Pass or play: should regulators address the money laundering risks posed by cryptocurrencies themselves or await legislative reform?

Article

Accepted Version

Pass or Play: Should regulators address the money laundering risks posed by cryptocurrencies themselves or await legislative reform?

1. Introduction

This paper will appraise the benefits and drawbacks of regulator led and legislator led approaches to regulating cryptocurrency activity, contrasting the efficiency and efficacy, the stimuli for responding, and the common inadequacies in regulatory attempts thus far. It will be seen that the regulator led approach is the most efficient, and in the case of the US, the most effective, but the window of opportunity for regulators to lead changes to regulation is closing as governments pay increased attention to cryptocurrencies. The paper contends that while a regulator led approach risks piecemeal reform which can lead to a confusing landscape for regulated entities, effective AML/CTF regulation of cryptocurrencies requires an engaged and proactive regulator, which should be responsive in adapting its practices.

Firstly, the paper will assess the comparative speed with which the regulatory gap can be closed. Speed is an unrefined metric to use to determine which approach is superior, as it does not measure the quality of the regulation. However, the speed at which the regulatory gap is closed is significant, as it follows that the longer the gap remains open, the more it may be exploited. Next, the stimuli for regulation will be analysed, in this section the money laundering and terrorist financing risks associated with cryptocurrencies are categorised as either constant or growing risks, and each

risk factor is assessed to consider the extent to which it was a justification for regulation. Having appraised the stimuli for AML/CTF regulation, the level to which each of the case study jurisdictions has implemented regulation will be critiqued. While the sample size is limited, this section will provide observations on the efficacy of the approaches, which will allow recommendations to be made. Finally, a summary of the main findings is provided with suggestions for further research.

Bitcoin is the first widely known cryptocurrency,[1] created by Satoshi Nakamoto in 2008.[2] Bitcoin is distinguishable from preceding digital currencies by its use of cryptography,[3] and subsequent cryptocurrencies can be seen to have adopted Bitcoin's technology. Cryptography techniques allow for the identity of the sender and receiver of a transfer to be concealed, which, when combined with speed, transnationality, and operating outside of the regulated financial system, present clear money laundering risks. Cryptocurrencies have attracted the attention of international organisations such as the European Union (EU) and the Financial Action Task Force (FATF).[4] This paper will contrast the responses of the United States (US), Australia,

[1] Though widely considered the first cryptocurrency, the original paper proposing Bitcoin references previous proposals for web-based money such as: Dai, W. 'B-Money' (November 1998) <http://www.weidai.com/bmoney.txt> accessed 18 November 2021.
[2] Nakamoto, S. 'Bitcoin: A Peer-to-Peer Electronic Cash System' (31 October 2008) <https://nakamotoinstitute.org/static/docs/bitcoin.pdf> accessed 18 November 2021.
[3] Bitcoin is not the first digital currency; previous digital currencies existed but failed to persist. Examples include 'Beenz' which launched in 1999 and closed in 2001 and 'Flooz' which shut down in January 2002. See: BBC News, 'Business: The Company File - Beenz means business' (16 March 1999) <http://news.bbc.co.uk/1/hi/business/297133.stm> accessed 18 November 2021, Mark W. Vigoroso, 'Beenz.Com Closes Internet Currency Business' (Commerce Times, 17 April 2001) <http://www.ecommercetimes.com/story/12892.html> accessed 18 November 2021, and CNET, E-currency site Flooz goes offline' (2 January 2002) <https://www.cnet.com/news/e-currency-site-flooz-goes-offline/> accessed 18 November 2002.
[4] Established in 1989, the FATF is as "*a policy-making body which works to generate the necessary political will to bring about*" change to Member States AML legislation. In this capacity, the FATF issues 40 Recommendations which it states are the "*International Standards on Combating Money Laundering.*" The Recommendations were first published in 1990, they have been amended regularly, but most notably in 1996, 2001, 2003, and 2012. See: Financial Action Task Force 'Who We Are' <http://www.fatf-gafi.org/about/> accessed 02 February 2022.

and the United Kingdom (UK) to the money laundering risks posed by the development of cryptocurrencies.

Cryptocurrencies are exchanged globally and referred to in similar terms as money, such as ‘currency’ within cryptocurrency, the ‘cash’ in Bitcoin Cash, and the symbol used in Bitcoin’s logo being akin to a monetary symbol. Cryptocurrencies are also traded for fiat currencies, at times for significant sums, notably Bitcoin, which surpassed $68,000 per Bitcoin in November 2021.[5] Cryptocurrencies are virtual currencies, with no physical form, the European Central Bank (ECB) defines a virtual currency as a “*digital representation of value, not issued by a central bank, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money.*”[6] Southall and Taylor trace asymmetric cryptography, the technique used by Bitcoin and many other cryptocurrencies, to proposals made by Chaum in 1981.[7] Asymmetric cryptography involves the use of pairs of alphanumeric keys; senders encrypt messages using a public key, the message can only be unencrypted by the recipient using the corresponding private key.[8] Chaum subsequently suggested the technique could be used to facilitate anonymous payments.[9] This anonymity will be lost if a user’s key were to become public, as then all their transactions may be traced. The anonymity attached to cryptocurrencies is

[5] J. Kollewe, ‘Bitcoin price surges to record high of more than $68,000’ (The Guardian, 9 November 2017) <https://www.theguardian.com/technology/2021/nov/09/bitcoin-price-record-high-cryptocurrencies-ethereum> accessed 14 February 2022.
[6] ECB, ‘Virtual currency schemes – a further analysis’ <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> accessed 11 February 2022 at 2.2
[7] E. Southall and M Taylor ‘Bitcoins’ (2013) 19 (6) Computer and Telecommunications Law Review 177 at p.177.
[8] D. Chaum, ‘Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms. (1981) 24 (2) Communications of the ACM’ 84 at p85-86.
[9] D. Chaum, ‘Blind Signatures for Untraceable Payments’ in: D. Chaum, R.L. Rivest, and A.T. Sherman, eds. *Advances in Cryptology: Proceedings of Crypto 82* (Springer 1982) at p.119.

described as pseudonymous by the United States Government Accountability Office in their 2014 report.[10] This is because, although the users name is unknown, other details are published on the blockchain, such as their Bitcoin address, the time of the transaction, and the amount. The use of keys rather than names allows all transactions to be public and verifiable, ensuring that no coins are spent twice, but retains the anonymity of those transacting. The difference between asymmetric cryptographic messages, as proposed by Chaum, and cryptocurrencies is the presence of a distributed ledger, known as a blockchain, and that part of the message, the value of cryptocurrency being transferred, is public. The cryptocurrency value being transferred is required for the distributed ledger to function, allowing the network to verify transactions.

Money laundering is the process by which criminal proceeds are made to look legitimate; as observed by Stokes, "*it is the process by which criminals cleanse the fruits of their criminal labours.*"[11] Stokes refers to Lilly's definition; "*the process whereby the identity of dirty money that is the proceeds of crime and the real ownership of these assets is transformed so that the proceeds appear to originate from a legitimate source.*"[12] The aim of money laundering is to conceal the origins of the money, and enable criminals to enjoy the benefits of it without reproach. Money laundering may take many forms and may utilise anything that has value.[13] Estimating

[10] United States Government Accountability Office, 'Virtual Currencies: Emerging Regulatory, Enforcement, and Consumer Protection Challenges' (May 2014) <http://gao.gov/assets/670/663678.pdf> accessed 1 February 2022 at p.6.
[11] R. Stokes, 'Virtual money laundering: the case of Bitcoin and the Linden dollar' (2012) 21(3) Journal of Money Laundering Control 221 at 222.
[12] P. Lilley, *Dirty Dealing: The Untold Truth about Global Money Laundering* (London, Kogan Page, 2006).
[13] N. Ryder, 'The Financial Services Authority and Money Laundering: A Game of Cat and Mouse' (2008) 67(3) Cambridge LJ 635.

the extent of money laundering is difficult due to the breadth of the crime and its understandably secretive nature, as a result estimations are unlikely to be accurate. In 2009, the United Nations Office on Drugs and Crime (UNODC) estimated 2.7% of global GDP,[14] equating to $1.6 trillion was being laundered annually.[15] This correlates with the International Monetary Fund (IMF) estimate in 1998, which suggested money laundering could be valued at 2-5% of global GDP.[16] Domestically, the UK Financial Conduct Authority (FCA) estimate that "*£10billion of illicit funds*"[17] passes through the UK financial system; and in the US the Treasury believes "*about $300 billion is generated annually in illicit proceeds.*"[18] The Australian Transaction Reports and Analysis Centre (AUSTRAC) estimate that AUD 200 billion is laundered in the Asia-Pacific region.[19] The issues in quantifying the extent and impacts of money laundering are not limited to monetary terms, other impacts should be considered, money laundering is not a victimless crime. Unger notes that while there are no direct victims of money laundering, "*there are always secondary victims such as family, friends, acquaintances, and society at large.*"[20] Money laundering through cryptocurrencies is a fast growing issue; in 2018, Europol estimated that "*3-4% of the £100bn in illicit*

---

[14] Gross Domestic Product: "*an aggregate measure of production equal to the sum of the gross values added of all residents, institutional units engaged in production (plus any taxes, and minus any subsidies, on products not included in the value of their outputs).*" Organization for Economic Co-operation and Development, 'Gross Domestic Product' <http://stats.oecd.org/glossary/detail.asp?ID=1163> accessed 15 June 2022.

[15] United Nations Office on Drugs and Crime, 'Illicit Money: How Much is Out There?' <http://www.unodc.org/unodc/en/frontpage/2011/October/illicit-money_-how-much-is-out-there.html> accessed 15 June 2022.

[16] International Monetary Fund, 'Money Laundering: The Importance of International Countermeasures' <http://www.imf.org/external/np/speeches/1998/021098.htm> accessed 15 June 2022.

[17] Financial Conduct Authority, 'Anti-Money Laundering Annual Report 2012/13' <http://www.fca.org.uk/static/documents/anti-money-laundering-report.pdf> accessed 15 June 2022.

[18] United States Treasury, 'National Money Laundering Risk Assessment' <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf> accessed 5 September 2019.

[19] AUSTRAC, 'Introduction to Money Laundering' <https://michaelsmithnews.typepad.com/files/money-laundering.pdf> accessed 5 September 2019.

[20] B. Unger & D. v.d. Linde, *Research Handbook on Money Laundering* (Edward Elgar, Cheltenham, 2013) at p.20

proceeds in Europe"[21] were laundered through cryptocurrencies, equating to £3-4 billion, and in 2021, Chainalysis estimated that cryptocurrencies were used to launder over £6.3bn.[22]

Money launderers may be attracted by the levels of anonymity, the speed brought about by automation, and the transnational nature of cryptocurrencies. Irwin *et al* identified the key considerations of money launderers as ease, time, amount laundered, cost, risks mitigated, and chances of detection,[23] arguing that cryptocurrencies appeal due to the levels of anonymity.[24] In 2012, Stokes argued that the "*emergence of new and alternative payment technologies and products pose a genuine money laundering risk*"[25] and that more research is required into cryptocurrencies.[26] Irwin *et al* found that each money launderer will have their own preferences in their techniques, but that "*the more techniques that are used, the more cash can be successfully laundered or concealed.*"[27] Kethineni and Cao found Bitcoin to be the cryptocurrency of choice for criminals, and that dark web market places were being utilised for money laundering and wider criminal activity.[28] Cryptocurrencies provide an additional technique to launder the proceeds of crime, which is clearly being

[21] BBC News, 'Criminals hide 'billions' in crypto-cash – Europol' (12 February 2018) <https://www.bbc.co.uk/news/technology-43025787> accessed 08 October 2019.
[22] Estimated at $8.68bn here: Chainalysis, 'The 2022 Crypto Crime Report' (16 February 2022) <https://go.chainalysis.com/2022-Crypto-Crime-Report.html> accessed 14 April 2022 at p10. £6.3bn estimate reached based on an average USD/GBP 2021 exchange rate of $1.3757/£1: Office for National Statistics, 'Average Sterling exchange rate: US Dollar XUMAUSS' (11 April 2022) <https://www.ons.gov.uk/economy/nationalaccounts/balanceofpayments/timeseries/auss/mret> accessed 14 April 2022.
[23] A. S. M. Irwin, R.K.K. Choo, and L. Liu, 'An analysis of money laundering and terrorism financing typologies' (2012) 15(1) Journal of Money Laundering Control 85 at 100.
[24] Ibid at 99.
[25] R. Stokes, 'Virtual Money Laundering: The Case of Bitcoin and the Linden Dollar' (2012) 21(3) Information and Communications Technology Law 221 at 231.
[26] ibid at 232.
[27] A. S. M. Irwin, R.K.K. Choo, and L. Liu, 'An analysis of money laundering and terrorism financing typologies' (2012) 15(1) Journal of Money Laundering Control 85 at 105.
[28] S. Kethineni and Y. Cao, 'The Rise in Popularity of Cryptocurrency and Associated Criminal Activity' (2020) 30(3) International Criminal Justice Review 325 at 337.

utilised by criminals, as demonstrated by convictions.[29] Efforts have been made to begin to address the problem, such as the actions of the Financial Crimes Enforcement Network (FinCEN) in the US,[30] the guidance of the FATF,[31] and the EU's 5th Anti-Money Laundering Directive.[32]

Legislators around the world are extending the powers of regulators to address the perceived gaps in anti-money laundering and counter-terrorism financing (AML/CTF) regulation created by cryptocurrencies but, as demonstrated by some more proactive regulators, the existing powers of regulators means that legislative reform may be unnecessary.[33] This paper will analyse the responses of the US, Australia, and the UK as they provide a contrasting array of approaches to cryptocurrencies; the US was quick to regulate via a regulator led approach, Australia took a legislator led approach, and the UK did neither until it was required to regulate to comply with EU legislation.

---

[29] See examples: J Hall, 'Restraint orders: R. v Teresko (Sergejs) Kingston Crown Court: HH Judge Lodder QC: unreported 11 October 2017' (2018) 1 CLR 81, Department of Justice, U.S. Attorney's Office Southern District of New York, 'Ross Ulbricht, A/K/A "Dread Pirate Roberts," Sentenced in Manhattan Federal Court To Life In Prison' (Manhattan, New York, 29 May 2015) <https://www.justice.gov/usao-sdny/pr/ross-ulbricht-aka-dread-pirate-roberts-sentenced-manhattan-federal-court-life-prison> accessed 05 September 2021, and BBC News, 'Criminals hide 'billions' in crypto-cash – Europol' (12 February 2018) <https://www.bbc.co.uk/news/technology-43025787> accessed 08 October 2021.

[30] FinCEN, 'Guidance - FIN-2013-G001 - Issued: March 18, 2013 - Subject: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies' (18 March 2013) <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf> accessed 06 July 2021 at p3.

[31] Financial Action Task Force, 'Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers' (October 2021) <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf> accessed 12 January 2022.

[32] Council Directive 2018/843/EU of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance) [2018] OJ L 156/43.

[33] For examples responses see: Library of Congress, 'Regulation of Bitcoin in Selected Jurisdictions' (January 2014) <https://tile.loc.gov/storage-services/service/ll/llglrd/2014427360/2014427360.pdf> accessed 09 September 2021.

2. Speed of the Regulatory Response

The regulation of cryptocurrency service providers (CSPs) is possible; and adapting an AML/CTF approach to include CSPs can be achieved in a timely fashion. Both Australia and the US demonstrate that by widening their AML regulation to require CSPs to adhere to customer due diligence (CDD) and reporting requirements, CSPs can be regulated in the same way as traditional financial institutions. Though the result has been similar in both jurisdictions, they have each taken a different method to developing their AML regulation. In the US, FinCEN has taken the lead in a regulatory led widening of the regulatory perimeter,[34] compared to Australia where Parliament has delivered a legislator led widening of the regulatory perimeter.[35]

It is indisputable that a regulator led widening of regulation to cover cryptocurrencies will be significantly quicker than a legislator led one. The position adopted by FinCEN in March 2013 put the US years ahead of other jurisdictions. The US appears to be the first jurisdiction to include cryptocurrencies in its regulation, over four years after Bitcoin's genesis block (Block Zero) was mined in January 2009.[36]

Australia appears to have been the quickest jurisdiction to implement a legislator led expansion of regulation to cover cryptocurrencies and, as with the US regulation, the focus in Australia has been to widen AML/CTF regulation to address cryptocurrencies.

---

[34] FinCEN, 'Guidance - FIN-2013-G001 - Issued: March 18, 2013 - Subject: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies' (18 March 2013) <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf> accessed 06 July 2021.
[35] Through the Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017.
[36] Blockchain.com, 'Block 0' <https://www.blockchain.com/btc/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f> accessed 28 June 2021.

The 2017 amendment to the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act 2006)[37] inserted "*digital currency*"[38] into the definitions section. The definition follows that of the FATF, focussing on the functions of money being performed, but without a government or central authority backing the currency.[39] The terms "*registered digital currency exchange provider*"[40] and "*registrable digital currency exchange service*"[41] were also added to the AML/CTF Act, which recognises the existence of CSPs, and these terms have been added to the list of designated services which are regulated by the AML/CTF Act 2006.[42] The 2017 reforms mean that Australia is compliant with the FATF guidance issued in 2019,[43] before the guidance was released. The legislation came into force on 3rd April 2018, and while Australia has been comparably quick to legislate on cryptocurrency AML/CTF regulation, this was over nine years after Block Zero was mined and five years after FinCEN instigated a regulator led approach in the US.

The UK has been comparably slow to address the AML/CTF risks posed by cryptocurrencies, despite taking advice on the issue relatively early in the development of cryptocurrencies. HM Treasury first issued a call for information in 2014,[44] and in

[37] Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017.
[38] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.5.
[39] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.5: Digital Currency (a)(i)-(ii).
[40] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.5.
[41] ibid.
[42] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.6(2) Item 50A.
[43] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' (21 June 2019) <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2019.
[44] GOV.UK, 'Digital currencies: call for information' <https://www.gov.uk/government/consultations/digital-currencies-call-for-information/digital-currencies-call-for-information> accessed 11 March 2019.

March 2015,[45] published responses stating that the government intended "*to apply anti-money laundering regulation to digital currency exchanges.*"[46] The UK Government failed to follow through on its plan to regulate cryptocurrency exchanges, which could in part be attributed to the protracted fallout from the 2016 EU referendum dominating the political agenda. A further factor in the UK being slow to legislate on cryptocurrencies is that the UK legislature is passing fewer Acts of Parliament per year than it did previously; the average number of Acts of Parliament passed per year between 2010 to 2020 is 31, compared to 38 from 2000-2009, and 54 per year in the 1980s and 90s.[47] The actions of the relevant regulator in the UK, the FCA, have been described as feeble by the Treasury Committee, and it argued that more powers should be granted to the FCA.[48] Ultimately, the UK regulation of cryptocurrencies has been supranational legislator led rather than the domestic approaches taken by the US and Australia; the UK was required to extend AML/CTF regulation to cover cryptocurrencies in order to comply with the 5th Anti-Money Laundering Directive of the EU.[49] In December 2019, five years after the initial consultation, and nearly 11 years after Block Zero was mined, cryptocurrency activities were regulated in the UK for AML/CTF purposes.[50]

---

[45] GOV.UK, 'Digital currencies: response to the call for information' <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf> accessed 11 March 2022.
[46] ibid.
[47] All figures based on data gathered from: Legislation.Gov, 'Your search for UK Public General Acts has returned more than 200 results' <https://www.legislation.gov.uk/ukpga> accessed 20 September 2022.
[48] Treasury Committee, *Crypto-assets* (HC 2017-19, 910) p.43 para 21.
[49] Council Directive 2018/843/EU of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance) [2018] OJ L 156/43.
[50] The Money Laundering and Terrorist Financing (Amendment) Regulations 2019, SI 2019/1511.

Regulator led responses to any novel issue will always be quicker than the process required to enact legislation. FinCEN demonstrates this point clearly, it has applied AML/CTF regulation to CSPs since 2013. Efficient legislators can enact reforms quickly in specific circumstances, but time in the chambers of legislative bodies is prioritised based on political pressures. While providing testimony to the US Senate, Nelson observed that the international landscape is a patchwork of attitudes, proactivity, and levels of regulation, and called for harmonisation across countries.[51] Cryptocurrencies do not currently command the level of attention apportioned to other issues; this is clearly illustrated by the protracted route to regulation in the UK.

3. Stimuli for Regulation

The development of cryptocurrencies has brought with it new opportunities for criminals; the FATF first considered cryptocurrencies in 2014, identifying the potential AML/CTF risks,[52] and other pertinent organisations and bodies such as the EU,[53] and the IMF,[54] have since considered the crime threats. The FATF and the EU promote a 'risk-based approach' to preventing and detecting financial crime.[55] A risk-based

[51] R. M. Nelson, 'Statement of Rebecca M. Nelson before U.S. Senate Committee on Banking, Housing, and Urban Affairs' (30 July 2019) <https://www.banking.senate.gov/imo/media/doc/Nelson%20Testimony%207-30-19.pdf> accessed 17 May 2022 at p.14.
[52] Financial Action Task Force, 'Virtual Currencies – Key Definitions and Potential AML/CFT Risks' (27 June 2014) <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 27 July 2021.
[53] R. Houben and A. Snyers, 'Study Requested by the TAX3 Committee: Cryptocurrencies and Blockchain – Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion' (Publications Office of the EU, 6 September 2018) <https://op.europa.eu/en/publication-detail/-/publication/631f847c-b4aa-11e8-99ee-01aa75ed71a1> accessed 24 June 2021.
[54] International Monetary Fund, 'Global Financial Stability Report—COVID-19, Crypto, and Climate: Navigating Challenging Transitions' (Washington, DC, 12 October 2021) <https://www.imf.org/en/Publications/GFSR/Issues/2021/10/12/global-financial-stability-report-october-2021> accessed 25 November 2021.
[55] Financial Action Task Force, 'The FATF Recommendations' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> accessed 05 July 2022 at p62.

approach means enhanced measures must be taken in higher risk circumstances.[56] Higher risk situations include the peculiarity of the business relationship,[57] geographic risk factors,[58] or specific services or transactions deemed to increase the risk.[59] While specific examples of risks are given, the importance of the risk-based approach is in a more general sense; the FATF states that the risk based approach "*should be an essential foundation to efficient allocation of resources*"[60] across AML/CTF regimes.

In keeping with the international approach of a risk-based approach, the risks posed by cryptocurrencies must be assessed, and their influence on a jurisdiction's decision to impose regulation. While there is a broad consensus on the prominent risks of financial crime presented by cryptocurrencies,[61] the risks are so numerous and varied, it is helpful to identify categories of risk as they will be of differing importance for each financial crime. Cryptocurrency financial crime risks can be categorised into two broad categories: constant risks and growing risks. Constant risks are ever-present; these are AML/CTF risks posed by the characteristics of cryptocurrencies such as high levels of anonymity, the concept of decentralisation, and that customer relationships are not established face-to-face.[62] Growing risks relate to both new threats emerging

---

[56] ibid.
[57] ibid.
[58] ibid at p63.
[59] ibid.
[60] ibid at p.9.
[61] The risk factors have been considered by R. Houben and A. Snyers, 'Study Requested by the TAX3 Committee: Cryptocurrencies and Blockchain – Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion' (Publications Office of the EU, 6 September 2018) <https://op.europa.eu/en/publication-detail/-/publication/631f847c-b4aa-11e8-99ee-01aa75ed71a1> accessed 24 June 2021, G. Mantalara, 'An overview of the ML/TF risks and regulatory responses in the crypto-asset landscape' (2021) 36(11) Journal of International Banking Law and Regulation 487, and M. Campbell-Verduyn, 'Bitcoin, crypto-coins, and global anti-money laundering governance' (2018) 69 Crime Law Soc Change 283.
[62] Financial Action Task Force, 'Virtual Currencies – Key Definitions and Potential AML/CFT Risks' (27 June 2014) <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 27 July 2021 at p9.

through the development of cryptocurrency technology and services, and constant risks being exacerbated by the increasing numbers of cryptocurrency participants and service providers.[63] Constant risks and growing risks are stimuli for jurisdictions to regulate cryptocurrencies. Furthermore, the two types of risk lead to a third category of stimuli: external influence from international organisations whose attention has been drawn to the constant and growing risks posed by cryptocurrencies.

3.1. Constant Risks

The potential to use cryptocurrencies for criminal purposes, or to avoid AML/CTF regulation, is a constant threat due to the characteristics of cryptocurrencies and appears to be the biggest motivator for jurisdictions to reform their AML/CTF regulation.

Cryptocurrencies have been linked to numerous scandals and incidents of criminal activity, examples include the dark web marketplace Silk Road,[64] the collapse of the MtGox exchange in February 2014,[65] and that Bitcoin is the preferred payment method for ransomware demands, such as in the 'WannaCry' cyber-attack on the NHS in May 2017.[66] The FATF found the key appeal of cryptocurrencies for criminals were

[63] Financial Action Task Force, 'Virtual Currencies – Key Definitions and Potential AML/CFT Risks' (27 June 2014) <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 27 July 2021 at p10.
[64] FBI New York, 'Ross Ulbricht, the Creator and Owner of the Silk Road Website, Found Guilty in Manhattan Federal Court on All Counts' (5 February 2015) <https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/ross-ulbricht-the-creator-and-owner-of-the-silk-road-website-found-guilty-in-manhattan-federal-court-on-all-counts> accessed 26 July 2021.
[65] BBC News, 'MtGox bitcoin exchange files for bankruptcy' (28 February 2014) <https://www.bbc.co.uk/news/technology-25233230> accessed 07 October 2022.
[66] BBC News, 'NHS cyber-attack: GPs and hospitals hit by ransomware' (13 May 2017) <https://www.bbc.co.uk/news/health-39899646> accessed 02 September 2021.

anonymity levels, decentralisation, and their inherently global nature.[67] In 2014, the National Crime Agency (NCA) in the UK concluded that the criminal risks of cryptocurrencies were principally through online marketplaces,[68] which while clearly a threat, showed a lack of foresight for other criminal applications, such as ransomware, money laundering, and fraud. As noted by Ryder,[69] the NCA repeated this position in a 2018 consultation,[70] which contrasted with the FCA, who in the same consultation stated that wide-scale criminal activity was taking place.[71] Contrastingly, in Australia in 2015, the Senate Economics References Committee in Australia received evidence from numerous contributors which all highlighted criminal threats of cryptocurrencies.[72] The committee gave a cautious conclusion, acknowledging both the benefits and the risks of cryptocurrencies, but with regards to AML regulation of cryptocurrencies; it recommended a statutory review which "*considers applying AML/CTF regulations to digital currency exchanges.*"[73] The advice of the committee

[67] Financial Action Task Force, 'Virtual Currencies – Key Definitions and Potential AML/CFT Risks' (27 June 2014) <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 27 July 2021 at p9-10.
[68] GOV.UK, 'Digital currencies: response to the call for information' <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf> accessed 11 July 2021 at 3.2.
[69] N. Ryder, 'Cryptoassets, social media platforms and defence against terrorism financing suspicious activity reports: a step into the regulatory unknown' (2020) 8 Journal of Business Law 668 at 684.
[70] House of Commons Treasury Committee, *Crypto-assets Twenty-Second Report of Session 2017–19* (2018) at p25.
[71] Financial Conduct Authority, "Financial Conduct Authority's Written Submission on Digital Currencies" (April 2018), http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/treasury-committee/digital-currencies/written/81677.pdf> accessed 18 September 2022 at para 29.
[72] Parliament of Australia, 'Digital Currency – Game Changer or bit player' (August 2015) <http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Digital_currency/~/media/Committees/economics_ctte/Digital_currency/report.pdf> accessed 21 July 2021from 3.1.
[73] ibid at para 6.37.

was adopted, and a statutory review published its findings in 2016,[74] which ultimately led to an amendment of the AML/CTF Act 2006 in 2017.[75]

The growing awareness of constant risks being a stimulus for regulation is illustrated by the response of the regulator in the US. It was in 2013, the same year that the FBI took down the Silk Road dark web marketplace,[76] that FinCEN specified that its guidance applied to exchanges of convertible virtual currencies and thereby determined that such exchanges were subject to the Bank Secrecy Act 1970.[77] It is clear that US authorities were aware of the potential for criminal activity to involve cryptocurrencies, given that they were investigating high profile instances of such activity.

The US and Australia responded to the perceived criminal risks of cryptocurrencies by promptly widening AML/CTF regulation, in the US this was regulator led compared to being legislator led in Australia. The UK concluded that AML/CTF regulation should be imposed,[78] but failed to act in a prompt manner; taking until 2020 to do so,[79] five

[74] See Recommendations 4.11-13 in: Australian Government: Attorney-General's Department, 'Report on the Statutory Review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and Associated Rules and Regulations' (April 2016) <https://www.austrac.gov.au/sites/default/files/2019-07/report-on-the-statutory-review-of-the-anti-money-laundering.pdf> accessed 18 May 2022 at p53.
[75] Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017.
[76] FBI New York, 'Ross Ulbricht, the Creator and Owner of the Silk Road Website, Found Guilty in Manhattan Federal Court on All Counts' (5 February 2015) <https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/ross-ulbricht-the-creator-and-owner-of-the-silk-road-website-found-guilty-in-manhattan-federal-court-on-all-counts> accessed 26 July 2021.
[77] FinCEN, 'Guidance - FIN-2013-G001 - Issued: March 18, 2013 - Subject: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies' (18 March 2013) <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf> accessed 06 July 2021 at p1.
[78] GOV.UK, 'Digital currencies: call for information' (March 2015) <https://www.gov.uk/government/consultations/digital-currencies-call-for-information/digital-currencies-call-for-information> accessed 11 July 2021 at 4.2.
[79] The Money Laundering and Terrorist Financing (Amendment) Regulations 2019, SI 2019/1511.

years after the consultation and ultimately after an EU Directive compelling regulation, which was the principal stimulus rather than the UK consultation process.

3.2. Growing Risks

A jurisdiction will face more pressure to regulate if the subject of the regulation is affecting a considerable proportion of the population. The FATF found the risks posed by cryptocurrencies are "*exacerbated by the rapidly evolving nature of decentralised virtual currency technology and business models,*"[80] which leads to increasing numbers of participants and types of service providers.[81] In December 2019, the FCA estimated that 80% of UK cryptocurrency holdings were held by just 1% of the population,[82] and that 50% of people who had bought cryptocurrency had under £260 worth.[83] These statistics suggest that the industry is not popular enough to be of concern for the FCA. The findings in the UK are mirrored in Australia as the Reserve Bank's 2019 Consumer Payments Survey found that while over 80% of respondents had heard of cryptocurrencies, less than 1% used them.[84] While the proportion of the population using cryptocurrencies is still low, the equivalent values in fiat currency add to the level of risk posed.

---

[80] Financial Action Task Force, 'Virtual Currencies – Key Definitions and Potential AML/CFT Risks' (27 June 2014) <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 27 July 2021 at p10.
[81] Financial Action Task Force, 'Virtual Currencies – Key Definitions and Potential AML/CFT Risks' (27 June 2014) <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 27 July 2021 at p10.
[82] Financial Conduct Authority, 'Infographic: Cryptoasset consumer research 2020' (December 2019) <https://www.fca.org.uk/publication/documents/crypto-assets-infographic.pdf> accessed 22 July 2021.
[83] Financial Conduct Authority, 'Infographic: Cryptoasset consumer research 2020' (December 2019) <https://www.fca.org.uk/publication/documents/crypto-assets-infographic.pdf> accessed 22 July 2021.
[84] J. Caddy, L. Delaney, C. Fisher, and C. Noone, 'Consumer Payment Behaviour in Australia' (Reserve Bank of Australia, 19 March 2020) <https://www.rba.gov.au/publications/bulletin/2020/mar/consumer-payment-behaviour-in-australia.html#r2> accessed 27 July 2021.

The value of cryptocurrencies in fiat money is important; if cryptocurrencies are of too low a value, then they will be less appealing to criminals seeking to launder their illicit proceeds. In 2014, Irwin *et al* found that although the levels of anonymity provided were appealing for criminals, money laundering through virtual environments and virtual currencies was too labour intensive for operations over AUD 300,000.[85] While the values of cryptocurrencies are relevant to the likelihood of them being used to launder money, it is not a factor which is used to determine which cryptocurrencies face AML/CTF regulation. The focus of the FATF has been on what it describes as convertible decentralised virtual currencies,[86] and it has focused its guidance on the intersections between fiat money and cryptocurrencies.[87] There is no threshold value which triggers regulation, but it can be seen that the US regulated when one Bitcoin, the most prominent and valuable cryptocurrency, was worth less than $100, compared to Australia at $7,456, and the UK at $8,166.

[85] A.S.M. Irwin, J.A. Slay, R.K.K. Choo, and L. Lui, 'Money laundering and terrorism financing in virtual environments: a feasibility study' (2014) 17(1) Journal of Money Laundering Control 50 at p70.
[86] Financial Action Task Force, 'Virtual Currencies – Key Definitions and Potential AML/CFT Risks' (27 June 2014) <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 27 July 2021 at p9.
[87] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' (21 June 2019) <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 07 July 2021 at para 3.

Figure 1: Historical Value of Bitcoin[88]

The value of Bitcoin can be seen to rise and fall in a lurching manner, but the early extension of AML/CTF regulation by FinCEN to cryptocurrencies appears to be more linked to the convertible nature of cryptocurrencies and the presence of a regulatory gap, rather than the values in fiat currency. The focus of the guidance issued by FinCEN in 2013 related to the exchange of cryptocurrency for fiat money, but no reference was made to the equivalent value of the cryptocurrency.[89] It is also difficult to infer that the UK or Australia decided to regulate based on a specific change in value as they took legislator led approaches, so the date of enactment will come long after the legislators first decided to propose regulation.

A further area of growing risk concerned with cryptocurrencies is evolution of technology, both within existing cryptocurrencies new ones.[90] With regards to growing

[88] Produced using data from: XE, 'XBT to USD Chart' (updated daily) <https://www.xe.com/currencycharts/?from=XBT&to=USD&view=10Y> accessed 23 July 2021.
[89] FinCEN, 'Guidance - FIN-2013-G001 - Issued: March 18, 2013 - Subject: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies' (18 March 2013) <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf> accessed 06 July 2021 at p3.
[90] Kethineni and Cao found that while Bitcoin was the most popular, other cryptocurrencies have started to be adopted by criminals, see: S. Kethineni and Y. Cao, 'The Rise in Popularity of Cryptocurrency and Associated Criminal Activity' (2020) 30(3) International Criminal Justice Review 325 at 334.

risks within existing cryptocurrencies, mixer services have been developed to defeat the traceability of transactions on the blockchain.[91] Mixer services group transactions in such a manner that it is not clear which inputs relate to which outputs from a transaction.[92] The outside observer will simply see a list of inputs to a transaction and a list of outputs which will be of differing values. Examples of growing AML/CTF risks posed by new cryptocurrencies include the development of more privacy orientated cryptocurrencies, such as Monero, which publish much more limited information on their blockchains.[93] Privacy coins and ring signatures pose a risk, as they are harder to trace than cryptocurrencies following the Bitcoin model, however, cryptocurrency innovations have quickly become akin to cat and mouse, with cryptocurrency tracking services quickly developing relevant tools.[94] These developments are in the private sector, and not instigated by regulators or law enforcement agencies.

Concerns over the constant and growing AML/CTF threats posed by cryptocurrencies are not limited to nation states, prominent international organisations have begun assessing, advising, and in the case of the EU, legislating cryptocurrency activity for AML/CTF purposes.

---

[91] J. Levin, 'Written Testimony of Jonathan Levin Co-Founder and Chief Strategy Officer Chainalysis Inc. Before the Senate Banking Committee' (17 March 2022) <https://www.banking.senate.gov/imo/media/doc/Levin%20Testimony%203-17-223.pdf> accessed 17 May 2022 at p.27.

[92] The FATF identified mixers as an AML/CTF risk in 2014: Financial Action Task Force, 'Virtual Currencies – Key Definitions and Potential AML/CFT Risks' (27 June 2014) <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 27 July 2021.

[93] Privacy coins are growing in popularity with criminals as identified by Keatinge *et al*: T. Keatinge, D. Carlisle and F. Keen, 'Virtual currencies and terrorist financing: assessing the risks and evaluating responses' (study commissioned by the Directorate General for Internal Policies, Policy Department for Citizens' Rights and Constitutional Affairs, May 2018) at pp32-33.

[94] As evidence by the findings of: M. Möser, K. Soska, E. Heilman, K. Lee, H. Heffan, S. Srivastava, K. Hogan, J. Hennessey, A. Miller, A. Narayanan, and N. Christin, 'An Empirical Analysis of Traceability in the Monero Blockchain' (2018) 3 Proceedings on Privacy Enhancing Technologies 143 at 158.

3.3. Influence of International Organisations and Bodies

Whilst the US and Australia were stimulated to regulate cryptocurrencies due to the AML/CTF risks they pose, the UK only acted because it was compelled by an EU Directive to regulate cryptocurrencies. By the time the UK regulated, both the EU and the FATF had attempted to address the AML/CTF risks cryptocurrencies pose. Assessing the points in time at which each of the three jurisdictions regulated, it is clear that the FATF was not the stimulus for the US or Australia, as their regulation was in place before the FATF issued its detailed guidance. While the UK implemented its regulation after the FATF guidance was issued, it is also clear that the 5th Anti Money Laundering Directive of the EU compelled the UK to regulate. This section will consider the roles of the FATF and the EU in developing international best practice in cryptocurrency AML/CTF measures.

The FATF has been the most proactive international body in addressing the AML/CTF threats posed by cryptocurrencies, publishing three guidance documents on the issue, and two reports.[95] Despite this, without a clear statement from a jurisdiction it is difficult for the FATF to be seen as the stimulus for regulation, as its recommendations are not legally binding.[96] In June 2019, the FATF published guidance for applying the risk-based approach to cryptocurrencies, this recommend the regulation of the entities

[95] Financial Action Task Force, 'Publication Search: Virtual Currencies' <https://www.fatf-gafi.org/publications/?hf=10&b=0&q=Virtual%2520Currencies&s=desc(fatf_releasedate)> accessed 25 July 2021.

[96] Alexander notes that while the not legal binding, the FATF has set specific recommendations and mandatory for membership, see: K Alexander, 'The International Anti-Money-Laundering Regime: The Role of the Financial Action Task Force' (2001) 4(3) JMLC 231 at p.241.

which can be regulated.[97] The FATF guidance recommends that states apply AML/CTF regulation to "*both where those activities intersect with the regulated fiat currency financial system*"[98] and where the activities "*consist only of "virtual-to-virtual" interactions*."[99] As noted by Alexander, although the Recommendations of the FATF are "*non-binding in a legal sense, some of the 40 Recommendations have become mandatory.*"[100] Such mandatory Recommendations include criminalising money laundering and implementing 'know your customer' protocols.[101] The Recommendations are strengthened through the use of sanctions which Alexander describes as "*a series of graduated steps designed to pressure members to enact the necessary reforms to achieve compliance*."[102]

However, it was not the legal regime set out by the FATF that prompted the UK to regulate. The UK achieved a high level of compliance with the FATF Recommendations in its 2018 mutual evaluation, but this was based on regulation that predated both the FATF's cryptocurrency guidance and the 2019 reforms to widen the UK's regulation to include cryptocurrencies. The influence of the FATF does not appear prominent for the US or Australia either, both jurisdictions implemented their regulation prior to the FATF issuing their cryptocurrency guidance. The FATF mutual evaluation of the US in 2016 noted that FinCEN applied AML/CTF regulation to

[97] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' (21 June 2019) <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 07 July 2021.
[98] ibid at p18 para 52.
[99] ibid.
[100] K Alexander, 'The International Anti-Money-Laundering Regime: The Role of the Financial Action Task Force' (2001) 4(3) JMLC 231 at p.240.
[101] ibid at 231.
[102] ibid at 240.

cryptocurrency exchanges,[103] and the 2015 mutual evaluation of Australia observed that AUSTRAC was conducting research.[104] As has already been observed, the US and Australia regulated based on the constant risks posed, whereas for the UK, the stimulus for regulation was the EU.

The EU has been developing AML/CTF legislation since 1991,[105] but its legislation only included cryptocurrencies in 2018.[106] Unlike the FATF Recommendations, EU directives are legally binding, with Member States being required to meet the standards set by the directive.[107] Member States can choose the most suitable form and methods to meet such standards. The first directive was criticised for lacking specificity, leading to incoherent standards;[108] however, the EU AML/CTF directives have become more prescriptive with each iteration, promoting a more consistent approach across the EU.[109] The influence of EU directives on UK law is clear with legislative reform closely following updated directives. The Money Laundering

[103] Financial Action Task Force, 'Anti-money laundering and counter-terrorist financing measures: United States Mutual Evaluation Report' (December 2016) <https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-States-2016.pdf> accessed 14 April 2022 at p.44.
[104] Financial Action Task Force, 'Australia – Mutual Evaluation Report – April 2015' <http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Report-Australia-2015.pdf> accessed 05 September 2019 at p161.
[105] Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering [1991] OJ L166/77.
[106] Council Directive 2018/843/EU of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance) [2018] OJ L 156/43.
[107] Article 288 TFEU [2016] OJ C 202/47.
[108] V. Mitsilegas and B. Gilmore, 'The EU legislative framework against money laundering and terrorist finance: a critical analysis in light of evolving global standards' (2007) 56(1) International and Comparative Law Quarterly 119 at 120
[109] AML compliance has become a condition of membership of the EU, and the third AML Directive incorporated the risk based approach and due diligence requirements, as discussed by Ryder in: N. Ryder *Money Laundering - An Endless Cycle?: A Comparative Analysis of the Anti-Money Laundering Policies in the United States of America, the United Kingdom, Australia and Canada* (Routledge, London, 2012) at p.34.

Regulations 2007[110] were enacted to comply with the 3rd Anti-Money Laundering Directive,[111] which was superseded by the 4th Anti-Money Laundering Directive[112] and subsequently the Money Laundering Regulations 2007 were replaced by the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.[113] The fourth directive was replaced by the fifth directive,[114] which, despite the ongoing withdrawal of the UK from the EU, was adopted through an amendment to the 2017 Regulations.[115] By implementing the 5th Anti-Money Laundering Directive in December 2019, the UK took a supranational legislator led approach to regulating cryptocurrencies for AML/CTF purposes.

3.4. Summary

Given the position of a regulator, and their ability to act faster than a legislator, the direction a jurisdiction takes with regards to how it regulates cryptocurrencies is in the hands of the regulator. If a regulator fails to take decisive action, then the legislator will have to act, or in the case of the UK, be compelled to act by international organisations. It is arguable that legislators do not need to act where regulators already have the

[110] The Money Laundering Regulations 2007 S.I. 2003/3075.
[111] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system For the Purpose of Money Laundering and Terrorist Financing [2005] OJ L.309/15.
[112] Directive 2015/849/EU of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC [2015] OJ L.141/73.
[113] Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 S.I. 2017/692.
[114] Council Directive 2018/843/EU of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance) [2018] OJ L 156/43.
[115] The Money Laundering and Terrorist Financing (Amendment) Regulations 2019, SI 2019/1511.

required powers to expand their supervision to include cryptocurrencies, which was the case in the US.

A proactive regulator is required for the regulator led approach to be followed, if the regulator does not react, then direction is required from legislators; in both the UK and Australia, even though the regulator had the powers and means to regulate cryptocurrencies, they did not and required legislative reform. In the UK, prior to the 2019 amendment, Regulation 3 of the Money Laundering Regulations defined a 'money services business' as "*an undertaking which by way of business operates a currency exchange office, transmits money (or any representations of monetary value) by any means or cashes cheques which are made payable to customers.*"[116] Cryptocurrencies can be exchanged for fiat money, and the FCA could have applied AML/CTF regulation to cryptocurrencies in the same way as FinCEN did in the US. Instead, the FCA has repeatedly stated that it does not regulate cryptocurrencies. The leading lines of advice on the relevant page of the FCA website state that cryptocurrencies are "*considered very high risk, speculative investments*"[117] and those buying them should be prepared to lose all their money.[118] Similarly to the FCA, AUSTRAC did not show proactivity in widening AML/CTF regulation to cryptocurrencies; in 2015 it advised the Australian Parliament that legislative reform was needed for it to regulate cryptocurrencies.[119] AUSTRAC also stated that while

[116] Money Laundering Regulations 2017, Regulation 3(1)(d).
[117] Financial Conduct Authority, 'Cryptoassets' (07 March 2019, Updated 18 June 2021) <https://www.fca.org.uk/consumers/cryptoassets> Accessed 22 July 2021.
[118] ibid.
[119] Parliament of Australia, 'Digital Currency – Game Changer or bit player' (August 2015) <http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Digital_currency/~/media/Committees/economics_ctte/Digital_currency/report.pdf> accessed 21 October 2019 at para 6.29.

they acknowledged the risks posed by cryptocurrencies, they were not demanding Parliament give them oversight.[120] It is not clear why the UK and Australian regulators chose not to act, as it was increasingly clear cryptocurrencies were going to become part of their responsibilities.

Whereas the responses of the US and Australia were both domestically led and based on the constant AML/CTF risks posed by cryptocurrencies, the UK's reform was in response to the influence of an international organisation, the EU. Ultimately, while the manner of reform is important with regards to the speed with which the regulatory gap is closed, all approaches require a committed regulator as the legislative reforms will be of little effect if they are not implemented by the regulator. The next question to consider is whether the gap in regulation is addressed.

4. Closing the Regulatory Gap

Addressing a regulatory gap quickly is advantageous, as the longer it remains open the more it may be exploited. However, the gap needs to be sufficiently closed, both in the law and the enforcement of it, or the exploitation will simply continue. The US, Australia, and the UK have all implemented AML/CTF regulation of cryptocurrencies, and have addressed the gap on paper, but this section will analyse the extent to which each jurisdiction has implemented the relevant law.

[120] ibid at para 6.29

4.1 US

FinCEN is the regulatory agency with the biggest relationship with cryptocurrencies in the US, due to its role in implementing the Bank Secrecy Act 1970 (BSA 1970).[121] It is the financial intelligence unit (FIU) of the US, as identified by the FATF.[122] As the FIU, FinCEN is the recipient of both suspicious activity reports (SARs)[123] and currency transaction reports (CTRs),[124] and is responsible for deciding whether to take such reports further. FinCEN is also responsible for enforcing AML/CTF compliance.[125] In 2014, the US Government Accountability Office[126] stated that where entities engage in "*virtual currency transactions with U.S. customers or become customers of a U.S. financial institution,*"[127] Prior to this, in 2013, FinCEN already identified cryptocurrency exchanges as money services businesses[128] and took responsibility for regulating such exchanges.[129] FinCEN is responsible for ensuring that such entities comply with AML regulations.[130] AML/CTF supervision only applies to convertible virtual

[121] 31 CFR §1010.810(a), also see: FinCEN, 'What We Do' <http://fin-cenus.com/what-we-do.html> accessed 03 October 2019.
[122] Financial Action Task Force, 'Third Mutual Evaluation Report on Anti-Money Laundering and Combatting the Financing of Terrorism: United States of America' <http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20US%20full.pdf> accessed 28 October 2019.
[123] Required by 31 CFR §§103.18-20 (2002).
[124] Required by 31 CFR §103.22.
[125] FinCEN, 'Law Enforcement Overview' <https://www.fincen.gov/resources/law-enforcement-overview> accessed 30 August 2019.
[126] This office provides "*objective, non-partisan information on government operations. GAO plays a key role in helping Congress improve the performance of government, ensuring transparency and saving money.*" It acts "*at the request of congressional committees or subcommittees or is statutorily required by public laws or committee reports*.": Government Accountability Office 'What GAO Does' <https://www.gao.gov/about/what-gao-does> accessed 19 April 2022.
[127] United States Government Accountability Office, 'Virtual Currencies: Emerging Regulatory, Enforcement, and Consumer Protection Challenges' <http://gao.gov/assets/670/663678.pdf> accessed 04 September 2019 at p.12.
[128] FinCEN, 'Guidance - FIN-2013-G001 - Issued: March 18, 2013 - Subject: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies' (18 March 2013) <https://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf> accessed 06 July 2021 at p2.
[129] ibid at p1.
[130] 31 CFR §1010.810(a) and United States Government Accountability Office, 'Virtual Currencies: Emerging Regulatory, Enforcement, and Consumer Protection Challenges' <http://gao.gov/assets/670/663678.pdf> accessed 04 September 2019 at p.12.

currencies, which have value in fiat currency or may act as a substitute for fiat currency,[131] as a result FinCEN's regulatory remit includes cryptocurrencies.

Implementing and enforcing the BSA 1970 means FinCEN ensures relevant AML/CTF preventative measures are adopted. Such measures can be divided into two categories, reporting requirements which are implemented via CTRs and SARs and CDD which is covered through the know your customer (KYC) protocols. For the regulatory gap to be closed, the two broad categories of AML measures must interrelate; for example, a reporting entity is much better informed in deciding whether to submit a SAR if it has effective KYC provisions in place. FinCEN provides guidance to regulated entities for determining when to report, as well as some 'Red Flags' which may trigger suspicion which would lead to a report.[132] While some of FinCEN's guidance simply restates the law,[133] the guidance provided on Red Flags is more practical as FinCEN gives examples of incidents it believes should trigger suspicion; these include the use of fake identification, customers reacting negatively to requests for identification, transactions very close to the mandatory reporting value, and groups of transactions from multiple customers in a short period of time.[134] A Red Flag should be followed by considering questions such as whether the transaction is "*unusually*

[131] United States Government Accountability Office, 'Virtual Currencies: Emerging Regulatory, Enforcement, and Consumer Protection Challenges' <http://gao.gov/assets/670/663678.pdf> accessed 04 September 2019 at p.13.
[132] FinCEN, 'Reporting Suspicious Activity – A Quick Reference Guide for Money Services Businesses' <https://www.fincen.gov/sites/default/files/guidance/msbsar_quickrefguide.pdf> accessed 14 July 2021.
[133] Such as a transaction is reportable if it suspected to involve money from criminal activity, evade the BSA 1970, or have no apparent legal purpose: FinCEN, 'Reporting Suspicious Activity – A Quick Reference Guide for Money Services Businesses' <https://www.fincen.gov/sites/default/files/guidance/msbsar_quickrefguide.pdf> accessed 14 July 2021.
[134] ibid.

large",[135] whether the transaction outside the customer's normal pattern of business, or whether the frequency of transactions is unusual.[136] The inter-related nature of preventative measures is demonstrated here, as the questions may be best answered if the relevant KYC measures have been observed, and the reporting entity knows what is usual for the customer. Transactions through cryptocurrency businesses are more likely to be viewed as suspicious as they take place remotely. It is more difficult to verify an individual's identity over the internet so the Red Flag incidents relating to identity could be triggered frequently in cryptocurrency businesses, adding to the volume of SARs submitted to FinCEN. The guidance from FinCEN is not definitive as it cannot cover every possible instance of suspicion.[137] FinCEN regulation does not differentiate between exchanges of cryptocurrency for fiat currency and cryptocurrency for other cryptocurrencies which is advantageous as this allows the regulation to apply to a broader set of service providers.

Enforcement actions can act as demonstrations of both the effectiveness of the law to hold non-compliant actors to account, and the effectiveness of a regulator in using their powers. As of now, FinCEN has used its powers four times against those offering exchange services, predominantly exchanging Bitcoins for fiat currencies, apart from one case which only referred to cryptocurrency transactions. Whilst this might be commendable, it is highly likely that there are many others offering similar services continuing to operate without registering with FinCEN, despite this being an obligation.

---

[135] ibid.
[136] ibid.
[137] This is demonstrated by the case law on legal definition of suspicion in English courts, see: *Shaaban bin Hussein* v *Chong Fook Kam* [1970] 2 WLR 441, *K Ltd* v *National Westminster Bank plc (Revenue and Customs Commissioners and another intervening)* [2006] EWCA Civ 1039, *R v Da Silva* [2007] 1 WLR 303, *Shah* v *HSBC Private Bank (UK) Ltd* [2012] EWHC 1283, and Law Commission, *Anti-money laundering: the SARs regime* (Law Com No 384, 2018).

FinCEN is enforcing AML/CTF regulation of cryptocurrencies in the US; fines are being imposed, and the size of the fines imposed are clearly influenced by mitigating or aggravating factors. Deterrence is not mentioned in any of the enforcement notices, but as noted by Ryder,[138] one of FinCEN's objectives is the deterrence of financial crime,[139] therefore it is inferred that a consideration in determining a fine will be deterring others from the same activity. FinCEN has taken enforcement actions against cryptocurrency businesses, such as Ripple Labs,[140] BTC-e and Alexander Vinnik,[141] and Eric Powers.[142] In 2015, Ripple Labs Inc were fined $700,000 for breaching BSA 1970 requirements in what was the first FinCEN enforcement action against a cryptocurrency exchange business.[143] Ripple Labs were found to have acted as a money services business and traded a virtual currency without registering with FinCEN.[144] The case came two years after FinCEN first stated it would regulate cryptocurrency exchanges, and in addition to the financial penalty, Ripple Labs were required to "*conduct a three-year "look-back" to* [review] *suspicious activity reporting*

[138] N. Ryder, *Money laundering – an endless cycle? A comparative analysis of the anti-money laundering policies in the United States of America, the United Kingdom, Australia, and Canada* (Routledge, London, 2012) at p.50.
[139] FinCEN, 'FinCEN's Strategic Plan' <https://www.fincen.gov/about/fincens-strategic-plan> accessed 02 September 2019.
[140] FinCEN, 'FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger' (Washington, 5 May 2015) <https://www.fincen.gov/sites/default/files/enforcement_action/2016-08-02/20150505.pdf> accessed 02 September 2019.
[141] FinCEN, 'In the Matter of BTC-E a/k/a Canton Business Corporation and Alexander Vinnik' (Vienna, United States, 07 June) <2017https://www.fincen.gov/sites/default/files/enforcement_action/2017-07-27/Assessment%20for%20BTCeVinnik%20FINAL2.pdf> accessed 02 September 2019.
[142] FinCEN, 'In the Matter of Eric Powers' (Vienna, United States, 18 April 2019) <https://www.fincen.gov/sites/default/files/enforcement_action/2019-04-18/Assessment%20Eric%20Powers%20Final%20for%20Posting%2004.18.19_1.pdf> accessed 02 September 2019.
[143] FinCEN, 'FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger' (Washington, 5 May 2015) <https://www.fincen.gov/sites/default/files/enforcement_action/2016-08-02/20150505.pdf> accessed 02 September 2019 at p1.
[144] ibid at p1.

for prior suspicious transactions."[145] The 'look-back' demonstrated the commitment of FinCEN to ensuring AML regulations are adhered to, and that as the FIU, any potential intelligence was gathered. A contrasting enforcement action can be seen in July 2017, when a penalty of over $110 million was imposed on BTC-e, and a $12 million penalty imposed on Alexander Vinnik, the operator of the BTC-e exchange.[146] In this case the fines imposed were much larger, as the value of cryptocurrency being transferred was larger than in the Ripple Labs case; BTC-e transferred over $296 million in Bitcoin transactions,[147] as well as a considerable value in transactions in other cryptocurrencies.[148] The value of the transactions was not the only aggravating factor, BTC-e handled over 300,000 Bitcoins which were proceeds from the hacking of Mt. Gox exchange,[149] in which over 700,00 Bitcoins were stolen,[150] and while Ripple Labs agreed to a 'look-back', no such agreement appears in the BTC-e enforcement notice. The BTC-e and Vinnik case demonstrates that the punishments for not complying with FinCEN regulation can be severe, and financial penalties will increase if criminal activity is also discovered. The BTC-e case was linked to a further enforcement action in 2020, against Larry Harmon and his associated businesses in which Harmon was fined $60 million for AML failings in operating a money services business which included over $900,000 worth of transactions with BTC-e.[151] The case was novel as Harmon's activities involved 'mixing' services, which obfuscate cryptocurrency

[145] ibid at p2.
[146] FinCEN, 'In the Matter of BTC-E a/k/a Canton Business Corporation and Alexander Vinnik' (Vienna, United States, 07 June) <2017https://www.fincen.gov/sites/default/files/enforcement_action/2017-07-27/Assessment%20for%20BTCeVinnik%20FINAL2.pdf> accessed 02 September 2019 at p.9.
[147] ibid at p.2.
[148] ibid.
[149] ibid at p.6.
[150] BBC News, 'Top Bitcoin exchange MtGox goes offline' <https://www.bbc.co.uk/news/technology-26333661> accessed 02 September 2019.
[151] FinCEN, 'In the Matter of Larry Dean Harmon d/b/a Helix' (Akron, Ohio, United States, 19 November 2020) <https://www.fincen.gov/sites/default/files/enforcement_action/2020-10-19/HarmonHelix%20Assessment%20and%20SoF_508_101920.pdf> accessed 08 July 2021.

transactions through pooling transactions or breaking the chain of transactions.[152] In 2019, FinCEN imposed a $35,350 fine on Eric Powers.[153] The list of infractions against Powers was similar to previous enforcement actions by FinCEN; Powers was found to have breached a number of BSA 1970 provisions including failing to register with FinCEN, failing to implement an AML program, and failing to report suspicious activity or currency transactions.[154] However, Powers operation was smaller than that of Ripple Labs and BTC-e; Powers conducted over 1,700 transactions,[155] and his most prevalent suspicious customer's transactions equated to $86,000.[156] Furthermore, Powers was not directly implicated in any known crimes, which contrasts with BTC-e and Vinnik which linked to the Mt. Gox incident. FinCEN is clearly utilising the regulator led expansion of AML/CTF regulation to cryptocurrencies in line with its pre-existing enforcement approach.

The approach of FinCEN is commendable, they acted faster than regulators in other jurisdictions, and sooner than other US authorities. However, the multi-regulator landscape in the US demonstrates a weakness of the regulator led approach, which is that the approach can be piecemeal with regulators taking differing approaches. The Federal Reserve has shown limited interest in cryptocurrencies and considers other

[152] FinCEN, 'In the Matter of Larry Dean Harmon d/b/a Helix' (Akron, Ohio, United States, 19 November 2020) <https://www.fincen.gov/sites/default/files/enforcement_action/2020-10-19/HarmonHelix%20Assessment%20and%20SoF_508_101920.pdf> accessed 08 July 2021 at p.18 para 47-51.
[153] FinCEN, 'In the Matter of Eric Powers' (Vienna, United States, 18 April 2019) <https://www.fincen.gov/sites/default/files/enforcement_action/2019-04-18/Assessment%20Eric%20Powers%20Final%20for%20Posting%2004.18.19_1.pdf> accessed 02 September 2019 at p.7.
[154] FinCEN, 'In the Matter of Eric Powers' (Vienna, United States, 18 April 2019) <https://www.fincen.gov/sites/default/files/enforcement_action/2019-04-18/Assessment%20Eric%20Powers%20Final%20for%20Posting%2004.18.19_1.pdf> accessed 02 September 2019 at p.2.
[155] ibid.
[156] ibid at p.5.

threats more pertinent; in 2021 the Fed ranked cryptocurrencies 9th out of 14 in their list of most likely causes of shocks to financial stability.[157] Until 2021, the Securities Exchange Commission (SEC) did not have a clear policy on cryptocurrencies, but the incoming Chair of the SEC has stated that cryptocurrency investments should be regulated by the SEC under its responsibility to protect investors.[158] The Commodities Futures Trading Commission (CFTC) also claim jurisdiction over cryptocurrencies since a ruling against Coinflip in September 2015.[159] The CFTC state that cryptocurrencies meet the definition of a commodity under the Commodity Exchange Act,[160] and therefore trading platforms are subject to CFTC regulation. The CTFC have undertaken a small number of enforcement actions against CSPs in addition to Coinflip,[161] but such actions appear to make up a small percentage of the enforcement activity of the CFTC.[162] With the varying roles of the Federal Reserve, FinCEN, SEC, and CFTC, it is a perilous landscape for a CSP who may not know who they need to comply with to avoid sanction. With regards to closing the regulatory gap, the US has

[157] Board of Governors of the Federal Reserve System, 'Financial Stability Report – May 2021' (Federal Reserve, 06 May 2021) <https://www.federalreserve.gov/publications/files/financial-stability-report-20210506.pdf> accessed 25 June 2021 at p62.
[158] U.S. Securities and Exchange Commission, 'Office Hours with Gary Gensler: The SEC & Cryptocurrencies' (Washington, DC, United States, 16 August 2021) <https://www.youtube.com/watch?v=-kKGkbrwCT0&ab_channel=U.S.SecuritiesandExchangeCommission> accessed 25 August 2021.
[159] CFTC, 'In the Matter of: Coinflip, Inc., d/b/a Derivabit, and Francisco Riordan' (CFTC Docket No. 15-29, 17 September 2015) <https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoinfliprorder09172015.pdf> accessed 26 August 2021 at p3.
[160] 7 USC §1a(9).
[161] See examples: CFTC, 'CFTC Charges 20 Entities for Making False Registration Claims' (Washington, DC, United States, 01 September 2020) <https://www.cftc.gov/PressRoom/PressReleases/8229-20> accessed 26 August 2021, CFTC, 'CFTC Charges BitMEX Owners with Illegally Operating a Cryptocurrency Derivatives Trading Platform and Anti-Money Laundering Violations' (Washington, DC, United States, 01 October 2020) <https://www.cftc.gov/PressRoom/PressReleases/8270-20> accessed 26 August 2021, and CFTC, 'CFTC Charges Two Individuals with Multi-Million Dollar Digital Asset Pump-and-Dump Scheme' (Washington, DC, United States, 05 March 2021) <https://www.cftc.gov/PressRoom/PressReleases/8366-21> accessed 26 August 2021.
[162] See CFTC, 'Enforcement Actions' (Washington, DC, United States, Regularly Updated) <https://www.cftc.gov/LawRegulation/EnforcementActions/index.htm?year=all> accessed 26 August 2021.

not addressed its legislation, because it did not need to, a legislative gap did not exist, and the laws were already drafted widely enough to cover cryptocurrencies. The regulatory gap concerning AML/CTF was closed by FinCEN, and they appear to be enforcing their regulations. However, the reaction to cryptocurrencies in the US demonstrates a key weakness in the regulator led approach, as the other regulators have been less proactive, the broader regulatory landscape is confusing, and gaps remain. Legislation can alleviate this issue, by providing clarity to both the regulated entities and the regulatory agencies.

4.2 Australia

Australia utilised a legislator led widening of the AML/CTF regulatory perimeter via an amendment to the AML/CTF Act 2006.[163] Contrasting with the US approach where the regulator extended regulation itself under the existing law, the Australian Senate instigated the legislative reform to require its regulators to address CSPs.[164] AUSTRAC is the FIU of Australia, with regulatory responsibility for AML/CTF.[165] As the FIU, financial intelligence reports such as threshold transaction reports[166] and suspicious matter reports[167] are sent to AUSTRAC. The FIU then attempts to "*join the*

[163] Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017.
[164] The Senate referred the matter to the Economics References Committee, requesting an inquiry on developing a regulatory system for digital currencies, the Committee recommended the extension of AML/CTF regulation to cover cryptocurrency exchanges: Parliament of Australia, 'Digital Currency – Game Changer or bit player' (August 2015) <http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Digital_currency/~/media/Committees/economics_ctte/Digital_currency/report.pdf> accessed 20 April 2022 at 1.1 and 6.35.
[165] AUSTRAC, 'About AUSTRAC' <http://www.austrac.gov.au/about-us/austrac> accessed 14 July 2021.
[166] Required by Anti-Money Laundering and Counter-Terrorism Financing Act 2006 Part 3 s.43.
[167] Required by Anti-Money Laundering and Counter-Terrorism Financing Act 2006 Part 3 s.41.

dots to provide a complete financial intelligence picture,"[168] and the *"resulting financial intelligence is provided to partner agencies."*[169]

The 2017 amendment inserted "*digital currency*"[170] into the definitions section, which follows the one offered by the FATF: a digital currency performs the functions of money[171] while not being issued by a government or authority,[172] and it is interchangeable with money.[173] Importantly, to distinguish from shop vouchers or local currencies, the definition also requires the currency to be available to the public without restriction on its use as consideration.[174] The terms "*registered digital currency exchange provider*"[175] and "*registrable digital currency exchange service*"[176] have been added to the AML/CTF Act 2006. A registerable digital currency exchange service is defined as exchanging digital currency for fiat currency in the course of a business.[177] A registered digital currency exchange provider is simply anyone carrying out activity meeting the definition of a registerable digital currency exchange service.[178] The effect of the amendments is that businesses conducting exchanges of cryptocurrencies for fiat currencies are required to register with AUSTRAC in order to continue trading. An important gap in the Australian reform is the lack of coverage of inter-cryptocurrency exchanges since an exchange provider converting one cryptocurrency for another will not satisfy the term "*registrable digital currency*

[168] ibid.
[169] ibid.
[170] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.5.
[171] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.5, Digital Currency (a)(i).
[172] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.5, Digital Currency (a)(ii).
[173] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.5, Digital Currency (a)(iii).
[174] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.5, Digital Currency (a)(iv).
[175] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.5.
[176] ibid.
[177] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.6(2) Item 50A.
[178] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.5, Registrable Digital Currency Exchange Service (a).

exchange service" as per item 50A of table 1 in section 6 of the amended AML/CTF Act 2006.[179] This gap could mean that information which may have led to a suspicious matter report may be missed if transactions are first routed through an unregulated cryptocurrency only exchange. A further gap in the regulation is that transactions within a cryptocurrency network are not subject to regulation; an individual can transfer cryptocurrency to another without the need for an exchange service provider.

As explained above, in order to trade, businesses must register with AUSTRAC. Interestingly, the published list of 'digital currency exchange provider registration actions' shows that AUSTRAC has refused registration to three CSPs and cancelled the registration of six more.[180] This is rather concerning. First, the number of registration refusals and revocations appears low when considered against the 246 entities that have been registered up to 16th January 2019.[181] Second, these figures will not include unregulated entities which have not sought AUSTRAC registration for fear, or knowledge, of refusal and have continued to operate regardless. AUSTRAC does provide guidance to digital currency exchange businesses;[182] this guidance is similar to the advice that is given to other regulated entities, save for a few sections which are specific to CSPs.[183] Requirements include completing a risk assessment,

[179] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.6(2) Item 50A.
[180] AUSTRAC, 'Digital currency exchange provider registration actions' (Last updated: 17 May 2021) <https://www.austrac.gov.au/digital-currency-exchange-provider-registration-actions> accessed 12 July 2021.
[181] AUSTRAC, 'Freedom of Information request on 5 December 2018' (25 January 2019) <https://www.austrac.gov.au/sites/default/files/2019-06/AUSTRAC%20Cryptocurrency%20inquiries.pdf> accessed 12 July 2021.
[182] AUSTRAC, 'A guide to preparing and implementing an AML/CTF program for your digital currency exchange business' <https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/guide-preparing-and-implementing-amlctf-program-your-digital-currency-exchange-business> accessed 26 July 2022.
[183] AUSTRAC, 'AML/CTF programs overview' (Last updated: 14 Aug 2020) <https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-

training employees, complying with CDD requirements, and appointing an AML/CTF compliance officer who will be responsible for submitting suspicious matter reports and threshold transaction reports to AUSTRAC.[184]

Whilst the FATF has described AUSTRAC as a "*well-functioning*"[185] FIU, a criticism of AUSTRAC is that the information is collected and maintained but is not utilised frequently enough by State and Territory police forces.[186] AUSTRAC has powers of enforcement, through the AML/CTF Act 2006,[187] which it utilised in November 2017, when Tabcorp was fined $45million,[188] and in June 2018, when the Commonwealth Bank of Australia was fined $700million.[189] Whilst the Tabcorp and Commonwealth Bank fines were viewed in the press as landmark rulings,[190] the list of AUSTRAC enforcement actions is notably short compared to that of FinCEN in the US[191] and the FCA in the UK.[192] The latest fine of $1.3 billion, imposed on Westpac,[193] suggests that

resources/guide-preparing-and-implementing-amlctf-program-your-digital-currency-exchange-business> accessed 12 July 2021.

[184] ibid at p.3.

[185] Financial Action Task Force, 'Australia – Mutual Evaluation Report – April 2015' <http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Report-Australia-2015.pdf> accessed 05 July 2021 at p8.

[186] The FATF identified this as a key weakness as State and Territory police forces conduct the majority of investigations: ibid.

[187] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, Part 15.

[188] *Chief Executive Officer of Australian Transaction Reports and Analysis Centre* v *TAB Limited* (No 3) [2017] FCA 1296.

[189] *Chief Executive Officer of the Australian Transaction Reports and Analysis Centre* v *Commonwealth Bank of Australia Limited* [2018] FCA 930.

[190] P Durkin, '70pc jump in suspicious money laundering transactions: AUSTRAC' *Financial Review* (Melbourne, 18 October 2018) <https://www.afr.com/business/banking-and-finance/70pc-jump-in-suspicious-money-laundering-transactions-austrac-20181018-h16szs> accessed 24 July 2022.

[191] FinCEN have published 70 enforcement actions since 2006: FinCEN, 'Enforcement Actions' (18 April 2019) <https://www.fincen.gov/news-room/enforcement-actions> accessed 23 October 2022.

[192] The FCA have issued a similar number of fines in 2019 to total number of actions AUSTRAC has taken in its lifetime: FCA, '2019 Fines' (11 October 2019) <https://www.fca.org.uk/news/news-stories/2019-fines> accessed 23 October 2022.

[193] *Chief Executive Officer of the Australian Transaction Reports and Analysis Centre* v *Westpac Banking Corporation* [2020] FCA 1538.

AUSTRAC is focused on high-profile enforcement actions. There have been no AUSTRAC enforcement actions against CSPs to date.

Regulators in Australia have been reluctant to take responsibility for cryptocurrencies; both AUSTRAC and the Australian Securities and Investments Commission (ASIC) have been unwilling to apply regulation. AUSTRAC have recognised risks, but in 2015 stated that they were not demanding Parliament give them oversight,[194] and in 2019, Latimer and Duffy argued that although ASIC has the power to impose regulation, it has not done so.[195] Australia's legislator led approach has only involved AML/CTF regulation being implemented by AUSTRAC, but in 2021, ASIC issued guidance on cryptocurrency related activity, indicating it will regulate within its remit on investment products, and warned that products outside of this remit were not covered by regulation.[196] It is too early to assess the performance of ASIC, but it could be a sign that Australia is departing from a legislator led to a hybrid of legislator and regulator initiatives.

[194] Parliament of Australia, 'Digital Currency – Game Changer or bit player' (August 2015) <http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Digital_currency/~/media/Committees/economics_ctte/Digital_currency/report.pdf> accessed 21 October 2022 at para 6.29.
[195] P. Latimer and M. Duffy, 'Deconstructing Digital Currency and Its Risks: Why ASIC Must Rise to the Regulatory Challenge' (2019) 41(1) Federal Law Review 121 at 140.
[196] Australian Securities and Investments Commission, 'Regulating crypto-asset–based investment products within the financial services framework: Speech by Commissioner Cathie Armour at the AFR Cryptocurrency Summit' (6 April 2022) <https://asic.gov.au/about-asic/news-centre/speeches/regulating-crypto-asset-based-investment-products-within-the-financial-services-framework/> accessed 18 May 2022.

AUSTRAC has been praised by the FATF for its management of intelligence.[197] Irwin and Turner suggest that AUSTRAC should lead a more joined up approach for cryptocurrencies, as it is best placed to implement "*information sharing between multiple stakeholders from the law enforcement, financial intelligence units, cyber security organisations and fintech industry.*"[198] The reforms to the AML/CTF Act 2006 demonstrate proactivity from the Australian law makers, in commissioning reviews and being ahead of international best practice. However, the Australian reforms are limited, as the effect of the updated legislation is to simply apply existing AML/CTF regulation to CSPs, which indicates a lack of understanding of cryptocurrencies. Australia demonstrates the advantages of legislative reform; the resulting law is clear and addresses the gaps identified by legislators, however, gaps remain, notably a lack of regulation of solely cryptocurrency businesses, and it is unclear how effectively the regulator is implementing the reforms. Australia also demonstrates that a country can move between regulator and legislator led approaches, with ASIC beginning to assume responsibility for cryptocurrency regulation, which also supports the contention that a proactive regulator is required in both regulator led, and legislator led reform.

4.3 UK

The UK implemented the Fifth Anti-Money Laundering Directive[199] in December 2019 via an amendment to the Money Laundering, Terrorist Financing and Transfer of

[197] Financial Action Task Force, 'Australia – Mutual Evaluation Report – April 2015' <http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Report-Australia-2015.pdf> accessed 05 September 2022 at p8.
[198] A. S. M. Irwin and A. B. Tuner, 'Illicit Bitcoin transactions: challenges in getting to the who, what, when and where' (2018) 21(3) JMLC 297 at 310.
[199] Council Directive 2018/843/EU of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist

Funds (Information on the Payer) Regulations 2017 (MLR 2017).[200] The amendment meant that since 10th January 2020, the FCA is responsible for AML/CTF regulation of CSPs that exchange fiat currency for cryptocurrency,[201] exchange one cryptocurrency for another,[202] or provide custodian wallet services.[203]

The FCA gains its powers from the Financial Services and Markets Act 2000 (FSMA 2000),[204] and is a named regulator under the MLR 2017,[205] which specifically references the FCA's functions under FSMA 2000.[206] The legislation also bestows the FCA rule-making powers[207] which are found in the FCA Handbook.[208] The FCA's AML/CTF rules are contained in the Senior Management Arrangements, Systems and Controls (SYSC) section of the FCA Handbook, specifically SYSC 6.3. Srivastava notes that the risk-based approach in SYSC "*is intended to provide more flexibility to firms,*"[209] and Ryder observes that this flexibility "*allows them to identify the risks and determine how they can best allocate their resources in areas which are most*

financing and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance) [2018] OJ L 156/43.

[200] Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017/692 amended by The Money Laundering and Terrorist Financing (Amendment) Regulations 2019, SI 2019/1511.

[201] Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017/692, Regulation 14A(1)(a).

[202] Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017/692, Regulation 14A(1)(b).

[203] Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017/692, Regulation 14A(2).

[204] Financial Services and Markets Act 2000 Part 1A.

[205] Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017/692, Regulation 46(8).

[206] Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017/692, Regulation 46(9).

[207] Financial Services and Markets Act 2000 s.137A-FD.

[208] Financial Conduct Authority, 'FCA Handbook' <https://www.handbook.fca.org.uk/handbook> accessed 13 July 2021.

[209] A. Srivastava, 'UK Part II: UK Law and Practice' in A. Srivastava, M. Simpson, and N. Moffatt (eds) *International Guide to Money Laundering and Practice* (Haywards Heath, Bloomsbury, 2013) at 2.189.

vulnerable."[210] AML/CTF regulation in the UK, as in the US and Australia, can be divided into two broad elements: firstly, data collection in the form of record keeping and completing CDD requirements, and secondly, reporting requirements, which take the form of suspicious activity reports. The CDD requirements are set out in Part 3 of the MLR 2017. Regulation 27 established that CDD measures must be applied when a business relationship is first established,[211] when an occasional transaction exceeding €1,000 takes place,[212] where money laundering is suspected,[213] or where the "*veracity or adequacy*"[214] of the previously obtained information is doubted.[215] The focus of CDD is on identifying the customer, verifying their identity and obtaining information on the "*purpose and intended nature of the business relationship or occasional transaction*."[216] CSPs are likely to face additional challenges in completing CDD compared to traditional financial institutions as cryptocurrencies provide users with mechanisms to conceal their identity,[217] and as Irwin and Dawson note, "*cybercriminals are likely to be comfortable obtaining fraudulent documents*"[218] which can defeat CDD.

---

[210] N. Ryder *Money Laundering - An Endless Cycle?: A Comparative Analysis of the Anti-Money Laundering Policies in the United States of America, the United Kingdom, Australia, and Canada* (Routledge, London, 2012) at p.81.
[211] Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017/692, Regulation 27(1)(a).
[212] ibid Regulation 27(1)(b).
[213] ibid Regulation 27(1)(c).
[214] ibid Regulation 27(1)(d).
[215] ibid.
[216] ibid Regulation 28(2)(c).
[217] The anonymity attached to cryptocurrencies is addressed by the US Government Accountability Office in their 2014 report, which described such currencies as pseudonymous, as the although the users name is not known, other details are published on the blockchain; such as their Bitcoin address, the time of the transaction, and the amount: United States Government Accountability Office, 'Virtual Currencies: Emerging Regulatory, Enforcement, and Consumer Protection Challenges' <http://gao.gov/assets/670/663678.pdf> accessed 16 December 2015 at p.6.
[218] A. S. M. Irwin, and C. Dawson, 'Following the cyber money trail: Global challenges when investigating ransomware attacks and how regulation can help' (2019) 22(1) JMLC 110 at 125.

As with the US and Australian systems, the second element of the UK's preventative approach is reporting requirements, specifically through suspicious activity reports. A report is sent to the FIU when a transaction, or series of transactions, raises suspicions of money laundering or terrorist financing.[219] Reporting is conducted through regulated institutions, but the legal obligation is upon individuals within the regulated sector.[220] A person commits an offence if they know or suspect,[221] or have reasonable grounds to know or suspect,[222] that a person is engaged in money laundering based on information that came from their course of business,[223] and they fail to "*make the required disclosure as soon as is practicable after the information*"[224] comes to them. The reporting regime in the UK has been subject to criticism, as regulated entities are unsure when to report due to the ambiguity of the term 'suspicious'. In 2018, the Law Commission found the term suspicious "*ill-defined, unclear and inconsistently applied*"[225] by those submitting reports. The term has long been problematic in English law,[226] and the presence of criminal liability for failing to report creates further needs for a clear threshold for suspicion, which has not been provided. In *R v Da Silva*,[227] Longmore LJ held that "*it seems to us that the essential element of the word suspect and its affiliates, in this context, is that the defendant must think that there is a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice*."[228] *Da Silva* has been upheld, most notably by *K Ltd* v

[219] Proceeds of Crime Act 2002, ss.330-332.
[220] s.330 of the Proceeds of Crime Act 2002 sets out the criteria of the offence for a person in the regulated sector.
[221] ibid s.330(1)(a).
[222] ibid s.330(1)(b).
[223] ibid s.330(2).
[224] ibid s.330(3).
[225] Law Commission, *Anti-money laundering: the SARs regime* (Law Com No 384, 2018) para 5.13.
[226] See judgment of Lord Devlin in *Shaaban bin Hussein* v *Chong Fook Kam* [1970] 2 WLR 441.
[227] *R v Da Silva* [2007] 1 WLR 303.
[228] ibid at 308.

National Westminster Bank plc[229] and *Shah* v *HSBC Private Bank (UK) Ltd*[230] leaving the term 'suspicious' inadequately defined. With regards to CSPs, it could be of increased difficulty for them to establish what is, and is not, suspicious as they may have limited information with which to determine what is normal for their customer, particularly if their customer regularly transacts privately within cryptocurrency networks.

The amended AML/CTF legislation is only valuable if it is utilised by the FCA. The initial steps by the FCA appeared to be positive, with the announcement of a year-long registration period, but this time looks to have been wasted as only four entries appeared on the register in January 2021, rising to six by June 2021, 29 by the end of 2021, and only reaching 34 by April 2022.[231] Many more firms were on the original temporary registration list than have made it to the register,[232] it is unclear what has happened to these entries. A mitigating factor for the FCA's performance so far could be the COVID-19 pandemic, and that they are working through the original 104 applicants on the temporary registration list, but neither of these arguments hold up to scrutiny. Firstly, entries on the register were possible during 2020: four were added between 18th August and 1st September 2020, which illustrates that firms could be vetted within the pandemic restrictions in place over the summer and autumn of 2020. Secondly, the temporary register appears to have a very low bar for inclusion yet

[229] K Ltd v National Westminster Bank plc (Revenue and Customs Commissioners and another intervening) [2006] EWCA Civ 1039.
[230] *Shah* v *HSBC Private Bank (UK) Ltd* [2012] EWHC 1283.
[231] Financial Conduct Authority, 'Registered Cryptoasset firms' (last updated 23 June 2021) <https://register.fca.org.uk/s/search?predefined=CA> accessed 14 July 2021.
[232] Retrieved via 'Internet Archive: Way Back Machine: Financial Conduct Authority, 'Cryptoasset firms with Temporary Registration' (16th December 2020) https://web.archive.org/web/20201216074511/https://register.fca.org.uk/servlet/servlet.FileDownload?file=0154G0000062BtF> accessed 14 May 2022.

bestows included firms with "*temporary registration*"[233] to conduct regulated activities. The FCA state that the firms on the temporary list have not been assessed by them as "*fit and proper,*"[234] and the information appears to simply be an alphabetical list of firms which have applied to the FCA. The 104 temporary registered firms appear with their name, their address, and any other trading names used; however, this data is inputted in an inconsistent manner. There are entries which are in full capitals and other which lack capitals where required, the address formats vary, and there are two near identical entries; such errors and inconsistencies suggest the temporary register is simply pasted data from the firms' applications; this suggests the FCA is not committed to the regulation of cryptocurrencies. Questions might also be raised as to the integrity of the approved register too, as three of the four original entries are registered at the same address and two of those entries lack a registered telephone number. Based on the state of both the register and the temporary register, the dedication of the FCA to regulating CSPs can be questioned.

As with FinCEN and AUSTRAC, the FCA has enforcement powers,[235] and these are intended to support its objectives "*by making it clear there are real and meaningful consequences for firms and individuals who don't follow the rules.*"[236] Since its creation in 2013, until July 2021, the FCA has imposed over 200 fines,[237] amounting to over

[233] Financial Conduct Authority, 'Cryptoasset firms with Temporary Registration' (last updated 09 July 2021) <https://register.fca.org.uk/servlet/servlet.FileDownload?file=0154G0000062BtF> accessed 14 July 2021.
[234] Financial Conduct Authority, 'Cryptoasset firms with Temporary Registration' (last updated 09 July 2021) <https://register.fca.org.uk/servlet/servlet.FileDownload?file=0154G0000062BtF> accessed 14 July 2021.
[235] Financial Services and Markets Act 2000 s.206 gives the regulator the power to impose financial penalties of an amount it sees as appropriate.
[236] Financial Conduct Authority, 'Enforcement' (22 April 2016) <https://www.fca.org.uk/about/enforcement> accessed 14 July 2021.
[237] Based on published enforcement notices: Financial Conduct Authority, 'Enforcement' (22 April 2016) <https://www.fca.org.uk/about/enforcement> accessed 14 July 2021.

£3.8 billion, with an average fine of approximately £18 million. These figures are distorted by the extraordinary fines imposed on large banks for highly publicised failings in recent years, such as the LIBOR and FOREX scandals, and the record-breaking fines of £102 million for Standard Chartered[238] and £163 million for Deutsche Bank[239] for their AML failings. The FCA has issued fourteen fines over £100 million, if these are discounted then the average fine imposed by the FCA is £6.7 million. The FCA does not publish separate statistics for AML compliance enforcement actions, but in the 2018/19 Anti-Money Laundering Annual Report it was stated that since 2012, 18 AML enforcement cases had been concluded by the FCA and its predecessor the Financial Services Authority.[240] To date, the FCA has not imposed a fine on a CSP, its only enforcement action being with regards to Binance. In June 2016 the FCA issued a warning that Binance Markets Limited was "*not permitted to undertake any regulated activity in the UK.*"[241] Prior to the FCA's public warning on Binance, it did not appear on the list of firms with temporary registration in January 2021,[242] and unless the FCA's position changes, Binance will not appear on any future lists of registered firms.

[238] Financial Conduct Authority, 'FCA fines Standard Chartered Bank £102.2 million for poor AML controls' 09 April 2019) <https://www.fca.org.uk/news/press-releases/fca-fines-standard-chartered-bank-102-2-million-poor-aml-controls> accessed 14 July 2021.
[239] Financial Conduct Authority, 'FCA fines Deutsche Bank £163 million for serious anti-money laundering controls failings' (31 January 2017) <https://www.fca.org.uk/news/press-releases/fca-fines-deutsche-bank-163-million-anti-money-laundering-controls-failure> accessed 14 July 2021.
[240] Financial Conduct Authority, 'Anti-money laundering Annual report 2018/19' (09 July 2019) <https://www.fca.org.uk/publication/corporate/annual-report-2018-19-anti-money-laundering.pdf> accessed 18 September 2018 at p12.
[241] Financial Conduct Authority, 'Consumer warning on Binance Markets Limited and the Binance Group' (26 June 2021) <https://www.fca.org.uk/news/news-stories/consumer-warning-binance-markets-limited-and-binance-group> accessed 14 July 2021.
[242] Financial Conduct Authority, 'Cryptoasset firms with Temporary Registration' (version used: online 21 January 2021, last updated 09 July 2021) <https://register.fca.org.uk/servlet/servlet.FileDownload?file=0154G0000062BtF> accessed 21 January 2021.

The closing of the regulatory gap in the UK is comparable to that of Australia, the gap has been closed from a legislative perspective, but it is not clear if the regulatory gap has been addressed as the performance of the FCA appears limited. The FCA does appear to be engaging with its role to a degree, it provided a clear warning with regards to Binance, but there have been no enforcement actions taken against CSPs. The lack of enforcement actions is not surprising given the short amount of time since the FCA was given the responsibility for AML/CTF regulation of CSPs.

5. Recommendations

A regulator is in the strongest position to effect changes to regulation because it can act much more efficiently than a legislator, as demonstrated by FinCEN. While efficient legislators can enact reforms quickly in specific circumstances, the legislature's time is often taken up with other matters. Australia implemented its legislator led approach relatively quickly yet was still years behind the swift action of FinCEN. The swiftness of FinCEN is commendable, but the landscape in the US demonstrates a weakness of the regulator led approach in that it can be piecemeal. Regulators taking differing approaches leads to a confusing landscape for regulated entities to navigate. The reforms to the AML/CTF Act 2006 demonstrate proactivity from the Australian law makers, being compliant with international best practice before it is issued. The advantages of legislative reform can be seen through Australia; the resulting law is clear and regulated entities should know who to register with. However, the Australian reforms are limited in their scope as the updated legislation only applies existing AML/CTF regulation, and misses significant CSPs, suggesting a limited understanding of cryptocurrencies in the legislature. While there are weaknesses to both the legislator led and regulator led approaches, the strength of both approaches is the presence of

proactivity. The UK is demonstrative of what occurs if neither the regulator nor the legislature is proactive. The UK was perhaps fortunate that it was required to implement the Fifth Anti-Money Laundering Directive of the EU, as this required the legislator to act. Prior to this the UK failed to address the gaps in regulation due to other issues dominating legislators' time, and the regulator, the FCA, showed no signs of acting. The UK continues to exhibit a further weakness of the legislator led approach, which is the enduring reliance upon a committed regulator. The performance of the FCA since it was given responsibility for regulating cryptocurrency activity risks rendering the reforms ineffectual.

This paper has observed that the stimuli for action for both regulators, legislators, and international organisations and bodies, has been risks identified as constant risks, rather than growing risks. Acting on the constant risks, those that present due to the constant characteristics of cryptocurrencies is recommended because this demonstrates a commitment to addressing the regulatory issues, reducing the possibility of regulation being abandoned if the value or volume of cryptocurrency use reduces. The growing risks posed by cryptocurrencies should not be ignored, and it would be beneficial for more research to improve the understanding of these risks.

The UK, the US, and Australia have each addressed AML/CTF regulation of cryptocurrencies to a similar extent, but differences can be seen, and gaps remain in each jurisdiction. The regulation in the UK and the US appears to cover all cryptocurrency exchanges, compared to Australia where providers exchanging cryptocurrency for fiat currency are regulated, but those purely exchanging

cryptocurrencies for other cryptocurrencies are not. The UK regulation goes further than that of the US and Australia as it specifically refers to custodian wallet providers. However, all three jurisdictions appear to be missing high value transactions which take place within cryptocurrency networks, and in Australia those transactions will include transactions where cryptocurrencies are exchanged for other cryptocurrencies. Each of the jurisdictions appears to be compliant with the FATF guidance for applying the risk-based approach to cryptocurrencies. All three jurisdictions legislation incorporate "*funds or value-based terms*"[243] as including cryptocurrencies, meaning that relevant financial crimes are still satisfied where cryptocurrencies are used in lieu of traditional finance. The FATF also identify the services that should be regulated for AML/CTF purposes, setting out five key services: exchanging cryptocurrencies for fiat currencies, exchanging cryptocurrencies for other cryptocurrencies, transferring assets on behalf of others, providing custodian wallet services, and offering cryptocurrencies for sale.[244] Australia and the US appear to cover four of the five services identified by the FATF, as neither jurisdiction clearly addresses wallets. Contrastingly, while the UK can be criticised for the length of time it took to address cryptocurrencies, the UK legislation covers all five services and specifically identifies custodian wallet providers. Only the US appears to be proactive in enforcement, principally through FinCEN. The coverage of the regulation, and the lack of a tailored approach to AML/CTF regulation of cryptocurrencies is problematic, a more consistent approach is required, but more importantly, the compatibility of cryptocurrencies to existing measures needs greater consideration.

---

[243] Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' (21 June 2019) <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 25 June 2021 para 65 at p20.

[244] ibid at para 33 at p13-14.

As the constant risks demonstrate; cryptocurrencies provide novel challenges, which require novel solutions. Adopting a proportionate and appropriate response to cryptocurrencies, and effectively utilising resources, should also include adapting the regulation to fit cryptocurrencies, rather than applying existing measures which are incompatible with the new technology. FIUs should take responsibility for blockchain analysis and surveillance of cryptocurrency networks, as financial intelligence will be produced, and this should be used to support regulation and investigations. Closing the remaining regulatory gaps and implementing effective use of blockchain data will require engaged and proactive regulators.

While the regulator led approach is recommended, if this has not already occurred, such a recommendation is unlikely to be followed, as a reluctant regulator is unlikely to expediently transform into a proactive one. A legislator will have to lead in jurisdictions where the regulator fails to, but it is difficult to envisage strong implementation from a regulator which is forced to take on such responsibility. It is possible for a hybrid approach to be adopted, where the legislators and regulators each take initiatives; the beginnings of this are being seen in Australia with the proactivity of ASIC.

6. Conclusions

This paper has explored the merits of legislator led and regulator led approaches to regulatory reform and contends that the determining factor for a jurisdiction in choosing an approach rests with the regulator. It is also argued that the proactivity of the

regulator determines the efficacy of the regulation, whether it leads the development of AML/CTF regulation or not.

While FinCEN in the US demonstrates the impact of a proactive regulator, and Australia's legislation shows the effect of a relatively proactive legislature; the UK's approach to cryptocurrencies is demonstrative of what occurs if neither the regulator nor the legislature is proactive. Weaknesses of the legislator led approach include the length of time it takes to address the gap in regulation and the risk that the issue slips down the politically driven list of legislator priorities. A further weakness of the legislator led approach demonstrated by the UK is the reliance upon the regulator to implement the amended legislation, to which the FCA appears to be lacklustre.

Motivations for reform are divided into constant and growing risks. Constant risks are ever-present, based on the AML/CTF risks posed by the permanent characteristics of cryptocurrencies. Growing risks relate to both new threats emerging through the development of cryptocurrency technology and services, and constant risks being exacerbated by the increasing numbers of cryptocurrency participants and service providers. The paper identified a third motivation, that of pressure from international organisations which have reacted to the constant and growing AML/CTF risks of cryptocurrencies before the regulator or legislature of a national jurisdiction. For the US and Australia, the constant risks of criminals utilising cryptocurrencies were the principal stimulation for applying AML/CTF regulation. The driving force for UK reform was the requirement to comply with the Fifth Anti-Money Laundering Directive.

While the AML/CTF threats posed by cryptocurrencies are beginning to be addressed, the remaining gaps are no doubt being exploited for criminal purposes. Consistency is required with regards to which market participants are regulated and where traditional regulation is not possible, active monitoring should be adopted to utilise the open-source intelligence available.

Bibliography

Primary Sources

EU Treaties

Consolidated Version of The Treaty on The Functioning of The European Union [2016] OJ C 202/47.

EU Legislation

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

Council Directive 2005/60/EC of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, [2005] OJ L309/15.

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

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

Council Directive 2018/843/EU of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance) [2018] OJ L 156/43.

Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering [1991] OJ L166/77.

United Kingdom Acts of Parliament

Financial Services and Markets Act 2000.

Proceeds of Crime Act 2002.

United Kingdom Statutory Instruments

Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 S.I. 2017/692.

Money Laundering and Terrorist Financing (Amendment) Regulations 2019, SI 2019/1511.

The Money Laundering Regulations 2007 S.I. 2003/3075.

Australia National Legislation

Anti-Money Laundering and Counter-Terrorism Financing Act 2006.

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

United States of America National Legislation

Bank Secrecy Act, Pub. L. 91–508.

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

Money Laundering Control Act Pub. L. 99-570.

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

US Code Title 18 - Crimes and Criminal Procedure.

US Code Title 31 - Money and Finance.

US Code Title 7 – Agriculture.

United Kingdom Case Law

K Ltd v *National Westminster Bank plc (Revenue and Customs Commissioners and another intervening*) [2006] EWCA Civ 1039.

R v *Da Silva* [2007] 1 WLR 303.

Shaaban bin Hussein v *Chong Fook Kam* [1970] 2 WLR 441.

Shah v *HSBC Private Bank (UK) Ltd* [2012] EWHC 1283.

Australia Case Law

Chief Executive Officer of Australian Transaction Reports and Analysis Centre v TAB Limited (No 3) [2017] FCA 1296.

Chief Executive Officer of the Australian Transaction Reports and Analysis Centre v Commonwealth Bank of Australia Limited [2018] FCA 930.

Chief Executive Officer of the Australian Transaction Reports and Analysis Centre v Westpac Banking Corporation [2020] FCA 1538.

Secondary Sources

Books

Chaum D, 'Blind Signatures for Untraceable Payments' in: D. Chaum, R.L. Rivest, and A.T. Sherman, eds. Advances in Cryptology: Proceedings of Crypto 82 (Springer 1982).

Lilley P, Dirty Dealing: The Untold Truth about Global Money Laundering (London, Kogan Page, 2006).

Ryder N, Money Laundering - An Endless Cycle?: A Comparative Analysis of the Anti-Money Laundering Policies in the United States of America, the United Kingdom, Australia and Canada (Routledge, London, 2012).

Srivastava A, 'UK Part II: UK Law and Practice' in A. Srivastava, M. Simpson, and N. Moffatt (eds) International Guide to Money Laundering and Practice (Haywards Heath, Bloomsbury, 2013).

Unger B, & Linde D vd, Research Handbook on Money Laundering (Edward Elgar, Cheltenham, 2013).

Journal Articles

Campbell-Verduyn M, 'Bitcoin, crypto-coins, and global anti-money laundering governance' (2018) 69 Crime Law Soc Change 283.

Alexander K, 'The International Anti-Money-Laundering Regime: The Role of the Financial Action Task Force' (2001) 4(3) JMLC 231.

Chaum D, 'Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms. (1981) 24 (2) Communications of the ACM' 84.

Hall J, ‘Restraint orders: R. v Teresko (Sergejs) Kingston Crown Court: HH Judge Lodder QC: unreported 11 October 2017’ (2018) 1 CLR 81.

Houben R and Snyers A, ‘Study Requested by the TAX3 Committee: Cryptocurrencies and Blockchain – Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion’ (Publications Office of the EU, 6 September 2018) <https://op.europa.eu/en/publication-detail/-/publication/631f847c-b4aa-11e8-99ee-01aa75ed71a1> accessed 24 June 2021.

Irwin ASM and Tuner AB, ‘Illicit Bitcoin transactions: challenges in getting to the who, what, when and where’ (2018) 21(3) JMLC 297.

Irwin ASM, and Dawson C, ‘Following the cyber money trail: Global challenges when investigating ransomware attacks and how regulation can help’ (2019) 22(1) JMLC 110.

Irwin ASM, Kim-Kwang RC, and Liu L, ‘An analysis of money laundering and terrorism financing typologies’ (2012) 15(1) JMLC 85.

Irwin ASM, Slay J, Kim-Kwang RC, Lui L, ‘Money laundering and terrorism financing in virtual environments: a feasibility study’ (2014) 17(1) JMLC 50.

Keatinge T, Carlisle D, and Keen F, ‘Virtual currencies and terrorist financing: assessing the risks and evaluating responses’ (study commissioned by the Directorate General for Internal Policies, Policy Department for Citizens’ Rights and Constitutional Affairs, May 2018).

Kethineni S and Cao Y, ‘The Rise in Popularity of Cryptocurrency and Associated Criminal Activity’ (2020) 30(3) International Criminal Justice Review 325 at 337.

Kethineni S and Cao Y, ‘The Rise in Popularity of Cryptocurrency and Associated Criminal Activity’ (2020) 30(3) International Criminal Justice Review 325.

Latimer P and Duffy M, ‘Deconstructing Digital Currency and Its Risks: Why ASIC Must Rise to the Regulatory Challenge’ (2019) 41(1) Federal Law Review 121.

Mantalara G, ‘An overview of the ML/TF risks and regulatory responses in the crypto-asset landscape’ (2021) 36(11) Journal of International Banking Law and Regulation 487.

Mitsilegas V and Gilmore B, ‘The EU legislative framework against money laundering and terrorist finance: a critical analysis in light of evolving global standards’ (2007) 56(1) International and Comparative Law Quarterly 119.

Money Laundering Regulations 2017.

Möser M, Soska K, Heilman E, Lee K, Heffan H, Srivastava S, Hogan K, Hennessey J, Miller A, Narayanan A, and Christin N, 'An Empirical Analysis of Traceability in the Monero Blockchain' (2018) 3 Proceedings on Privacy Enhancing Technologies 143.

Ryder N, 'Cryptoassets, social media platforms and defence against terrorism financing suspicious activity reports: a step into the regulatory unknown' (2020) 8 Journal of Business Law 668.

Ryder N, 'The Financial Services Authority and Money Laundering: A Game of Cat and Mouse' (2008) 67(3) Cambridge LJ 635.

Southall E, and Taylor M, 'Bitcoins' (2013) 19 (6) Computer and Telecommunications Law Review 177.

Stokes R, 'Virtual Money Laundering: The Case of Bitcoin and the Linden Dollar' (2012) 21(3) Information and Communications Technology Law 221 at 231.

Reports

Australian Government: Attorney-General's Department, 'Report on the Statutory Review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and Associated Rules and Regulations' (April 2016) <https://www.austrac.gov.au/sites/default/files/2019-07/report-on-the-statutory-review-of-the-anti-money-laundering.pdf> accessed 18 May 2022 at p53.

Australian Securities and Investments Commission, 'Regulating crypto-asset–based investment products within the financial services framework: Speech by Commissioner Cathie Armour at the AFR Cryptocurrency Summit' (6 April 2022) <https://asic.gov.au/about-asic/news-centre/speeches/regulating-crypto-asset-based-investment-products-within-the-financial-services-framework/> accessed 18 May 2022.

House of Commons Treasury Committee, Crypto-assets Twenty-Second Report of Session 2017–19 (2018).

Law Commission, Anti-money laundering: the SARs regime (Law Com No 384, 2018).

Treasury Committee, Crypto-assets (HC 2017-19, 910).

Newspapers

Kollewe J, 'Bitcoin price surges to record high of more than $68,000' (The Guardian, 9 November 2017) <https://www.theguardian.com/technology/2021/nov/09/bitcoin-price-record-high-cryptocurrencies-ethereum> accessed 14 February 2022.

P Durkin, ‘70pc jump in suspicious money laundering transactions: AUSTRAC’ Financial Review (Melbourne, 18 October 2018) <https://www.afr.com/business/banking-and-finance/70pc-jump-in-suspicious-money-laundering-transactions-austrac-20181018-h16szs> accessed 24 July 2022.

Online Sources

AUSTRAC, ‘A guide to preparing and implementing an AML/CTF program for your digital currency exchange business’ <https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/guide-preparing-and-implementing-amlctf-program-your-digital-currency-exchange-business> accessed 26 July 2022.

AUSTRAC, ‘About AUSTRAC’ <http://www.austrac.gov.au/about-us/austrac> accessed 14 July 2021.

AUSTRAC, ‘AML/CTF programs overview’ (Last updated: 14 Aug 2020) <https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/guide-preparing-and-implementing-amlctf-program-your-digital-currency-exchange-business> accessed 12 July 2021.

AUSTRAC, ‘Digital currency exchange provider registration actions’ (Last updated: 17 May 2021) <https://www.austrac.gov.au/digital-currency-exchange-provider-registration-actions> accessed 12 July 2021.

AUSTRAC, ‘Freedom of Information request on 5 December 2018’ (25 January 2019) <https://www.austrac.gov.au/sites/default/files/2019-06/AUSTRAC%20Cryptocurrency%20inquiries.pdf> accessed 12 July 2021.

AUSTRAC, ‘Introduction to Money Laundering’ <https://michaelsmithnews.typepad.com/files/money-laundering.pdf> accessed 5 September 2022.

BBC News, ‘Business: The Company File - Beenz means business’ (16 March 1999) <http://news.bbc.co.uk/1/hi/business/297133.stm> accessed 18 November 2021.

BBC News, ‘Criminals hide 'billions' in crypto-cash – Europol’ (12 February 2018) <https://www.bbc.co.uk/news/technology-43025787> accessed 08 October 2022.

BBC News, ‘Criminals hide 'billions' in crypto-cash – Europol’ (12 February 2018) <https://www.bbc.co.uk/news/technology-43025787> accessed 08 October 2021.

BBC News, ‘MtGox bitcoin exchange files for bankruptcy’ (28 February 2014) <https://www.bbc.co.uk/news/technology-25233230> accessed 07 October 2022.

BBC News, ‘NHS cyber-attack: GPs and hospitals hit by ransomware’ (13 May 2017) <https://www.bbc.co.uk/news/health-39899646> accessed 02 September 2021.

BBC News, ‘Top Bitcoin exchange MtGox goes offline’ <https://www.bbc.co.uk/news/technology-26333661> accessed 02 September 2022.

Blockchain.com, ‘Block 0’ <https://www.blockchain.com/btc/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f> accessed 28 June 2021.

Board of Governors of the Federal Reserve System, ‘Financial Stability Report – May 2021’ (Federal Reserve, 06 May 2021) <https://www.federalreserve.gov/publications/files/financial-stability-report-20210506.pdf> accessed 25 June 2021.

Caddy J, Delaney L, Fisher C, Noone C, ‘Consumer Payment Behaviour in Australia’ (Reserve Bank of Australia, 19 March 2020) <https://www.rba.gov.au/publications/bulletin/2020/mar/consumer-payment-behaviour-in-australia.html#r2> accessed 27 July 2021.

CFTC, ‘CFTC Charges 20 Entities for Making False Registration Claims’ (Washington, DC, United States, 01 September 2020) <https://www.cftc.gov/PressRoom/PressReleases/8229-20> accessed 26 August 2021.

CFTC, ‘CFTC Charges BitMEX Owners with Illegally Operating a Cryptocurrency Derivatives Trading Platform and Anti-Money Laundering Violations’ (Washington, DC, United States, 01 October 2020) <https://www.cftc.gov/PressRoom/PressReleases/8270-20> accessed 26 August 2021.

CFTC, ‘CFTC Charges Two Individuals with Multi-Million Dollar Digital Asset Pump-and-Dump Scheme’ (Washington, DC, United States, 05 March 2021) <https://www.cftc.gov/PressRoom/PressReleases/8366-21> accessed 26 August 2021.

CFTC, ‘Enforcement Actions’ (Washington, DC, United States, Regularly Updated) <https://www.cftc.gov/LawRegulation/EnforcementActions/index.htm?year=all> accessed 26 August 2021.

CFTC, ‘In the Matter of: Coinflip, Inc., d/b/a Derivabit, and Francisco Riordan’ (CFTC Docket No. 15-29, 17 September 2015) <https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoinfliprorder09172015.pdf> accessed 26 August 2021.

Chainalysis Inc. Before the Senate Banking Committee’ (17 March 2022) <https://www.banking.senate.gov/imo/media/doc/Levin%20Testimony%203-17-223.pdf> accessed 17 May 2022.

Chainalysis, ‘The 2022 Crypto Crime Report’ (16 February 2022) <https://go.chainalysis.com/2022-Crypto-Crime-Report.html> accessed 14 April 2022.

CNET, E-currency site Flooz goes offline’ (2 January 2002) <https://www.cnet.com/news/e-currency-site-flooz-goes-offline/> accessed 18 November 2002.

Dai W, ‘B-Money’ (November 1998) <http://www.weidai.com/bmoney.txt> accessed 18 November 2021.

Department of Justice, U.S. Attorney’s Office Southern District of New York, ‘Ross Ulbricht, A/K/A “Dread Pirate Roberts,” Sentenced in Manhattan Federal Court to Life in Prison’ (Manhattan, New York, 29 May 2015) <https://www.justice.gov/usao-sdny/pr/ross-ulbricht-aka-dread-pirate-roberts-sentenced-manhattan-federal-court-life-prison> accessed 05 September 2021.

ECB, ‘Virtual currency schemes – a further analysis’ <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> accessed 11 February 2022.

FBI New York, ‘Ross Ulbricht, the Creator and Owner of the Silk Road Website, Found Guilty in Manhattan Federal Court on All Counts’ (5 February 2015) <https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/ross-ulbricht-the-creator-and-owner-of-the-silk-road-website-found-guilty-in-manhattan-federal-court-on-all-counts> accessed 26 July 2021.

FCA, ‘2019 Fines’ (11 October 2019) <https://www.fca.org.uk/news/news-stories/2019-fines> accessed 23 October 2022.

Financial Action Task Force ‘Who We Are’ <http://www.fatf-gafi.org/about/> accessed 02 February 2022.

Financial Action Task Force, ‘Anti-money laundering and counter-terrorist financing measures: United States Mutual Evaluation Report’ (December 2016) <https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-States-2016.pdf> accessed 14 April 2022.

Financial Action Task Force, ‘Australia – Mutual Evaluation Report – April 2015’ <http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Report-Australia-2015.pdf> accessed 05 September 2022.

Financial Action Task Force, ‘Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers’ (21 June 2019) <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 07 July 2021.

Financial Action Task Force, ‘Publication Search: Virtual Currencies’ <https://www.fatf-gafi.org/publications/?hf=10&b=0&q=Virtual%2520Currencies&s=desc(fatf_releasedate)> accessed 25 July 2021.

Financial Action Task Force, ‘The FATF Recommendations’ <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> accessed 05 July 2022.

Financial Action Task Force, ‘Third Mutual Evaluation Report on Anti-Money Laundering and Combatting the Financing of Terrorism: United States of America’ <http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20US%20full.pdf> accessed 28 October 2022.

Financial Action Task Force, ‘Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers’ (October 2021) <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf> accessed 12 January 2022.

Financial Action Task Force, ‘Virtual Currencies – Key Definitions and Potential AML/CFT Risks’ (27 June 2014) <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 27 July 2021.

Financial Conduct Authority, ‘Anti-Money Laundering Annual Report 2012/13’ <http://www.fca.org.uk/static/documents/anti-money-laundering-report.pdf> accessed 15 June 2022.

Financial Conduct Authority, ‘Anti-money laundering Annual report 2018/19’ (09 July 2019) <https://www.fca.org.uk/publication/corporate/annual-report-2018-19-anti-money-laundering.pdf> accessed 18 September 2018.

Financial Conduct Authority, ‘Consumer warning on Binance Markets Limited and the Binance Group’ (26 June 2021) <https://www.fca.org.uk/news/news-stories/consumer-warning-binance-markets-limited-and-binance-group> accessed 14 July 2021.

Financial Conduct Authority, ‘Cryptoasset firms with Temporary Registration’ (last updated 09 July 2021) <https://register.fca.org.uk/servlet/servlet.FileDownload?file=0154G0000062BtF> accessed 14 July 2021.

Financial Conduct Authority, ‘Cryptoassets’ (07 March 2019, Updated 18 June 2021) <https://www.fca.org.uk/consumers/cryptoassets> Accessed 22 July 2021.

Financial Conduct Authority, ‘Enforcement’ (22 April 2016) <https://www.fca.org.uk/about/enforcement> accessed 14 July 2021.

Financial Conduct Authority, ‘FCA fines Deutsche Bank £163 million for serious anti-money laundering controls failings’ (31 January 2017) <https://www.fca.org.uk/news/press-releases/fca-fines-deutsche-bank-163-million-anti-money-laundering-controls-failure> accessed 14 July 2021.

Financial Conduct Authority, ‘FCA fines Standard Chartered Bank £102.2 million for poor AML controls’ 09 April 2019) <https://www.fca.org.uk/news/press-releases/fca-fines-standard-chartered-bank-102-2-million-poor-aml-controls> accessed 14 July 2021.

Financial Conduct Authority, ‘FCA Handbook’ <https://www.handbook.fca.org.uk/handbook> accessed 13 July 2021.

Financial Conduct Authority, ‘Infographic: Cryptoasset consumer research 2020’ (December 2019) <https://www.fca.org.uk/publication/documents/crypto-assets-infographic.pdf> accessed 22 July 2021.

Financial Conduct Authority, ‘Registered Cryptoasset firms’ (last updated 23 June 2021) <https://register.fca.org.uk/s/search?predefined=CA> accessed 14 July 2021.

Financial Conduct Authority, “Financial Conduct Authority’s Written Submission on Digital Currencies” (April 2018), http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/treasury-committee/digital-currencies/written/81677.pdf> accessed 18 September 2022.

FinCEN, ‘Enforcement Actions’ (18 April 2019) <https://www.fincen.gov/news-room/enforcement-actions> accessed 23 October 2022.

FinCEN, ‘FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger’ (Washington, 5 May 2015) <https://www.fincen.gov/sites/default/files/enforcement_action/2016-08-02/20150505.pdf> accessed 02 September 2022.

FinCEN, ‘FinCEN’s Strategic Plan’ <https://www.fincen.gov/about/fincens-strategic-plan> accessed 02 September 2022.

FinCEN, ‘Guidance - FIN-2013-G001 - Issued: March 18, 2013 - Subject: Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies’ (18 March 2013) <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf> accessed 06 July 2021.

FinCEN, ‘In the Matter of BTC-E a/k/a Canton Business Corporation and Alexander Vinnik’ (Vienna, United States, 07 June) <2017https://www.fincen.gov/sites/default/files/enforcement_action/2017-07-27/Assessment%20for%20BTCeVinnik%20FINAL2.pdf> accessed 02 September 2022.

FinCEN, ‘In the Matter of Eric Powers’ (Vienna, United States, 18 April 2019) <https://www.fincen.gov/sites/default/files/enforcement_action/2019-04-18/Assessment%20Eric%20Powers%20Final%20for%20Posting%2004.18.19_1.pdf> accessed 02 September 2022.

FinCEN, ‘In the Matter of Larry Dean Harmon d/b/a Helix’ (Akron, Ohio, United States, 19 November 2020) <https://www.fincen.gov/sites/default/files/enforcement_action/2020-10-19/HarmonHelix%20Assessment%20and%20SoF_508_101920.pdf> accessed 08 July 2021.

FinCEN, ‘Law Enforcement Overview’ <https://www.fincen.gov/resources/law-enforcement-overview> accessed 30 August 2022.

FinCEN, ‘Reporting Suspicious Activity – A Quick Reference Guide for Money Services Businesses’ <https://www.fincen.gov/sites/default/files/guidance/msbsar_quickrefguide.pdf> accessed 14 July 2021.

FinCEN, ‘What We Do’ <http://fin-cenus.com/what-we-do.html> accessed 03 October 2022.

GOV.UK, ‘Digital currencies: call for information’ (March 2015) <https://www.gov.uk/government/consultations/digital-currencies-call-for-information/digital-currencies-call-for-information> accessed 11 July 2021.

GOV.UK, ‘Digital currencies: response to the call for information’ <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf> accessed 11 July 2021.

Government Accountability Office ‘What GAO Does’ <https://www.gao.gov/about/what-gao-does> accessed 19 April 2022.

International Monetary Fund, ‘Global Financial Stability Report—COVID-19, Crypto, and Climate: Navigating Challenging Transitions’ (Washington, DC, 12 October 2021) <https://www.imf.org/en/Publications/GFSR/Issues/2021/10/12/global-financial-stability-report-october-2021> accessed 25 November 2021.

International Monetary Fund, ‘Money Laundering: The Importance of International Countermeasures’ <http://www.imf.org/external/np/speeches/1998/021098.htm> accessed 15 June 2022.

Internet Archive: Way Back Machine: Financial Conduct Authority, ‘Cryptoasset firms with Temporary Registration’ (16th December 2020) https://web.archive.org/web/20201216074511/https://register.fca.org.uk/servlet/servlet.FileDownload?file=0154G0000062BtF> accessed 14 May 2022.

Levin J, ‘Written Testimony of Jonathan Levin Co-Founder and Chief Strategy Officer Chainalysis Inc. Before the Senate Banking Committee’ (17 March 2022) <https://www.banking.senate.gov/imo/media/doc/Levin%20Testimony%203-17-223.pdf> accessed 17 May 2022.

Legislation.Gov, ‘Your search for UK Public General Acts has returned more than 200 results’ <https://www.legislation.gov.uk/ukpga> accessed 20 September 2022.

Library of Congress, ‘Regulation of Bitcoin in Selected Jurisdictions’ (January 2014) <https://tile.loc.gov/storage-services/service/ll/llglrd/2014427360/2014427360.pdf> accessed 09 September 2021.

Mark W. Vigoroso, ‘Beenz.Com Closes Internet Currency Business’ (Commerce Times, 17 April 2001) <http://www.ecommercetimes.com/story/12892.html> accessed 18 November 2021.

Nakamoto, S. ‘Bitcoin: A Peer-to-Peer Electronic Cash System’ (31 October 2008) <https://nakamotoinstitute.org/static/docs/bitcoin.pdf> accessed 18 November 2021.

Nelson R M, ‘Statement of Rebecca M. Nelson before U.S. Senate Committee on Banking, Housing, and Urban Affairs’ (30 July 2019) <https://www.banking.senate.gov/imo/media/doc/Nelson%20Testimony%207-30-19.pdf> accessed 17 May 2022.

Office for National Statistics, ‘Average Sterling exchange rate: US Dollar XUMAUSS’ (11 April 2022) <https://www.ons.gov.uk/economy/nationalaccounts/balanceofpayments/timeseries/auss/mret> accessed 14 April 2022.

Organization for Economic Co-operation and Development, ‘Gross Domestic Product’ <http://stats.oecd.org/glossary/detail.asp?ID=1163> accessed 15 June 2022.

Parliament of Australia, ‘Digital Currency – Game Changer or bit player’ (August 2015) <http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Digital_currency/~/media/Committees/economics_ctte/Digital_currency/report.pdf> accessed 20 April 2022.

U.S. Securities and Exchange Commission, ‘Office Hours with Gary Gensler: The SEC & Cryptocurrencies’ (Washington, DC, United States, 16 August 2021) <https://www.youtube.com/watch?v=-kKGkbrwCT0&ab_channel=U.S.SecuritiesandExchangeCommission> accessed 25 August 2021.

United Nations Office on Drugs and Crime, ‘Illicit Money: How Much is Out There?’ <http://www.unodc.org/unodc/en/frontpage/2011/October/illicit-money_-how-much-is-out-there.html> accessed 15 June 2022.

United States Government Accountability Office, ‘Virtual Currencies: Emerging Regulatory, Enforcement, and Consumer Protection Challenges’ (May 2014) <http://gao.gov/assets/670/663678.pdf> accessed 1 February 2022.

United States Treasury, ‘National Money Laundering Risk Assessment’ <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf> accessed 5 September 2022.

XE, ‘XBT to USD Chart’ (updated daily) <https://www.xe.com/currencycharts/?from=XBT&to=USD&view=10Y> accessed 23 July 2021.