Kiran Vaidya, “Origins and Philosophical ideology behind Bitcoin” (Medium, 11 November 2016) <https://medium.com/all-things-ledger/origins-and-philosophical-ideology-behind-bitcoin-680f09a6a063> accessed 31 August 2021.

Kraken, ‘About’ (Kraken, 2017) < https://www.kraken.com/en-gb/about> accessed 31 August 2021.

Kraken, “Buy Bitcoin and Crypto” (Kraken, 2021) <https://www.kraken.com/en-gb/> accessed 31 August 2021.

Lexis Nexis, ‘North American Financial Services Firms Spend More than $31.5 Billion a Year on Anti-Money Laundering Compliance According to LexisNexis Risk Solution Study’ (LexisNexis, 23 July 2019) <https://risk.lexisnexis.com/about-us/press-room/press-release/20190723-true-cost-aml> accessed 31 August 2021.Lexology, “Law Commission Suspicion” (Lexology, 20 January 2020) <https://www.lexology.com/library/detail.aspx?g=4766a27f-d2c0-4896-914c-0f4f853a53a3> accessed 31 August 2021.

Libra, ‘Welcome to the official Libra White Paper’ (Libra, 2020) <https://libra.org/en-US/white-paper/> accessed 31 August 2021.

Luke Conway, “Best Crypto Exchanges” (Investopedia, 9 April 2021) <https://www.investopedia.com/best-crypto-exchanges-507185> accessed 31 August 2021.

Lynn Paine, “Managing for Organisational Integrity” (Harvard Business Review, April 1994) <https://hbr.org/1994/03/managing-for-organizational-integrity> accessed 31 August 2021.

Magdalena Roibu, “A Bit(coin) dirty. The new means of money laundering” (Schonherr, 1 February 2021) <https://www.schoenherr.eu/content/a-bit-coin-dirty-the-new-means-of-money-laundering/> accessed 31 August 2021.

Marie Huillet, “Turkish police detained 62 over $2B Thodex crypto exchange fraud” (*CoinTelegraph*, 23 April 2021) <https://cointelegraph.com/news/turkish-police-detain-62-over-alleged-2b-thodex-crypto-exchange-fraud> accessed 31 August 2021.

Mark DeCambre, ‘Here’s how bitcoin could soon be worth $146,000 according to JPMorgan’ (Market Watch, 6 January 2021) <https://www.marketwatch.com/story/heres-how-bitcoin-could-soon-be-worth-146-000-says-jpmorgan-11609869356> accessed 31 August 2021.

Martin Young, “Coinbase’s Reddit AMA: It’s like Amazon in the early days” (Cointelegraph, 24 March 2021) <https://cointelegraph.com/news/coinbase-s-reddit-ama-it-s-like-amazon-in-the-early-days> accessed 31 August 2021.

Michael Lovaglia and Brent Simpson, “Elementary Theory: 25 Years of Expanding Scope and Increasing Precision” (*Research Gate*, August 2014) <https://www.researchgate.net/publication/285985192_Elementary_Theory_25_Years_of_Expanding_Scope_and_Increasing_Precision> accessed 28 August 2021.

Mike Orcutt, ‘A new money-laundering rule is forcing crypto exchanges to scramble’ (MIT Technology Review, 6 February 2020) <https://www.technologyreview.com/f/615151/crypto-fatf-travel-rule> accessed 31 August 2021.

Mike Orcutt, ‘Criminals laundered $2.8 billion in 2019 using crypto exchanges, finds a new analysis’ (MIT Technology Review, 16 January 2020) <https://www.technologyreview.com/f/615064/cryptocurrency-money-laundering-exchanges/> accessed 31 August 2021.

Mike Orcutt, ‘Surprise! Hundreds of ICOs are probably scams’ (MIT Technology Review, 18 May 2018) <https://www.technologyreview.com/f/611170/surprise-hundreds-of-icos-are-probably-scams/> accessed 31 August 2021.

Modulus, “Start your crypto exchange” (Modulus, 2021) <https://www.modulusfe.com/products/data-servers-exchanges/how-to-start-a-bitcoin-exchange-business/#:~:text=Attain%20funding%20for%20venture.,-Before%20starting%20on&text=In%20order%20to%20develop%20and,government%20registration%20and%20initial%20advertising> accessed 31 August 2021.
Monero, ‘Monero: a reasonable private digital currency’ (Monero, 2020) <https://www.getmonero.org/> accessed 10 January 2020.

MyCryptoMixer, “Bitcoin Mixer” (MyCryptoMixer, 2021) <https://mycryptomixer.com/> accessed 31 August 2021.

MyCryptoMixer, “MyCryptoMixer.com: How to mix your coins using the best bitcoin mixer (tumbler) in 2020” (Bitcoin Magazine, 3 August 2020) <https://bitcoinmagazine.com/culture/mycryptomixer-com-how-to-mix-your-coins-using-the-best-bitcoin-mixer-tumbler-in-2020> accessed 31 August 2021.

Nasdaq, ‘Gold – Latest Price & Chart for CBOT Gold’ (*Nasdaq*, 22 November 2011) <http://www.nasdaq.com/markets/gold.aspx> accessed 31 August 2021.

Nathan Reiff, “What is ERC-20 and what does it mean for Ethereum” (Investopedia, 6 September 2020) <https://www.investopedia.com/news/what-erc20-and-what-does-it-mean-ethereum/> accessed 31 August 2021.

Nick Chong, ‘Crypto Industry Execs: This Bitcoin Bear Market is The Best Yet’ (News BTC, 26 March 2019) <https://www.newsbtc.com/2019/03/26/crypto-industry-execs-this-bitcoin-bear-market-is-the-best-yet/> accessed 31 August 2021.

Nikhilesh De, “Libra Rebrands to ‘Diem’ in Anticipating of 2021 Launch” (Coindesk, 1 December 2020) <https://www.coindesk.com/libra-diem-rebrand> accessed 1 August 2021.

Noelle Acheson, ‘Crypto Long & Short: Bitcoin is more than a hedge against inflation – it’s a hedge against crazy’ (Yahoo Finance, 20 December 2020) <https://uk.finance.yahoo.com/news/crypto-long-short-bitcoin-more-220132584.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAALg6sJmfd_03fkigrGu9N9vVe24g2nh2dhNDroXdA_uZcOp1Ssqohblr2Q6ryg_NXLX5ygp18OSp9yYnZMd8-patfDgEwxerDlzpvZy-Y7xJt8p9EZd3hIjCLUTTIu81bJBOxFCDu1AXHI5cAjL-nDNMJoMMOIKK8HS-vbror5iV> accessed 31 August 2021.

PayPal, “Crypto for the people: Now you can discover crypto in the PayPal app” (PayPal, 2021) <https://www.paypal.com/us/webapps/mpp/crypto> accessed 31 August 2021.

Penny Crosman, ‘Crypto money laundering up threshold in 2018: report’ (American Banker, 3 July 2018) <https://www.americanbanker.com/news/crypto-money-laundering-rose-3x-in-first-half-2018-report> accessed 31 August 2021.

Peter Hardy, ‘Art and Money Laundering’ (The National law Review, 20 March 2019) <https://www.natlawreview.com/article/art-and-money-laundering> accessed 31 August 2021.

Peter Loshin and Michael Cobb, “Encryption” (TechTarget, 2021) <https://searchsecurity.techtarget.com/definition/encryption> accessed 31 August 2021.

Polobiex, ‘Welcome to Poloniex – Trade securely on the world’s most active digital asset exchange’ (Polobiex, 2017) <https://poloniex.com/> accessed 31 August 2021.

Rahman Ravelli, “Cryptocurrency Fraud: A Significant Judgment” (Legal 500, 9 February 2021) <https://www.legal500.com/developments/thought-leadership/cryptocurrency-fraud-a-significant-judgement/> accessed 31 August 2021.

Raphael Auer, Giulio Cornelli and Jon Frost, ‘Covid-19, cash and the future of payments’ (BIS, 2 April 2020) <https://www.bis.org/publ/bisbull03.pdf> accessed 10 June 2020.
Reddit, “Reddit: Home” (Reddit, 2021) <https://www.reddit.com/> accessed 31 August 2021.

Rigway Barker, “DeFi: Decentralised finance is on the rise” (WithersWorldWide, 7 August 2020) <https://www.withersworldwide.com/en-gb/insight/defi-decentralized-finance-is-on-the-rise> accessed 31 August 2021.

Satoshi Nakamoto “Bitcoin: A Peer-to-Peer Electronic Cash System” (Bitcoin Blog, October 2008) <https://bitcoin.org/bitcoin.pdf> accessed 31 August 2021.

Sean Williams, ‘Which Cryptocurrencies have the fastest transaction speeds?’ (The Motley Fool, 14 January 2018) <https://www.fool.com/investing/2018/01/14/which-cryptocurrencies-have-the-fastest-transactio.aspx> accessed 31 August 2021.

Sentencing Council, “Corporate offenders: fraud, bribery and money laundering” (Sentencing, 1 October 2014) <https://www.sentencingcouncil.org.uk/offences/magistrates-

court/item/corporate-offenders-fraud-bribery-and-money-laundering/> accessed 31 August 2021.

Shanhong Liu, 'Average energy consumption per transaction for Bitcoin and VISA 2018' (Statista, 2018) < https://www.statista.com/statistics/881541/bitcoin-energy-consumption-transaction-comparison-visa/> accessed 31 August 2021.

Shobhit Seth, 'The five most private cryptocurrencies' (Investopedia, 25 June 2019) <https://www.investopedia.com/tech/five-most-private-cryptocurrencies/> accessed 31 August 2021.

Shobhit Seth, 'The five most private cryptocurrencies' (Investopedia, 24 May 2020) <https://www.investopedia.com/tech/five-most-private-cryptocurrencies/> accessed 31 August 2021.

Shopify, "Alternative Payments: Cryptocurrency" (Shopify, 2021) <https://help.shopify.com/en/manual/payments/alternative-payments/cryptocurrency> accessed 31 August 2021.

Shrimpy, "Top 7 Privacy Coins in 2021 (Shrimpy, 3 March 2021) <https://blog.shrimpy.io/blog/top-7-privacy-coins-in-2021> accessed 31 August 2021.

Sloane Brakeville and Bhargav Perepa, 'Blockchain basics: Introduction to distributed ledgers' (IBM Developers, 18 March 2018) < https://developer.ibm.com/tutorials/cl-blockchain-basics-intro-bluemix-trs/> accessed 31 August 2021.

Stanislaw Drozdz, Jaroslaw Kwapien, Pawel Oswiecimka, Tomasz Stanisz and Marcin Watorek, "Complexity in Economic and Social Systems: Cryptocurrency Market at around COVID-19" (Entropy, 25 August 2020) <https://res.mdpi.com/d_attachment/entropy/entropy-22-01043/article_deploy/entropy-22-01043-v2.pdf> accessed 31 August 2021.

Storj, 'Storj Tocken Update' (Storj, 2017) < https://storj.io/tokensale.html> accessed 31 August 2021.

Tanzeel Akhtar, 'Switzerland's 'Crypto Valley' has started accepting Bitcoin, Ether for Tax payments' (*Coindesk*, 18 February 2021) <https://www.coindesk.com/switzerlands-crypto-valley-has-started-accepting-bitcoin-ether-for-tax-payments> accessed 31 August 2021.

Taylan Bilgic and Firat Kozok, " Turkish Crypto Exchange goes bust as Founder Flees Country" (*Yahoo News*, 22 April 2012) <https://uk.news.yahoo.com/turks-suspect-big-crypto-losses-095946382.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAADv5uAiepR4gUj876WKhbUugIEAJ5x1Trfzpi9m6iQ0ZOlBleyeV69pdqAFtEjEMzFyR2GNYp7t-E7W7navTsvDDU46P_YuA9G0losUgRwYDf0pqnNiVPdzU9eLQSyNxyPZt91Txg_tArC_uuY1c0tpCGv1nX-dGWi_G15nNdQLx> accessed 31 August 2021.

Tom Wilson, ‘Explainer: 'Privacy coin' Monero offers near total anonymity’ (Reuters, 15 May 2019) <https://www.reuters.com/article/us-crypto-currencies-altcoins-explainer/explainer-privacy-coin-monero-offers-near-total-anonymity-idUSKCN1SL0F0> accessed 31 August 2021.

Tom Wilson, “As scrutiny mounts, crypto exchange Binance to wind down derivatives in Europe” (Reuters, 20 July 2021) <https://www.reuters.com/technology/crypto-exchange-binance-wind-down-futures-derivatives-offerings-europe-2021-07-30/> accessed 31 August 2021.

Uniswap, “Decentralised Trading Protocol: Guaranteed Liquidity for millions of users and hundreds of Ethereum applications” (Uniswap, 2021) <https://uniswap.org/> accessed 31 August 2021.

Uniswap, “Introducing Uni” (Uniswap, 16 September 2020) <https://uniswap.org/blog/uni/> accessed 29 April 2021.

University of California Press, “3 Justifications of Practice: Utilitarian and Retributive” (UC Press E-Books Collection, 2021) <https://publishing.cdlib.org/ucpressebooks/view?docId=ft4q2nb3dn&chunk.id=d0e2447&toc.depth=100&toc.id=d0e2430&brand=ucpress> accessed 31 August 2021.

UNN Finance, “Union’s Crypto Default Swap” (Medium, 5 April 2021) <https://medium.com/union-finance-updates-ideas/unions-crypto-default-swap-7a6f7467b38a> accessed 31 August 2021.

Vitalik Buterin, “Vitalik Buterin’s website” (Vitalik Buterin, 2021) <https://vitalik.ca/> accessed 31 August 2021.
Warner Vermaak, “Uniswap vs PancakeSwap”, (CoinMarketCap, 5 March 2021) <https://coinmarketcap.com/alexandria/article/uniswap-vs-pancakeswap> accessed 31 August 2021.

Weusecoins, ‘Bitcoin ATM map how to find and use Bitcoin ATMs’ (Weusecoins, 2020) <https://www.weusecoins.com/en/bitcoin-atms/> accessed 31 August 2021.

Wikipedia, ‘Airdrop (cryptocurrency)’ (Wikipedia, 2020) <https://en.wikipedia.org/wiki/Airdrop_(cryptocurrency)> accessed 31 August 2021.

Wilfred Michael, “13 Best Crypto Exchanges in the UK” (Bitcourier, 2021) <https://bitcourier.co.uk/blog/crypto-exchanges-uk> accessed 31 August 2021.