Counter-Terrorism Financing in the Age of Digital Currencies: A Critical and Comparative Analysis of the legislative approaches in Bahrain and the United Kingdom

PhD Thesis

Student Name: Salman Isa Salman Aljawder

Student Number: 23012513

Submission Date: 18 December 2024

Abstract

This research examines the legislative responses and frameworks in Bahrain and the United Kingdom (UK) to counter-terrorism financing (CTF) involving cryptocurrencies. The study evaluates the effectiveness of international and national regulations in addressing cryptocurrency-related terrorism financing (TF), assesses the implementation of the 'Financial War on Terrorism' in both jurisdictions and analyses the strengths and weaknesses of their current CTF legal frameworks. It also proposes enhancements based on FATF Recommendations to address modern challenges in preventing the misuse of cryptocurrencies for TF and related financial crimes, such as money laundering (ML).

Key findings highlight the UK's cautious approach to regulating cryptocurrency exchanges through a framework established in 2018, which emphasises transparency and uniform requirements. In contrast, Bahrain employs a proactive approach with a regulatory sandbox under the Central Bank of Bahrain (CBB) tailored to the specific needs of exchanges. Both countries use a risk-based approach, adapting their regulations based on assessed risks.

The analysis of the 2018 Mutual Evaluation Reports (MERs) for both countries reveals strengths and weaknesses in their frameworks. The UK demonstrates a robust understanding of TF risks, effective public/private partnerships, and proactive enforcement. Bahrain, while developing a comprehensive system and proactive measures, faces challenges such as fewer prosecutions and a less integrated institutional framework.

The study also identifies ten common challenges faced by Financial Intelligence Units (FIUs) in both countries, including issues related to the quality of suspicious activity reports (SARs), resource limitations, and gaps in oversight of cryptocurrency exchanges. Both jurisdictions must address these challenges and adapt their regulatory frameworks to keep pace with technological advancements and evolving risks.

Ultimately, the research concludes that while both Bahrain and the UK have made significant progress, they can benefit from mutual insights. Bahrain could learn from the UK’s extensive regulatory experience, while the UK could enhance its collaborative capacities by emulating Bahrain’s integrated approach. Both countries should tailor their strategies to balance between novel and traditional financial avenues, ensuring robust defences against evolving terrorist

financing tactics. The study provides a comprehensive set of policy recommendations aimed at strengthening the CTF frameworks in both jurisdictions.

Contents

Acknowledgement

First and foremost, I extend my deepest gratitude to my beloved country, the Kingdom of Bahrain, under the wise leadership of His Majesty King Hamad bin Isa Al Khalifa and His Royal Highness Crown Prince and Prime Minister Shaikh Salman bin Hamad Al Khalifa. Their unwavering commitment to education and national development has been a cornerstone of my success.

I am profoundly grateful to my sponsor, the Ministry of Interior, under the leadership of His Excellency General Shaikh Rashid bin Abdulla Al Khalifa, for their unwavering support and dedication to fostering excellence. Their belief in the power of education has been pivotal in enabling me to pursue this journey. I also extend my heartfelt appreciation to the Bahrain Financial Intelligence National Center, especially Her Highness Shaikha May Bent Mohammed Al Khalifa, for her encouragement and invaluable support throughout this experience.

This academic journey would not have been possible without the guidance, mentorship, and friendship of Professor Nicholas Ryder. Not only is he one of the most outstanding experts in his field, but he is also an incredibly down-to-earth and approachable person. Nicholas has been a steadfast source of support, especially during the shared challenges of the pandemic. Together, we navigated through the uncertainty and difficulties, including transitioning between universities and adapting to unforeseen circumstances. His encouragement, belief in me, and his ability to bring calm during turbulent times truly made the difference. Beyond being my supervisor, he has been a trusted friend who walked this journey with me, shoulder to shoulder, making even the hardest days manageable. It was a privilege to have him by my side throughout this extraordinary experience, and I will forever cherish our bond.

I would also like to extend my sincere appreciation to the Cardiff University committee, whose support and insights have been invaluable throughout this process.

To my family, who stood by my side with unwavering love and encouragement, especially during the challenging times of the pandemic when I was back home, I owe my deepest thanks. Their support gave me the strength to persevere and complete this journey.

This has truly been an extraordinary journey of knowledge and self-growth, and I am deeply grateful to everyone who has supported me along the way.

Chapter 1: Introduction

1.1. Research Background

Prior to the al Qaeda-financed terrorist attacks in the United States of America (US) on September 11 2001 ('9/11'), terrorism financing ('TF') was largely overlooked by international financial crime policies, with the focus being instead on money laundering ('ML)[1]. This is illustrated by the multiplicity of anti-money laundering ('AML') legislative measures introduced by the United Nations ('UN'), the European Union ('EU') and the soft law Recommendations of the Financial Action Task Force ('FATF').[2] It was not until after 9/11 that terrorism financing garnered international attention,[3] prompting actions such as the UN Security Council Resolution 1373, which mandates countries to report suspicious terrorist transactions, to broaden AML measures to cover alternative payment systems and to strengthen customer identification processes.[4]

Terrorism financing has evolved from depending on direct state sponsorship and charitable donations to utilising more sophisticated and elusive methods, reflecting the adaptability of terrorist organisations to global financial surveillance.[5] Initially, TF was reliant on support from sympathetic governments and public contributions; however, such early methods were relatively straightforward for authorities to monitor and disrupt – especially with the cooperation of banking institutions and international partners – and as international scrutiny intensified, terrorists diversified their sources by engaging in increasingly more criminal activities to maintain funding streams.[6] The post-Cold War era saw a shift towards exploiting charitable organisations and informal transfer systems like *hawala*, allowing for discreet cross-border fund transfers.[7] The attacks on 9/11 highlighted the use of such methods, with the hijackers receiving funding through

[1] N Ryder, *Financial Crime in the 21st Century: Law and Policy (*Edward Elgar Publishing, 2011) 12-13.
[2] N Ryder, *Money laundering an endless cycle? A comparative analysis of the anti-money laundering policies in the USA, UK, Australia and Canada* (Routledge, 2012).
[3] R Alexander, 'Money laundering and terrorist financing: time for a combined offence' (2009) Company Lawyer, 30(7), 200–204, 200.
[4] O Elagab, 'Control of terrorist funds and the banking system' (2006) Journal of International Banking Law and Regulation, 21(1), 38–44, 43.
[5] J K Giraldo and Harold A Trinkunas (eds.) *Terrorism Financing and State Responses: A Comparative Perspective* (Stanford University Press, 2007).
[6] N Ridley, *Terrorist Financing: The Failure of Counter Measures* (Edward Elgar, 2012).
[7] EA Akartuna, SH Johnson and AE Thornton, 'The money laundering and terrorist financing risks of new and disruptive technologies: a futures-oriented scoping review' (2022) 36 Secur J 615.

wire transfers and cash deliveries facilitated by al-Qaeda's global financial network.[8] Although these methods presented challenges for detection, international regulatory efforts, including tighter regulations on charitable organisations and informal transfer systems, began to limit the use of these avenues for suspicious transactions.[9]

At the same time, it is important to acknowledge that the UK's HM Treasury highlighted the low costs of conducting effective terrorist attacks,[10] with the 2017 National Risk Assessment noting that terrorism financing in the UK often involves modest amounts for overseas transfers, travel or funding the planning of an attack.[11] This reflects a shift towards self-financed and low-budget terrorism,[12] illustrated by incidents such as the 1993 Bishopsgate bombing, which caused damage (£1bn) on a minimal budget (£3,000).[13] The emergence of digital currencies added complexity to tracking and controlling terrorism financing because unlike traditional financial systems regulated by central banks, cryptocurrencies offer a decentralised alternative that offers anonymity, provides ease of transfer and significantly reduces detection risk, complicating the efforts to monitor and disrupt terrorist financing networks.[14] The affordability and anonymity provided by digital currencies, coupled with the limited legislation of certain jurisdictions, have become attractive for terrorist funding, presenting new challenges in the fight against terrorism.[15]

Cryptocurrencies (e.g. Bitcoin, Ethereum, Monero) introduce features that significantly enhance the anonymity of the transactions, complicating the efforts to track and prevent terrorism financing.[16] Unlike traditional financial systems governed by strict regulations such as Know Your

[8] N Ryder, *The Financial War on Terrorism: A Review of Counter-Terrorist Financing Strategies Since 2001* (Routledge 2015)
[9] C Dion-Schwarz, D Manheim and P B. Johnston, *Terrorist Use of Cryptocurrencies: Technical and Organisational Barriers and Future Threats* (RAND Corporation, 2019).
[10] HM Treasury, *Combating the financing of terrorism. A report on UK action* (HM Treasury: London, 2002) 11.
[11] HM Treasury, *National risk assessment of money laundering and terrorist financing* (HM Treasury: London, 2017) 6.
[12] A Acharya, Targeting Terrorist Financing – International Cooperation and New Regimes (Routledge Cavendish: London, 2009) at 11. For a more detailed discussion see US Department of State County Reports on Terrorism 2017 (US Department of State: 2018) and D Byman S Kreps, 'Agents of Destruction? Applying Principal-agent Analysis of State Sponsored Terrorism' (2010) International Studies Perspectives 11(1) 1-18.
[13] See Ryder above, n 8 at 49.
[14] C Friesendorf and A Blutener, *Decentralized Financed (DeFi): How Decentralized Applications (dApps) Disrupt Banking* (Springer, 2023).
[15] A Brill and L Keene, 'Cryptocurrencies: The Next Generation of Terrorist Financing?" 6 Defence against Terrorism Review. 1, 7- 30.
[16] D K C Lee and R H Deng *Handbook of Blockchain, Digital Finance, and Inclusion, vol. I: Cryptocurrency, FinTech, InsurTech, and Regulation* (Academic Press, 2018).

Customer ('KYC') and AML, cryptocurrencies operate on networks without a central authority, using blockchain technology to distribute transaction ledgers across a multitude of global computers.[17] This structure, combined with the pseudonymous nature of the transactions, along with sophisticated encryptions and privacy-focused designs, makes it difficult to link transactions to real identities.[18] More specifically, technologies such as ring signatures, zk-SNARKs,[19] and peer-to-peer networks, along with mixing services or tumblers that shuffle cryptocurrencies among multiple users, further obscure transaction details and eliminate the need for intermediaries, significantly complicating monitoring efforts.[20] These attributes starkly contrast with the transparent, regulated environment of traditional banking, posing significant hurdles for law enforcement and regulatory bodies in identifying and preventing illicit financial flows, including those related to terrorism.[21]

Thus, it is no surprise that terrorism financiers have increasingly turned to digital currencies to support their activities, leveraging their ability to facilitate transactions with a high degree of anonymity and utility in illicit trades.[22] Indeed, the use of cryptocurrencies for criminal enterprises has grown exponentially during the past years – notably, from $14bn in 2021[23] to $20bn in 2022[24] – and unsurprisingly, the appeal for such financiers is multifaceted. Firstly, their widespread use in criminal and illegal drug trades – activities often intertwined with terrorist operations, as proven by the success of platforms such as the Silk Road – highlights their effectiveness in bypassing traditional financial monitoring systems.[25] Additionally, the anonymity provided by digital

[17] S Merz, *Blockchain Technology - The Next Big Thing: Introduction To A Technology That May Change the World* (Books on Demand, 2021).
[18] E S Prasad, *The Future of Money: How the Digital Revolution Is Transforming Currencies and Finance* (Harvard University Press, 2021).
[19] Acronym for 'Zero-Knowledge Succinct Non-Interactive Argument of Knowledge' – protocol used in encryption.
[20] S Patnaik and others, *Blockchain Technology and Innovations in Business Processes* (Springer, 2021).
[21] Friesendorf and Blutener, n 14.
[22] Ryder, n 8.
[23] T Wilson, Crypto crime hit record $14 billion in 2021, research shows (*Reuters* 2022) < https://www.reuters.com/markets/us/crypto-crime-hit-record-14-billion-2021-research-shows-2022-01-06/> accessed 19 January 2024
[24] E Howcroft, Crypto crime hits record $20 bln in 2022, report says (*Reuters* 2023) <https://www.reuters.com/business/finance/crypto-crime-hits-record-20-bln-2022-report-says-2023-01-12/> accessed 10 January 2024
[25] An online marketplace on the darknet where criminals trades in illegal goods and services, and relied on digital currencies as their main medium of exchange. For a more detailed discussion of Silk Road Maddox, A., Barratt, M., Allen, M. and Lenton, S. 'Constructive activism in the dark web: cryptomarkets and illicit drugs in the digital deminonde' (2016) 19 Information, Communication & Society, 111-126.

currencies allows financiers to remain hidden during the acquisition and transfer of funds, offering a layer of protection for those wishing to support terrorism without direct involvement.[26] This anonymity also extends to the recipients of the funds, further complicating efforts by authorities to trace and disrupt financial networks supporting terrorism.[27] Thus, as cryptocurrencies are decentralised and anonymous, evading traditional banking regulations and oversight, their use enhances the challenges associated with tracing transactions back to their sources or intended terrorist activities.[28] Therefore, Bahrain and the United Kingdom ('UK') need to develop and implement tailored regulatory frameworks that can encompass the digital nature of these transactions while ensuring robust monitoring mechanisms are in place. This may include leveraging technology to enhance the transparency of cryptocurrency transactions, instituting stronger collaboration between international financial bodies and fostering innovation in detecting and mitigating the risks associated with digital terrorism financing.[29]

However, the response to TF in the UK and Bahrain is being influenced by their distinct regulatory environments, financial systems and geopolitical contexts. On the one hand, Bahrain's approach to cryptocurrencies in TF is influenced by its position as a financial hub in the Middle East and its strategic importance in the Gulf region.[30] More specifically, the country operates within a smaller but rapidly growing financial market with an increasing interest in digital currencies and FinTech innovation.[31] To this end, Bahrain has been proactive in developing a regulatory framework for digital financial services, including cryptocurrencies, to attract investment while ensuring financial stability and security.[32] The Central Bank of Bahrain ((CBB) has issued regulations on cryptoassets, aiming to prevent their misuse of TF and ML while supporting technological innovation.[33] The main challenge for Bahrain lies in balancing these objectives within the context

[26] I Salami, 'Terrorism Financing with Virtual Currencies: Can Regulatory Technology Solutions Combat This?' (2017) Studies in Conflict & Terrorism, 1–22.
[27] Jeanne K Girlado and Harold A Trinkunas (eds) *Terrorism Financing and State Responses: A Comparative Perspective* (SUP, 2007).
[28] Friesendorf and Blutener, n 14.
[29] G Kaur, P Lekhi and S Popli, *Exploring Central Bank Digital Currencies: Concepts, Frameworks, Models, and Challenges* (IGI Global, 2024).
[30] N Alam, and S N Ali, *Fintech, Digital Currency and the Future of Islamic Finance: Strategic, Regulatory and Adoption Issues in the Gulf Cooperation Council* (Switzerland, Springer, 2020).
[31] C Haddadm and L. Hornuf, 'The Emergence of Global FinTech Market: Economic and Technological Determinants', (2019) 58, Small Bus Eco, 81.
[32] M E Lokanan, and N Nasimi, 'The effectiveness of Anti-Money Laundering policies and procedures within the Banking Sector in Bahrain', (2019), 23, Journal of Money Laundering Control', 4.
[33] CBB Rule Book, *Financial Crime Module, Vol 1: Conventional Banks* (CBB 2021).

of Islamic finance principles, which play a significant role in the country's banking sector.[34] Additionally, Bahrain's regional proximity to conflict zones increases the importance of effective AML and counter-terrorism financing (CTF) measures, and the country's efforts to counter TF through cryptocurrencies also involve regional cooperation with Gulf Cooperation Council (GCC) members and adherence to international standards set by bodies such as the FATF.[35]

On the other hand, as a leading global financial centre with a sophisticated banking sector, the UK faces significant risks from the use of cryptocurrencies in TF due to the high volume of international transactions processed within its jurisdiction.[36] The country's advanced digital economy also means there is widespread familiarity with and access to cryptocurrencies, increasing and potentially facilitating their use for illicit purposes.[37] The UK's regulatory framework for cryptocurrencies is evolving, with efforts to extend existing AML/CTF regulations to include digital currency exchanges and wallet providers.[38] However, the anonymity and cross-border nature of cryptocurrency transactions pose challenges for enforcement.[39] Additionally, the UK's commitment to financial innovation and technology means it must balance regulatory measures with not stifling the FinTech sector. Given its role in international finance and its exposure to global terrorism risks, the UK is particularly focused on collaboration with international bodies such as the FATF to address the challenges cryptocurrencies pose to TF.[40]

For both the UK and Bahrain, the specific influence of cryptocurrencies on TF strategies involves navigating the complex interplay between maintaining financial innovation and ensuring robust measures against the misuse of digital currencies for terrorist purposes. Overall, each country's approach reflects its unique financial landscape, regulatory priorities and geopolitical considerations, all of which are further explored in the chapters dedicated to each jurisdiction.

---

[34] CBB Rule Book, *Financial Crime Module, Vol 2: Islamic Banks* (CBB 2021).
[35] Alam and Ali, n 30
[36] I H Chiu, '*Regulating Crypto-Finance: A Policy Blueprint', ECGI Working Paper Series in Law,* (2021) <https://ecgi.global/sites/default/files/working_papers/documents/chiufinal.pdf> accessed 15 January 2024
[37] S Kebbell, 'The Law Commission: anti-money laundering and counter-terrorism financing - reform of the suspicious activity reporting regimes' (2018), 11 Criminal Law Review.
[38] OPBAS, '*Office for Professional Body Anti-Money Laundering Supervision (OPBAS): Sourcebook for Professional body anti-money laundering supervision'* (2018), <https://www.fca.org.uk/publication/opbas/opbas-sourcebook.pdf> accessed 15 January 2024
[39] M Hopkins, and N Shelton, 'Identifying Money Laundering Risk in the United Kingdom: Observations from National Risk Assessments and a Proposed Alternative Methodology', (2019), 25, Eur J Crim Policy Res, 70.
[40] T Parkman, '*Mastering Anti-Money Laundering and Countering-Terrorist Financing: A Compliance Guide for Practitioners'* (Pearson, 2020).

1.2 Brief History of Terrorism Financing Definitions

A number of key terms, such as money laundering, terrorism financing, crytoassets and the financial war on terrorism, must be defined for this project. Money laundering can be defined as the process in which illegally gotten assets are intermixed with legitimate money so that the former can appear to have been procured through legitimate means.[41] According to Mugarura, successful money laundering involves three stages: first, the ill-gotten money must be moved from its source; second, the money chain must be concealed to prevent law enforcement from discovering the true origin of money; and third, the money must be injected into legal business activities so that they can appear that they have been derived from such.[42] The main investigatory challenge of prosecuting money laundering offences is that money laundering is a dynamic process in which criminals are finding new ways of exploiting the vulnerabilities of the financial systems and have increasingly used new technologies to hide the proceeds of crime.[43]

Unlike money laundering, the term terrorist financing is a bit more ambiguous to define, mostly because there is disagreement on what acts can be defined as terrorist activities. Indeed, there are more than 200 definitions of the term terrorism in the academic literature.[44] According to the International Convention for the Suppression of the Financing of Terrorism, an individual can be implicated in this crime if "directly or indirectly, unlawfully and willfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out terrorism".[45] Terrorism financing is comprised of two separate offences: the financing of active terrorist organisations, while the second one is raising money to support such groups, an offence that is mostly carried out by non-governmental organisations.[46] The problem with terrorist financing is that conventional mechanisms used to prosecute and deter money laundering might be impotent in detecting terrorist financing mostly because the money

[41] Muhammad Saleem Korejo, Ramalinggam Rajamanickam and Muhamad Helmi Md. Said, The concept of money laundering: a quest for legal definition (2021) 24 Journal of Money Laundering Control
[42] Norman Mugarura, *The Global AML Regulatory Landscape in Less Developed Countries*, (Routledge 2016).
[43] Stefan Cassella, 'Illicit finance and money laundering trends in Eurasia.' (2019) 22 Journal of Money Laundering Control, 388-399.
[44] Bruce Hoffman, "The confluence of international and domestic trends in terrorism.' 1997 9 Terrorism and Political Violence 1-15.
[45] International Convention for the Suppression of the Financing of Terrorism (adopted on 9 December 1999, entered into force on 10 April 2002), 2178 UNTS
[46] Zaiton Hamin, Rohana Othman, Normah Omar and Hayyum Suleikha 'Conceptualizing terrorist financing in the age of uncertainty.' (2016) 19 Journal of Money Laundering Control 397-406.

used for carrying out a terrorist attack might not have an illicit origin, as terrorist financing can involve clean money. [47] Reverse money laundering[48], according to Ryder, occurs before an illegal act has been committed, and the contemporary approaches to terrorist financing have evolved to fight not only ML but also reverse money laundering in recognition that terrorist attacks such as 9/11 were enabled because of reverse money laundering.[49]

With technology coming to the forefront of contemporary financial operations, cryptoassets have offered criminals new opportunities for both ML and TF. The term cryptoassets refers to "digital units that are created and transferred between the users through the use of cryptography".[50] Other researchers emphasise that a cryptoasset is, in fact, an alternative digital currency developed based on cryptographic and blockchain technology that has a variety of financial and monetary functions. [51] According to the European Securities and Market Authority (ESMA), cryptoassets are assets built through cryptographic methods and distributive ledger technologies.[52] Such definitions, however, are not entirely precise as cryptoassets can also include a wide variety of economic assets, including monetary, equity, debt and hybrid assets.[53] In that respect, Coelho argues that cryptoassets have six features; first, they are a new asset type; second, there is digital support behind those asset types; third they are built on distributive ledger technology and cryptographic technology, fourth operate autonomously of the central banking system, fifth they have a conventional course and last but not least, they have high functional versatility.[54]

Before the 9/11 attacks, the definition of TF in the UK was based on the provisions under two key legislative frameworks. First, the Northern Ireland (Emergency Provisions) Act 1973 gave the Crown the power of seizure over anything perceived as being, has been or is destined for use in

[47] Stefan Cassella, 'Money laundering, terrorism, regulation, laws and legislation. (2004) 7 Journal of Money Laundering Control 92-94.
[48] Reverse money laundering can be defined as the practice of using money obtained through legitimate activities for funding illegitimate operations such as terrorist activities. It should be differentiated from the money laundering which uses moneys from illegal activities.
[49] See Ryder above, n 1.
[50] Gabriel Söderberg, Are Bitcoin and other crypto-assets money. (2018) 5 Economic Commentaries14.
[51] Prior Stabile and AM, Hinkes. *Digital assets and blockchain technology: US law and regulation.* (Edward Elgar Publishing; 2020).
[52] ESMA, *Advice Initial Coin Offerings and Crypto-Assets* (ESMA, 2019)
[53] D Kochergin, Crypto-assets: Economic nature, classification and regulation of turnover." (2022) 17 International organisations research journal 75-113.
[54] Pereira Coelho The Construction of the Legal Definition of Crypto-Asset under MiCAR, Including the Legal Subcategories: A Very Brief Summary SRNN Electronic Journals https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4884719

committing a scheduled offence, including terror-related activities. Second, the Prevention of Terrorism (Temporary Provisions) Act 1974 authorised courts to seize the assets that were under the control of persons found guilty of being members of a group associated with terror in Northern Ireland. [55]

The confiscation regime was, however, found ineffective under an appraisal of the terrorism strategy in the UK in 1998, which culminated in the proposition for modernisation and streamlining of the various fragmented legislation to optimise the effectiveness and appropriateness to all forms of terrorism. [56] The driving factor behind the appraisal was the recognition of the fact that whereas most of the legislation targeted terror threats from Irish territories, there were emergent international threats. In response, the UK has undertaken a dynamic approach, with elements of proactivity coupled with a response to emergent and extant risks of TF, through the following legal frameworks.

Before 9/11, legal measures targeting the proceeds of criminal activities focused specifically on the entities associated with manufacturing and distributing narcotics. Under the UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances,[57] member countries commit the following:

- The criminalisation of the laundering of the proceeds from drugs and other controlled substances.
- Implementation of frameworks and instruments that enable the jurisdictions to determine the offences under ML
- Allow the forceful confiscation of the proceeds from the dealings in the banned substances while ensuring that the legalisation of the substances is clearly articulated.
- Introduce mechanisms to extradite offenders, as well as create mutual legal agreements for cross-border enforcement of the provisions of the legal frameworks.

[55] Laura Donahue '*The cost of counterterrorism –power, politics and liberty* (Cambridge University Press: 2008) 130. Northern Ireland (Emergency Provisions) Act 1973, s 11, who attributes the prompt adoption of the act to the Birmingham pub attacks of 1974,

[56] Cabinet Office Recovering the Proceeds of Crime—A Performance and Innovation Unit Report (2000) 118-120 identifies a number of legislations, including Criminal Justice Act 1988, Drug Trafficking Act 1994 and Proceeds of Crime Act 1995 as being part of the legislation that lay the foundation for ultimate definition of TF in the UK

[57] Article 3 to 7 of the UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1998), hence forth referred to as Vienna Convention (1998)

The Financial War on Terror was driven by UN Security Council Resolution 1373[58] (Resolution 1373), which obliged member states and signatories to adopt the measures effectively combatting terrorism financing in their jurisdiction, obliging them to update their legislation against TF. Subsequent resolutions included 2133 (2014)[59], 2170 (2014)[60], 2161 (2014)[61] and 2199 (2015).[62] The subsequent chapters will examine the approaches to terrorism financing that have been implemented in Bahrain and the UK to supplement the findings of this chapter.

1.3 TF Definitions in Bahrain

The definition of TF in Bahrain is deduced from a multiplicity of administrative rules, regulatory measures and laws (decrees). The definitions are aimed at presenting a Middle Eastern perspective of TF, considering that the nature of terrorism and criminal activities that are related to terror financing is unique.

1.3.1 Decree-Law 4/2001 (DL 4 2001)

The decree mandates that ML-related activities are outlawed, specifically activities associated with criminal entities, corruption, or to disguise the source of money.[63] Although these activities were outlawed in response to the expansion and complexity of the financial sector, they formed a foundation for CTF legislation in the amendments of the decree, which occurred in 2006,[64] 2013[65] and 2017[66]. The implementation of these decrees necessitated the establishment of the Bahrain Monetary Agency (BMA).[67] The establishment of the BMA facilitated the introduction

[58] That the resolution was introduced under Chapter 7 of the UN Charter and included measures to Aversion and suppression of TF in any form, Criminalisation of TF, Freezing the resources held by terrorists and entities that offer financial support and Stopping institutions and people from offering financial support to those interested in committing acts of terror.
[59] UN Security Council, *Security Council resolution 2133 (2014) [on threats to international peace and security caused by terrorist acts]*, 27 January 2014, S/RES/2133 (2014),.
[60] UN Security Council, *Security Council resolution 2170 (2014) [on threats to international peace and security caused by terrorist acts by Al-Qaida]*, 15 August 2014, S/RES/2170 (2014).
[61] UN General Assembly, *Security Council resolution 2161 (2014) [on threats to international peace and security caused by terrorist acts by Al-Qaida]*, 17 June 2014, S/RES/2161 (2014).
[62] UN Security Council, *Security Council resolution 2199 (2015) [on threats to international peace and security caused by terrorist acts by Al-Qaida]*, 12 February 2015, S/RES/2199 (2015).
[63] F. Alzubairi, 'Kuwait and Bahrain's Anti-Terrorism Laws in Comparative and International Perspective. (2011).
[64] Law No. (54) of 2006 (Bahrain)
[65] Law No. (25) of 2013 (Bahrain)
[66] Legislative Decree No. (36) of 2017 (Bahrain)
[67] BMA, which is the premier regulator for the financial sector in the country.

of several monitoring and control mechanisms, such as the reporting of suspicious transactions.[68] The identification and reporting of suspicious transactions facilitate the definition of TF since information about transactions that are viewed as not falling into pre-determined criteria can indicate actions that relate to the facilitation of terrorism.

Article 2 outlines the crimes under ML and TF in the country by prohibiting ML from the funds acquired through a multiplicity of sources that are widely known to be used for TF.[69] In particular, Article 2.3 outlines the activities that are deemed part of ML/TF, including destroying, misappropriating, and concealing documents that are key in facilitating the detection of crimes or perpetrators for TF or knowing the intention of perpetrators of ML for TF purposes, and assisting them to conceal the activity. Additional measures are outlined in Article 2.7, whereby actions are taken.

Article 4.1 of the decree also established the Anti-Money Laundering Policy Committee (AMLPC) based on the recognition that ML activities can be re-tasked for TF. Although the policy committee functions domestically, Article 8 outlines the measures that AML/CTF institutions in Bahrain can take to cooperate with foreign countries in recognition of the fact that ML/TF occurs across the border. Article 9 establishes the basis for information sharing, which ultimately culminates in the establishment of financial intelligence units.[70]

Bahrain also recognises the vulnerabilities of ML in TF, with an additional regulatory framework aimed at increasing vigilance on certain individuals based on their actions and who they are dealing with.[71] These entities have to adhere to a multiplicity of decrees, including the following.

- Decree 7 (2001) mandates corporations to establish baseline AML controls

[68] Suspicious transaction reporting is an integral part of TF, with a threshold in Bahrain being 6,000 dinars, the equivalent of US$15,000.
[69] Legislative Decree No. (4) Of 2001 with Respect to Prohibiting and Combating Money Laundering and Terrorism Financing (Bahrain)
[70] The AMLPC joined the Egmont Group of FIUs in 2003.
[71] KPMG, '*Anti-Money Laundering (AML) Advisory Services*. (KPMG 2019), identifies key entities and operations that can be classified as Designated Non-Financial Businesses and Professionals (DNFBPs), who must comply with the mandatory AML regulations, including persons involved in car sales, real estate, auctions and galleries, accountants and auditors, precious metals and jewelers and persons involved in high-value items whose price fluctuates.

- Decision 23 (2002) provides additional guidelines on the implementation of those controls and expands the sources of funds for money where ML can be suspected
- Decision 36 (2017) expands the scope of activities that are subjected to penalties for failure to comply with AML guidelines
- Order 173 (2017) provides additional guidelines for certain industries based on ML risks
- Decision 57 (2018) amends the definition of terrorism to accommodate emergent links between ML and TF
- Decree 108 (2018) amends the suspicious transaction reporting regime to enhance due diligence requirements

1.3.2 Law No. 58 of 2006

The Law on Protection of the Community against Terrorists Acts (2006) in Bahrain is designed to protect the country against terrorist attacks. In recognition of the role of TF in terror attacks, the law is fundamentally an extension of the Penal Code 2006, which outlines the punishments for monetary and other forms of support for terrorism. Article 2 outlines the multiplicity of crimes for which penalties set in the Act are applicable, with specific assertion that if such crimes are committed for terrorist purposes. The specific mention of the link between crime and TF is included in Article 2 (9), which imposes punitive measures for individuals who conceal criminal activities for items acquired in service of a crime associated with terrorism. Similarly, Article 30 states that:

> "The Public Prosecution shall order proceeding with access or obtaining any data or information related to the accounts, deposits, trusts or safe deposit boxes with banks or other financial institutions or the transactions related thereto if this is deemed necessary for revealing the truth in any of the crimes provided for in this Law. For taking such actions, prior permission shall be obtained from the High Court judge." [72]

An amendment in 2019 recognises the role of electronic money and the fact that there is an emergent threat from criminal gangs operating from foreign countries.[73] During the review, Bahrain also identified particular entities as designated terrorist groups, imposing restrictions on

[72] Law No. 58 Of 2006 With Respect to Protection of the Community Against Terrorist Acts (2006) (Bahrain)
[73] Bureau of Counterterrorism, 'Country Reports on Terrorism 2019' (2020), 114.

their activities as part of the AML/CTF strategies.[74] Bahrain has shown increasing interest in defining the range of vulnerabilities and suspicious activities that mark TF.[75] Under Legislative Decree No. 21 of 1989,[76] charities are mandated to acquire licences before operating in the country and to report all transactions for authentication to determine whether they are for humanitarian objectives. However, the primary challenge with AML/CTF measures occurs when institutions in the country have to comply with the guidelines on handling cash from countries with a poorer compliance regime compared to Bahrain or where the transactions involve parties from countries that have a history of ML/TF.

1.3.3 Resolution No. 83 of 2020

In response to changing TF strategies, Bahrain has introduced measures to determine the 'Ultimate Beneficial Owner'(UBO).[77] The identification of the UBOs facilitates compliance with Financial Action Task Force (FATF) requirements, prevents tax avoidance, and wards off global security concerns. Under the UBO rules,[78] the definition under the FATF,[79] the identification of beneficial owners is integral to TF since it fosters accountability for all the resources within institutions. The measures to identify 'beneficial owners', which were introduced by FATF in 2012, were necessary due to the increased complexity in the structures and types of corporations that were utilised in various jurisdictions.[80] In 2014, additional measures to guide countries on

[74] Ibid, 115, these entities include Hizballah of Bahrain, ISIS in Iraq and Syria, the 14 February Youth Coalition, al-Ashtar Brigades, People's Resistance Brigades, al-Mukhtar Brigades and Bahrain Freedom Movement, implying that under Article 2 of Law No. 58, any transactions with these entities have to be scrutinised carefully.

[75] H A Fakhro, 'Anti-Money Laundering/Terrorist Financing and Self-Defence for Real Estate Agents and Professionals' (n.d) < https://www.rera.gov.bh/EN/downloads/FAQ/AML_GUIDE_MoIC.pdf > accessed 11 January 2024 which primary focuses on general indicators, vulnerabilities in reporting, the nature of identity documents, cash transactions, use of economic resources, cross-border transactions.

[76] Amended in 2004, to enhance protections against terror financing, with requirements for reporting all transactions above 20,000 Dinars (US$41,000) to the BMA.

[77] KPMG, *Ultimate Beneficial Owner: KPMG in Bahrain's Tax Webinar*, (KPMG 2021), which defines the ultimate beneficial owner (UBO) as the individual or entity that benefits from or is positively impacted from a company though they are not formally named as the owner of a business.

[78] M Hill, 'Bahrain Ultimate Beneficial Owner ("UBO") Rules Take Effect (2020)', who indicates that the rule, which is adapted from the 'Beneficial Owner' guidelines under FATF, was introduced under Resolution No. 83 of 2020 by the Ministry of Industry, Commerce and Tourism

[79] Under FATF guidelines, a beneficial owner is a natural person who controls or owns a customer, and or the natural person on whose behalf a transaction is being conducted.

[80] FATF *Best Practices on Beneficial Ownership for Legal Persons,* (FATF 2019), whereby there is an increased need for countries to enhance their standards on identification of the beneficial ownership of instruments such as bearer shares and nominees, as well as ownership of trusts and the individuals who actually control or own the information.

determining the beneficial ownership were provided under the FATF guidance,[81] where the use of novel corporate vehicles, including foundations, trusts, partnerships and other forms of creating legal persons, were discussed in full, vis-à-vis the risks of ML/TF in various jurisdictions. The transparency achieved through the identification of UBOs within Bahrain is a step ahead of what the FATF proposes in the most current guidelines under Recommendations 24 mandates by focusing on the natural person who ultimately benefits from the resources in question. Similarly, UBOs are defined based on the amount of influence they have within corporations and other forms of legal persons since such individuals have the power to make decisions on the utilisation of resources, including for use in TF.[82]

The identification of UBOs enables Bahrain to achieve its CTF strategies through increased accountability for the movement of funds and resources within the country's corporate infrastructure. The approach is in furtherance of due diligence within corporations and is integral to the financial intelligence goals under CTF.[83] However, AML/CTF strategies based on beneficial owners are limited in six ways, including:[84]

- Insufficient risk assessment mechanisms for misuse of ML/TF
- Insufficiency in provisions for ML/TF for bearer shares and nominated shareholders
- Ineffective and disproportionate measures to sanction companies that fail to adhere to the provisions
- Inadequacies in the mechanisms to monitor the quality of assistance for cross-border transactions
- Lack of mechanisms for ensuring that qualified authorities have access to the information on beneficial owners
- Lack of measures to ensure that the information on beneficial owners

Bahrain has adopted a proactive and responsive approach in its AML/CTF strategies. The definition of TF includes actions, intent, or failure to act, all of which culminate in the facilitation

[81] *FATF Guidance, Transparency and Beneficial Ownership* (FATF 2014) and *Anti-Money Laundering and Counter Terrorist Financing Measures: Kingdom of Bahrain Mutual Evaluation Report* (MENA FATF 2018).
[82] FATF Recommendations 24 requires countries to ensure that competent authorities have timely access to adequate, accurate and up-to-date beneficial ownership information.
[83] See Hill above, n 79.
[84] FATF, n(80)

of TF. The focus of the country is directed towards institutions that have the potential to engage in TF, as well as the actions of individuals. A review of CTF regimes on which these definitions are based was found to lack legitimacy despite being effective in achieving their objectives.[85] There are claims of extensive restrictiveness of these provisions on the civil liberties of the citizens due to the implementation of the laws.[86]

1.4 TF Definitions in the UK

1.4.1 Terrorism Acts 2000 and 2006

The appraisal by the Home Office[87] led to conclusions that the scope of the existing TF provisions was too narrow to cover all potential threats from terrorism. The emergence of the global terror threats from organised groups led to innovative approaches, such as terror groups raising funds from individuals who were not directly involved in the terror attacks.

The Terrorism Act of 2000 criminalised TF activities and is essentially the foundation of all CTF strategies discussed herein. Under the Act, terrorism finance is defined with recognition of the involvement of domestic and international groups, retained the principles of proscription, creation of a commission for appeals organisations affected by proscription, new powers for forfeitures and seizures and the provision of guidelines through which financial institutions can detect accounts that are associated with investigations on terrorism.[88]

The Act established criminal offences which culminate in the forfeiture or seizure of assets held by terrorists, with the provisions extending to the obligations under ML reporting that existed before 9/11. The offences included:

- Raising funds for use in terrorism-related activities[89]
- Possession and use of resources for terror-related activities[90]

[85] A Almutawa, *The Legitimacy of Counterterrorism Financing Measures in Bahrain with Reference to the United Kingdom* (PHD University of Leeds 2019)
[86] A Almutawa, 'Terrorism measures in Bahrain, proportionality and the interplay between security, civil liberties and political stability'. (2018) 3 The International Journal of Human Rights, 3, who indicates that the lack of proportionality in the goals of securing the country and achieving civil liberties.
[87] Home Office *Legislation against Terrorism –A consultation paper* (1998).
[88] I Awan, 'Glorifying and encouraging terrorism: preserving the golden thread of civil liberties in Britain' (2012) 4, Journal of Aggression, Conflict and Peace Research, 3, 144.
[89] Section 15, of the Terrorism Act, 2000.
[90] Section 16, of the Terrorism Act, 2000.

- Making arrangements for funding terror[91]
- Insuring payments destined for terrorist demands[92]
- Warning targets of investigations and surveillance for TF about the activities of the law enforcement agencies.[93]
- ML activities[94]
- Failure to disclose activities relating to terror financing
- Failure to disclose activities that support the commission of terrorist activities.

Under these Acts, CTF measures involved confiscation and forfeiture, whereby the orders involved the payment of the number of benefits or value arising from the criminal act. In this accord, TF was considered a criminal act that led to some form of quantifiable benefit that was deduced from the benefit that accrued to those who engaged in terrorist activities.[95] Before assets were confiscated or forfeited, the courts considered whether the individual had engaged in a lifestyle that was considered criminal, which resulted in profits. The minimum amount is set at £5,000, with the activity only perceived as a criminal lifestyle if it is ongoing for more than six months.[96]

1.4.2. Anti-Terrorism, Crime and Security Act 2001 (ATCSA 2001)

The ATCSA 2001 was introduced to broaden the definition of TF compared to the preceding laws, based on the sanctions imposed on terror financing activities. Furthermore, by adopting the UN sanctions regime, the ATCSA 2001 broadened the definition of TF to include suspicious activities. To effect this, freezing orders, which were utilised under the UN sanctions regime, were introduced. The freezing orders were utilised for terror financing acts whereby:

- The actions that are detrimental to all or part of the economy of the UK have been or have the likelihood of being committed by one or more persons.[97]

[91] Section 17, of the Terrorism Act, 2000.
[92] Section 17A of the Terrorism Act, 2000.
[93] Section 21D (1) of the Terrorism Act, 2000.
[94] Section 18, of the Terrorism Act, 2000.
[95] Section 21 of the Act also makes provisions for three exemptions, where the TF activities occurred with express consent from law enforcement agencies, such as with protected informants for surveillance purposes, arrangements without prior consent but within reasonable time and where the events occur for reasonable excuses.
[96] However, these provisions must be understood from the Provisions of the Section 75 of the Proceeds of Crime Act, 2002.
[97] Section 4 (2)(a) of the Anti-terrorism, Crime and Security Act 2001.

- The acts that threaten the property or life of one or more citizens or residents of the UK have been or have the likelihood of being committed by one or more persons.[98]

The introduction of freeze orders enabled the UK to define TF to include the actions of individuals within and outside the UK, as well as other governments and nation-states outside the UK. Through the orders, the UK can prevent the availability of those finds until the HM Treasury can determine otherwise, for a period exceeding two years if necessary.

The measures that the Act envisioned for those suspected of such activities include:

- Forfeiture of cash held by terrorists
- The imposition of freezing orders for assets
- Seizure of financial assets held by terrorists anywhere in the UK
- Examination of bank accounts that have the potential to be used to support terror
- The imposition of orders to require the disclosure of information
- The imposition of orders for restraining the disclosure of information

The measures, which represented the first CTF strategy under the FATF, outlined the objectives of the UK as being the deterrence, detection and disruption of the financial infrastructures of terrorists. The implementation of the strategy involved the Home Office, whose primary objective was to limit and prevent the ability of terror groups to move financial assets into and out of the UK.[99] The ATCSA 2001 also introduced suspicious activity reporting (SAR), which has played an integral role in the utilisation of financial intelligence in CTF.[100] SAR expanded the definition of TF to include transactions that were viewed as being out of the norm, even when they bore characteristics of legal transactions within the jurisdictions.

1.4.2 Counter-Terrorism Act 2008 (CTA 2008)

The introduction of account monitoring orders under the Terrorism Act of 2006 laid down the foundation for the expansion of the preventive measures under the CTA 2008. Schedule 7 of CTA 2008 introduced an account monitoring scheme with a broader range of applications and impacts by authorising the treasury to make orders for pursuing a country that presents risk under

[98] Section 4 (2)(b) of the Anti-terrorism, Crime and Security Act 2001.
[99] Home Office, '*Counter terrorist finance strategy'* (Home Office, 5 June 2013).
[100] Law Commission, 'Anti-Money Laundering: the SARS Regime Consultation Paper' (Law Commission 2018) which made it possible for TF activities to be determined based on how suspicious a transaction was.

the AML/CTF guidelines under FATF.[101] The Act also permits the UK to impose a diversity of actions, including economic sanctions, if there is reasonable evidence that the country presents a risk to the UK concerning ML/TF activities.

Schedule 7 of CTA 2008 further outlines the obligations that can be imposed on private sector entities, as well as the directions for imposing those obligations.[102] The directions can include sanctions or instructions for improvement in the due diligence in their actions as a way of preventing risk exposures. To expand the jurisdiction and effectiveness of the Act, Schedule 7 provides for actions brought based on recommendations by the FATF, as well as based on a reasonable assessment by the treasury.[103] The introduction of the principle of reasonability into TF broadens the range of actions that can be considered illegal, both domestically and internationally. Essentially, this represents the increased proactivity and responsiveness to potential risks for TF.

The definition of TF under the Act is deduced from the fact that the Treasury has the power to impose directions to any individuals who are reasonably perceived as posing a significant threat to the UK as outlined in the past legislature, as well as persons involved in the facilitation, manufacture or development of weapons.[104] Persons involved in the financial sector are also viewed as integral in CTF activities because they are in contact with resources that can be easily directed to finance terror activities. Unlike in the past legal frameworks, the heightened risk profiling of these individuals arises from the realisation that terror financing does not necessarily have to be a continuous activity, especially in the era of lone-wolf or opportunistic terror attacks. The willingness of terrorist groups to plan and finance each attack through a unique approach

[101] M Goldby, 'The impact of Schedule 7 of the Counter-Terrorism Act 2008 on banks and their customers'. (2010), 13, Journal of Money Laundering Control, 4, 351.
[102] HM Parliament, 'Post-legislative Scrutiny of the Counter-Terrorism Act 2008 (2014), which states that the Treasury can target a particular transaction, business ties, a nation state as well as a legal or natural person.
[103] FATF, *FATF steps up the fight against money laundering and terrorist financing*, (Financial Action Task Force, 16 February 2012), The original 40 recommendations focused on ML, specifically targeting organised crime groups, most of who had realised the value in exploiting the infrastructure and loopholes in the international financial system. An additional 9 recommendations were introduced following the 9/11 attacks in order to enable member countries to align their AML/CTF strategies to the emergent threat from terrorism, including implementation of UN resolutions for CT, criminalisation of TF, and improve reporting of suspicious transactions within the financial sector.
[104] G Rees and T Moloney '*The latest efforts to interrupt terrorist supply lines: Schedule 7 to the Counter-Terrorism Act 2008*' (2010) Criminal Law Review, 127, identifies the weapons referenced as including nuclear, chemical, biological and radiological.

drove the UK to focus more on prevention rather than intervening based on the learning curve approach that was adapted from the activities of organised criminal groups.

1.4.4 Terrorist Asset Freezing (etc) Act 2010 (TAFA (2010)

The ineffectiveness of forfeitures/confiscation and freezing of assets drove the UK to adopt a sanctions regime to amplify its preventions and interventions against terror attacks. The adoption of sanctions can be traced to United Nations Measures under Terrorist Order 2001.[105] The TAFA 2010 is designed to affect the provisions under Resolution 1452 while amending the CT Act of 2008 to enable the Treasury to sanction any country perceived as being involved in TF. Essentially, the 2010 Act diversified the definition of TF to include the involvement of countries while enabling the UK to rely on the legislative framework created by the UN when assessing the risk of TF. Essentially, TF under TAFA 2010 is divorced from the requirements for criminal intent that were introduced into CTF strategies under the previous legislation. By so doing, the burden of proof and scope of applicability is broadened to achieve the preventive goals. Furthermore, by combining sanctions, freeze orders and forfeitures/confiscation, TAFA 2010 relied on a highly restrictive and intrusive approach to achieving its objectives.

The criteria for determining involvement or assistance to TF was also magnified under TAFA 2010. The target by the US through its freeze orders include funds, financial services and other economic resources which can be used to facilitate terrorism.

1.4.5 The Afghanistan (Asset Freezing) Regulations 2011 (SI 2011/1893)

Although the Anti-terrorism, Crime and Security Act 2001 laid the foundation for the deployment of freeze orders in CTF, the regulations under The Afghanistan (Asset Freezing) Regulations 2011 broadened the provisions under a secondary asset freezing regime that fits into the sanctions by the UN Committee.[106] A similar approach is utilised under The Al-Qaida (Asset Freezing) Regulations 2011 (SI 2011/2742), which is designed to ensure that individuals associated with Al-Qaida and ISIL are treated as individuals who have a high propensity to engage in TF-related activities. As a result, the decision to treat them with suspicion is based on the fact

[105] J Stevens, 'Implementing 'Targeted' UN Sanctions in the UK: Is Freezing of Terrorist Assets Giving Fundamental Rights the Cold Shoulder? (2012) 3, Journal of Terrorism Research. 2, 1, Amended in 2006 and 2009, the Terrorism Order 2001 was aimed at empowering the UK to utilize UN's sanctions regime through smart and targeted sanctions.

[106] M Thomas, *Blackstone's Statutes on Property Law 2019-2020* (Oxford University Press, 2019).

that their relationships with the terror groups motivate their actions, and they have the willingness and commitment to finance terror activities either through:[107]

- Availing economic resources to the benefit of a designated person or terrorist group
- Availing economic resources to a designated person or entity
- Availing funds to benefit a designated person or entity
- Availing funds to a designated person

The provisions in these Acts are designed to counter the limitations arising from sovereignty guidelines, where the actions of persons in another country are protected under international law.[108]

1.4.6 Protection of Freedoms Act 2012

The effectiveness of freezing assets as a proactive and reactive measure towards TF is often discussed with mixed results. Although the propositions were introduced under Resolution 1373, the legislative framework for implementing it was only adopted after the ratification of the Anti-terrorism, Crime and Security Act 2001, following 9-11. On one hand, asset freezing was reported as an effective strategy[109] through disruption and deterrence. However, the effects of freezing assets cannot be quantified, thus trivialising its contribution to the CTF strategies. Similarly, over time, the amounts of assets frozen have reduced to negligible amounts.[110] The effectiveness of freezing assets as part of CTF was viewed as ineffective in changing or inhibiting the conduct of the targeted entities, thus leading to the strategy being considered as more of an auxiliary approach, as opposed to being a primary approach as it once was.

[107] Al-Qaida (Asset Freezing) Regulations 2011 (SI 2011/2742), (2011).
[108] See M Feinberg, *Sovereigty in the Age of Global Terrorism: The Role of International Organisations* (Brill, Boston, 2016), who indicates that the Acts enable the UK to impose sanctions on individuals who are assocaited with persons, properties and materials that are attached to the two terror groups, anywhere in the world.
[109] HM Treasury reported that over GB £100M in assets were frozen, thereby limiting the ability of over 200 individuals associated with over 100 institutions from engaging in terror-related activities.
[110] D Anderson, '*Second report on the operation of the Terrorist-Asset Freezing Etc. Act 2010'* (2012) 11, reports that in spite of the media fanfare, the amounts of frozen assets have reduced significantly, with only £100,000 in 2012, and only £61,000 in 2014, as indicated by D Anderson, '*Fourth report on the operation of the Terrorist-Asset Freezing Etc. Act 2010'* (2014) 11.

1.4.7 TF Definitions Post-Brexit

The UK has introduced two sanctions regimes for CT under the 2019 Regulations. The Regulations[111] aimed at ensuring that the UK's CTF strategy remains compliant with UNSCR 2368.[112] Similarly, in the post-Brexit era, the 2019 regulations enabled the UK to autonomously implement sanctions under its CTF strategies, specifically against international terror groups and entities that support such groups. The regulations apply to any individual residents or citizens, as well as entities in the UK, who hold any economic resources and are or have been involved in terror-related activities. The provisions extend to individuals who are involved with other persons or institutions that have been associated with terrorism by establishing a more robust definition of an 'involved person'.

In summary, the definition of TF under these Acts is dynamic and in response to the transformation of terror financing activities. The changes in the definition of TF under each of these legal frameworks arise from a cause-and-effect relationship between the actions, reactions and counter-actions of terror groups and the UK government. Either entity has shown increased ability and willingness to expand the horizons of its strategies. On one hand, terror groups have reinvented themselves in response to the restrictions imposed by the laws and the actions of the institutions within the UK. On the other hand, the UK has found it necessary to expand the horizons and coverage of provisions of the legal frameworks while creating an institutional infrastructure that is robust enough to cover emergent and extant terror threats.

1.5 Research Aims and Objectives

Therefore, the study aims to conduct a comparative analysis of the approaches adopted by the UK and Bahrain towards cryptocurrencies in the context of TF and ML, evaluating their relevance and efficacy against modern challenges. To address this aim, the following research objectives have been set:

1. To identify the CTF legislative responses towards terrorism financing in Bahrain and the UK;

[111] See Thomas, n 107.
[112] T Keatinge and F Keen, 'Social Media and (Counter) Terrorist Finance: A Fund Raising and Disruption Tool'. (2019) 42, Studies in Conflict & Terrorism. 1, 178, indicates that the resolution is an upgrade to the provisions under Resolution 1373 in response to prevention and suppression of the financing of terrorist activities.

2. To identify the relevant international and national frameworks that regulate efforts against cryptocurrency use in terrorism financing in general, as well as in Bahrain and the UK;
3. To ascertain the implementation and efficiency of 'The Financial War on Terrorism' to counter cryptocurrency-related terrorism financing in Bahrain and the UK;
4. To propose an effective and appropriate CTF legal framework to tackle terrorism financing via cryptocurrencies based on the implementation of the FATF Recommendations.

Considering the research aims and objectives, this thesis seeks to answer the following questions:

1. What are the legislative responses to terrorism financing in the UK and Bahrain, and how effective are they?
2. What distinguishes Bahrain's strategy in executing the Financial War on Terrorism from the UK's, particularly in addressing the threat of digital currencies used for terror financing?
3. How successful is Bahrain in mitigating the risks posed by the use of digital currencies for terrorism financing through its Financial War on Terrorism measures?
4. What recommendations can be made for the UK and Bahrain to enhance their legal framework for AML and CTF in relation to digital currency-based terror finance?

The thesis will also aim to address the following sub-questions:

1. How has TF evolved since the 2001 terrorist attacks in America?
2. How have terrorists embraced new forms of technologies, and do they use cryptocurrencies?
3. Does the international legal framework apply to cryptocurrencies?
4. Does the Financial War on Terrorism re-tackle the concept of terrorism financing?
5. Do the UN counter-terrorism financing provisions after 9/11 address this new form of TF?
6. Does the FATF cover this? If so, what does that entail?
7. How does the FATF evaluate this?
8. To what extent is the UK compliant or not with the FATF recommendations?
9. What is the UK model of regulation towards cryptocurrencies?
10. To what extent is Bahrain compliant with the FATF recommendations?
11. What is Bahrain's model of regulation towards cryptocurrencies?

12. What lessons could be learned from both countries?

1.6 Contribution to Knowledge

Before 9/11, academic research focused on money laundering[113] and fraud,[114] with TF receiving scant attention, considering that until then, tangible currency, goods or property were used to fund terrorism.[115] This focus started to change as the financing mechanisms of terrorist groups, such as Al Qaeda, and the use of charitable donations for terrorism became subjects of interest,[116] along with the broader 'Financial War on Terrorism' and international efforts to curb these funds.[117] Recently, the emphasis shifted towards the financing channels of groups like the Islamic State of Iraq and the Levant,[118] exploring the concept of 'cheap terrorism'[119] and the potential use of digital currencies in terrorism financing, areas surprisingly under-researched[120] despite being recognised threats by HM Treasury[121] and the FATF.[122]

With this in mind, this study examines the challenges cryptocurrencies pose to tracking terrorist financing in the UK and Bahrain, highlighting the shift from traditional financing methods and the recent difficulties in integrating AML measures within peer-to-peer networks. It seeks to understand the specific context of Bahrain by reviewing existing literature on the threats posed by digital currencies in terrorism financing, emphasising the need for novel technical skills and resources to track such transactions effectively, particularly noting that cryptocurrencies have

[113] See M Levi and P Reuter 'Money laundering' (2006) 34 Crime & Justice, 289–368.
[114] See E Podgor, 'Criminal fraud', (1999) 48 American University Law Review, , 729–768.
[115] P A Schott, *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* (The World Bank, 2006).
[116] J Gurulé, *Unfunding Terror: The Legal Response to the Financing of Global Terrorism* (Edward Elgar Publishing, 2008).
[117] N Ryder, 'A false sense of security? An analysis of legislative approaches towards the prevention of terrorist finance in the United States and the United Kingdom', (2007) Journal of Business Law, November, 821-850.
[118] Herein ISIS.
[119] N Ryder, 'Out with the Old and … In with the Old? A Critical Review of the Financial War on Terrorism on the Islamic State of Iraq and Levant' (2018) 41 Studies in Conflict and Terrorism, 79-95.
[120] N Ryder 'Cryptoassets, social media platforms and defence against terrorism financing suspicious activity reports: a step into the regulatory unknown' (2020) Journal of Business Law, accepted for publication; M Campbell-Verduyn, 'Bitcoin, crypto-coins, and global anti-money laundering governance' (2018) 62 Crime, Law and Social Change, 69(2) and K Choo, 'Cryptocurrency and virtual currency: corruption and money laundering/terrorism financing risks?' In: Cheun, D, H*andbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data (*Academic Press 2015), 283-307.
[121] HM Treasury n(110).
[122] FATF, *Anti-money laundering and counter-terrorist financing measures – United Kingdom, Fourth Round Mutual Evaluation Report,* (FATF, 2018) < http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-united-kingdom2018.html > accessed 14 January 2024

complicated this process. The analysis intends to analyse the existing data by outlining preventive measures and lessons that the two countries chosen as case studies (i.e. Bahrain and the UK) can learn from each other's experience in combating TF in the cryptocurrency era.

1.7 Research Structure

This thesis is structured to provide a comprehensive analysis of terrorism financing, beginning with the introduction that provides relevant background information and explains the overall purpose of the research. The following chapter delves consist of the literature review, exploring the challenges associated with TF and the current research gap, and also outlines the research methodology, including the justification of the data collection and analysis methods, and providing the rationale for the chosen case studies that were used in the research – Bahrain and the United Kingdom. The third chapter presents a historical overview of terrorism financing, setting the stage for chapter four, which examines international legal frameworks addressing this issue. Following this extensive examination of international practices, chapters five and six focus on the chosen case studies of Bahrain and the UK, respectively, offering detailed insights into each country's approach to combating terrorism financing. An additional chapter is afterwards devoted to a comparative analysis between these two countries, highlighting the similarities and differences in their strategies and legal frameworks. The final chapter synthesises the findings to conclude, providing recommendations for future policies and research.

Chapter II: Literature Review

2.1. Introduction

This chapter provides a comprehensive overview of the available literature on Terrorism financing ('TF') and money laundering ('ML'). The literature search was conducted through a review of the publications related to terrorism financing in a number of academic databases such as JSTOR, ScienceDirect, Scopus, and Web of Science. To identify the relevant publications on the topic, the researcher used key phrases such as "terrorism financing", "money laundering", "terrorism threats" "terrorism and cryptocurrencies", "cryptocurrency regulation counter-terrorism", "financial crime prevention digital currency", "blockchain technology and terrorism financing". The Boolean operators AND/OR were also used to facilitate the literature search. Priority was given to studies that have been published in the past fifteen years as the researcher acknowledges that the laws surrounding terrorism financing, as well as the method used by terrorists, have undergone a significant revolution in the past fifteen years, which is not accounted for in the older literature.

Therefore, this chapter ascertains the challenges associated with TF. In doing so, the chapter starts by examining the reasons why TF poses a threat to lawmakers, law enforcement agencies and regulators, namely considering the diversity of legal and illegal money-raising sources, as well as the potential victims of such endeavours as the threat of terrorism financing constitutes the first theme in this chapter. The second section examines the investigative, legislative and regulatory challenges that make tackling TF such a formidable task. The third theme examines the regulatory framework and the methods of international evaluation, focusing on the Mutual Evaluation Report (MER). Section four identifies the research gap. The last section of the chapter explains and outlines the methodological approaches employed in this thesis, namely the socio-legal approach and comparative analysis, before ending with the ethical considerations of this research.

2.2. Challenges Associated with TF

The first theme identified from the literature review relates to the legal challenges associated with TF, with the scholarship appraising that the cross-border nature of these activities is a significant

issue that challenges the ability of investigators and auditors to investigate as their jurisdiction is restricted to a single state.[123]

Criminals involved in TF, who frequently also engage in ML, exploit loopholes, privacy laws and banking regulations in order to shield their activities from scrutiny.[124] The evolving tactics employed by these illicit networks, therefore, demand constant adaptation of legal frameworks and enforcement strategies, which are usually hindered by slow national law adoption practices and political interests.[125] Secondly, there is a need to consider how public, private and third-sector organisations operate at a national and international level because they are required to balance compliance with business needs, which may result in limited manpower for reporting and investigating suspicious activity, which further limits information sharing among the different actors.[126] Lastly, the human aspect of these crimes introduces a myriad of other challenges, such as the need to understand the motivations behind TF or to protect witnesses from retaliation.[127]

Investigating and effectively regulating activities related to TF represent complex and multifaceted challenges due to the myriad of legal and illegal sources through which illicit funds can flow and also because of the diverse range of potential victims affected by these crimes.[128] At the same time, balancing the need to enact robust laws and regulations to counter TF and that of ensuring the protection of individual rights and privacy is a complex and intricate challenge. The discussion below explores the multifaceted nature of TF and the inherent complexities of designing and implementing effective legal and regulatory frameworks to mitigate these threats.

2.2.1. The Threat of TF: An Abundant Assortment of Sources and Victims

TF can emanate from both lawful and unlawful origins, rendering it arduous for law enforcement agencies and financial institutions to discern between legitimate financial activities and those intended to support terrorism. Thus, the abundance of sources (e.g. donations, illicit trade, ML, cryptocurrencies, state sponsorship) and victims (i.e. entities including the third sector governments,

[123] Pierre-Laurent Chatain, Emile van der Does de Willebois and Maud Bökkerink, *Preventing Money Laundering and Terrorist Financing* (2nd edn, World Bank Group, 2022) 5.
[124] Schott n(116)
[125] Nina H B Jørgensen *The International Criminal Responsibility of War's Funders and Profiteers* (CUP, 2020).
[126] Wouter H Muller, Christian H. Kalin and John G Goldsworth, *Anti-Money Laundering: International Law and Practice* (John Wiley, 2007).
[127] Timothy Wittig, *Understanding Terrorist Finance* (Palgrave Macmillan, 2011).
[128] Jae-myong Koh, *Suppressing Terrorist Financing and Money Laundering* (Springer, 2006).

businesses and individuals) emerges from the literature review as a significant theme, highlighting TF as a threat to society as a whole.

On the one hand, the legal sources of TF include donations and fundraising from unknowing individuals, from state sponsorships or by exploiting third-sector organisations (e.g. NPOs, NGOs). As such, terrorist organisations rely on donations and fundraising efforts, attracting financial contributions from individuals and sympathetic organisations that are driven by political, religious or ideological motivations, often disguising these transactions as charitable donations or religious obligations.[129] Additionally, they manipulate religious obligations, such as zakat – or the religious duty incumbent upon eligible Muslims to contribute a specified portion of their annual wealth to charitable endeavours,[130] to solicit donations, pressuring individuals to contribute under the guise of fulfilling religious duties, even though the funds are ultimately used for violent purposes.[131] To further obscure their funding sources, terrorist organisations sometimes exploit charitable donations, establishing fake charities or manipulating legitimate ones, making it challenging for authorities to distinguish between genuine charitable giving and support for terrorism.[132] Thus, terrorist groups tend to either create or infiltrate NPOs and NGOs that appear to promote humanitarian or social causes, leveraging the sector's perceived legitimacy and its usefulness for social cohesion.[133] These organisations more easily gain the trust of the public, making it easier to solicit donations and move funds internationally without arousing suspicion.[134] As a result, non-profits serve as intermediaries for receiving and directing funds to terrorist groups, using their financial systems to facilitate money flow while maintaining the façade of engaging in legitimate charitable work. While the vulnerability of their sector to terrorism financing is widely examined, there is a lack of literature on how terrorist groups in Bahrain are exploiting the vulnerabilities of the third sector. There is also a gap in the literature which examines whether the Bahrain government has undertaken counter-measures to limit TF through the third sector and

[129] Emile van der Does de Willebois, *Nonprofit Organisations and the Combatting of Terrorism Financing: A Proportionate Response* (The World Bank, 2010)
[130] Tim Parkman and Gill Peeling, *Countering Terrorist Finance: A Training Handbook for Financial Services* (Gower Publishing Limited, 2007) 41.
[131] Nadim Kyriakos-Saad and others, *Islamic Finance and Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT)* (International Monetary Fund, 2016) 8-11.
[132] Ehi Eric Esoimeme, *Deterring and Detecting Money Laundering and Terrorist Financing: A Comparative Analysis of Anti-money Laundering and Counterterrorism Financing Strategies* (DSC Publications, 2018).
[133] See de Willebois n(124)
[134] Mark Sidel, *Regulation of the Voluntary Sector: Freedom and Security in an Era of Uncertainty* (Routledge, 2010)

whether those measures have been able to support the wider objective of the state to limit money laundering.

Furthermore, the use of cryptocurrencies in non-profit organisations poses unique challenges for tracking and regulation, making it ideal for TF. Pseudonymous transactions in cryptocurrencies obscure the identities of senders and receivers, making it challenging for authorities to trace the source of funds, thus providing a veil of anonymity for terrorist sympathisers making donations.[135] Moreover, cryptocurrencies facilitate global reach, allowing terrorist groups to solicit donations from supporters worldwide and receive funds quickly, bypassing the traditional banking system and its associated regulatory checks.[136]

Additionally, state sponsorship plays a significant role in TF, as some states either directly or indirectly sponsor terrorist groups as a means of furthering their own geopolitical agendas.[137] Indeed, it is not uncommon for certain states to offer financial support to such organisations, aiming to achieve political goals such as destabilising neighbouring countries, countering rivals, or even pursuing proxy wars.[138] State-sponsored terrorism also serves as a tool to exert pressure on other nations or non-state actors, allowing state sponsors to pursue their agendas while exerting a degree of control over local terrorist groups.[139] To maintain plausible deniability and avoid international sanctions or military retaliation, state sponsors operate covertly, utilising intermediaries and clandestine channels to fund terrorists.[140] Cryptocurrencies, for instance, offer state-sponsored terrorist groups an avenue for untraceable financial support, as these groups can receive funds from their sponsors in the form of anonymous and nearly untraceable transactions that avoid the traditional banking system, thus avoiding potential legal or international sanctions.[141] While the literature has acknowledged the propensity of state-sponsored terrorist

[135] Cynthia Dion-Schwarz, David Manheim and Patrick B. Johnston, *Terrorist Use of Cryptocurrencies: Technical and Organisational Barriers and Future Threats* (RAND Corporation, 2019).
[136] Kim-Kwang Raymond Choo, 'Cryptocurrency and Virtual Currency: Corruption and Money Laundering/Terrorism Financing Risks?' in David Lee Kuo Chuen (ed) *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data* (Academic Press, 2015).
[137] Michael Freeman, *Financing Terrorism: Case Studies* (Ashgate, 2012).
[138] Tim Krieger and Daniel Meierrieks, 'Terrorism: causes, effects and the role of money laundering' in Brigitte Unger and Daan van der Linde (eds) *Research Handbook on Money Laundering* (Edward Elgar, 2013) 84.
[139] Nick Ridley, *Terrorist Financing: The Failure of Counter Measures* (Edward Elgar, 2012).
[140] Doron Goldbarsht, *Global Counter-Terrorist Financing and Soft Law: Multi-Layered Approaches* (Edward Elgar Publishing, 2020).
[141] See Dion-Schwarz and others, n 136

groups to rely on cryptoassets for their operations, there is a gap in the literature on how the state of Bahrain has been able to address the proliferation of cryptoassets in the digital realm and whether it has responded well to the terrorism threat emanating from neighbouring Iran. The literature examining how the UK money laundering legislation has evolved to respond to those threats is also scarce, which makes both states an interesting case for further research and comparison.

Conversely, terrorist organisations engage in a variety of illegal activities to fund their activities. One of the most common approaches is to exploit various legitimate channels to obscure the origins of their ill-gotten gains, employing a range of fraudulent and embezzlement tactics to finance their operations.[142] ML is a crucial aspect of this illicit financial ecosystem, as criminals seek to legitimise the proceeds of their illicit activities by running seemingly legal business ventures and even investing in legitimate businesses in the tech, energy, real estate, agriculture and retail sectors.[143] Then, these businesses generate income and provide cover for mixing illicit funds with legally earned profits, making it challenging for law enforcement to trace and disrupt their financial activities.[144] Furthermore, the use of cryptocurrencies plays a pivotal role in facilitating ML, as criminals can easily convert their ill-gotten gains into seemingly legitimate assets, which they then invest in legitimate businesses without arousing suspicion.[145] It is also not uncommon that tax fraud and evasion are employed by individuals and entities involved in terrorist financing to obscure their illegal income, who declare less profits to minimise tax payment and thus maximise the amount of money that can be diverted to terrorist operations.

Additionally, sympathisers within legitimate public, private or third-sector organisations that are in no way related to terrorist groups may embezzle funds from their employers, subsequently channelling these stolen resources to support terrorist groups.[146] Even more so, criminals may resort to identity theft and financial fraud, encompassing credit card fraud, bank fraud or online scams, all of which offer a means for terrorists to acquire substantial and illicit sums of money

[142] N Ryder *White Collar Crime and Risk: Financial Crime, Corruption and the Financial Crisis* (Palgrave Macmillan, 2018).
[143] Koh above, n (129)
[144] Schott above, n(116)
[145] David Lee Kuo Chuen (ed) *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data* (Academic Press, 2015).
[146] See Esoimeme, n(133)

wrongly.[147] Terrorist organisations may also engage in cybercrime, targeting financial institutions through hacking or by manipulating transactions to divert funds into their accounts,[148] while fraudulent real estate transactions, such as mortgage fraud or property flipping schemes, provide more opportunities for terrorist financing and illicit income generation.[149] Likewise, investment fraud, counterfeit financial instruments, pyramid and Ponzi schemes are additional avenues for diverting funds for terrorist financing, and so is healthcare fraud, or the act of submitting false claims to insurance companies or government healthcare programs to obtain fraudulent reimbursements.[150] An aggravating factor is a tendency for criminals to engage in counterfeiting activities involving the production and trade of counterfeit currency and goods, providing terrorists with a multitude of income streams.[151] This proposition will be examined in this thesis through a comparison of the ALM approaches introduced in both Bahrain and the United Kingdom.

For instance, many terrorist groups engage in narcotics or arms trade, participating in the production, trafficking and distribution of illegal drugs and weapons, which are not only lucrative but which are also used as means of destabilising certain countries or regions.[152] Human trafficking is another profitable venture for certain terrorist groups, as vulnerable individuals are often sold into forced labour or sexual exploitation as a means of diversifying and growing potential sources of terrorist financing.[153] Related to this, kidnapping, ransom and extortion are yet another approach commonly employed by terrorists, targeting individuals, businesses or governments and exploiting both emotional and financial vulnerabilities to amass substantial funds in short periods.[154] Smaller-scale approaches for terrorist financing include extortion and protection rackets, which are tactics used to impose unofficial protection taxes on local businesses and individuals, often through threats or violence, enabling criminals to collect funds from small businesses run by individuals who are afraid of retaliation.[155] While the literature has provided an extensive analysis of the

[147] John Madinger, *Money Laundering: A Guide for Criminal Investigators* (CRC Press, 2012).
[148] Brigitte Unger and Daan van der Linde *Research Handbook on Money Laundering* (Edward Elgar, 2013).
[149] Ryder above, n(143).
[150] Madinger above, n (148)
[151] Hitha Prabhakar, *Black Market Billions: How Organized Retail Crime Funds Global Terrorists* (FT Press, 2012).
[152] See Koh n 129
[153] Loretta Napoleoni, *Merchants of Men: How Kidnapping, Ransom and Trafficking Fund Terrorism and ISIS* (Atlantic Books, 2018).
[154] Jørgensen above n(126)
[155] Jeanne K Girlado and Harold A Trinkunas, *Terrorism Financing and State Responses: A Comparative Perspective* (SUP, 2007).

different sources of terrorism financing, there is little material exploring whether the states have developed a sufficiently robust framework to address terrorism financing and whether the existing regulations can effectively handle the different sources of terrorist financing.

Together, all of these various methods demonstrate the adaptability and resourcefulness of terrorist organisations in seeking financial support for their objectives, as well as the variety of crimes that can be committed to ensure TF emphasises the difficulty in tackling such activities. Another important point to consider is that terrorist financing has wide-reaching implications, affecting various parties on both national and international scales. More specifically, policymakers and governments grapple with the national security threat that terrorist financing poses, potentially leading to violence and instability while straining diplomatic relations; law enforcement and regulatory agencies face resource strain and must continually adapt their legal and regulatory frameworks.[156] Furthermore, financial institutions risk reputational damage and are likely to incur compliance costs frequently.[157] Similarly, NPOs may experience reputational harm and increased regulation, while individuals may suffer physical harm and psychological trauma alongside financial losses.[158]

A gap in the literature concerns the nuanced understanding of how different sources and victims interact and influence each other in the context of TF, and this thesis addresses this gap by acknowledging how those funding terrorist financing in the UK and Bahrain have utilised the gaps in the current counter-terrorism legislation to avoid detection and prosecution.

2.2.2. Investigative Challenges surrounding terrorist financing

The next theme identified from the review of the academic literature underscores the complexities and obstacles encountered in investigating terrorist financing activities, as the process is complex and challenging due to various international, national, organisational, economic, legal, political, operational and individual factors. The combination of these factors contributes to long

[156] Geoffrey Pigman, *Contemporary Diplomacy* (Polity Press, 2010).
[157] Ismail Odeh, *Anti-Money Laundering and Combating Terrorist Financing for Financial Institutions* (Dorrance Publishing, 2010).
[158] Oliver May and Paul Curwell, *Terrorist Diversion: A Guide to Prevention and Detection for NGOs* (Routledge, 2021).

investigation and prosecution processes, which inadvertently perpetuate the perception that both TF largely go unpunished, thus increasing the likelihood of such crimes being committed.[159]

First and foremost, there is a need to consider the multifaceted nature of terrorist financing. The cross-border nature of these activities, characterised by international transactions and networks, poses a formidable hurdle for investigators, who are forced to navigate through numerous legal systems, jurisdictions and international cooperation agreements every time for any ongoing investigation.[160] Anti-money laundering regulations tend to be primarily localised, which means that banks usually tend to comply with each country's specific regulations independently instead of pursuing the adoption of a global anti-money laundering perspective that encompasses a unitary set of professional standards.[161] Still, the critical element of international cooperation and trust between various law enforcement agencies and countries is indispensable in tackling the transnational aspects of these crimes.

Nevertheless, cultural differences, political considerations and even historical tensions may further obstruct collaboration, as the prosecution of TF cases is not solely a legal matter but usually also involves political considerations, diplomatic sensitivities and national security concerns.[162] Additionally, there are legal barriers such as privacy and data protection, as well as banking secrecy laws that act as deterrents to effective information sharing, hindering investigators who require access to sensitive customer data from financial institutions, who in turn may encounter legal obstacles when attempting to share customer data with authorities.[163] All of these factors inevitably influence the course and outcomes of investigations, adding a layer of international complexity to the efforts to combat these illicit financial activities. While culture is a factor that influences the development of legal frameworks, the literature has not examined the interplay of culture and politics in the responses to terrorism and terrorism financing. Indeed, the existent literature has examined how the recommendations from international organisations such as FATF

[159] Chady El Khoury, *Countering the Financing of Terrorism: Good Practices to Enhance Effectiveness* (IMF Library, 2023).
[160] Goldbarsht n(141)
[161] Esoimeme n(133)
[162] Nina n(126)
[163] Odeh n(158)

have influenced the ML framework for the states,[164] and much less is being written on how the national culture shapes the legal responses to TF.

Secondly, it is important to consider that the challenges inherent in investigating TF extend to various national and regional aspects related to legislation and the internal policies of affected organisations. A starting point of concern is the challenges related to legal definitions, which involve the precise scope of these crimes within a legal framework.[165] However, drafting laws that encompass a broad spectrum of activities while avoiding overreach that infringes on civil liberties is a complex task that must be done carefully and comprehensively.[166] Another contributing factor is the commonplace absence of standardised regulation across industries and markets, allowing criminals to exploit regulatory gaps and making it easier for illicit funds to flow, thus impeding efforts to track and prevent TF.[167] At the same time, frequent regulatory and political changes add another layer of complexity, with compliance inefficiencies starting to emerge as financial entities are frequently required to grapple with an influx of new regulations.[168] The evolving landscape of counterterrorism financing (CTF) and anti-money laundering (AML) regulations, driven by global events, shifting threats and criminal patterns, necessitates continuous adaptation by businesses and financial institutions, which often divert resources away from investigations and compliance efforts in order to implement new policy changes at the company-wide level.[169] Notably, excessive compliance demands have the potential to burden legitimate enterprises with bureaucratic practices, while insufficient oversight may inadvertently facilitate illicit financial activities by allowing vulnerabilities to be exploited.[170] Thus, the availability of investigative resources and expertise is paramount, while the sheer volume of suspicious activities and transactions can overwhelm public and private institutions, reducing their capacity for thorough monitoring and evaluation.[171] Unfortunately, there is a tendency for law enforcement agencies and regulatory bodies to grapple with resource limitations that affect their ability to combat these activities

[164] Nina n(126)
[165] Campbell n(121)
[166] Nathalie Rébé, *Counter-Terrorism Financing: International Best Practices and the Law* (Brill Nijhoff, 2020) 102-103.
[167] Girlado and Trinkunas above, n (156)
[168] Chatain and others n(124)
[169] Khoury n(160)
[170] Schott above, n(116).
[171] See Esoimeme n(133)

effectively, such as inadequate budgets and a shortage of experts.[172] Because of this tendency, the importance of training and supervision of financial and criminal experts capable of examining activities and identifying suspicious transactions cannot be overstated, as without proper training, investigators may struggle to identify and address suspicious activities in a timely and effective manner.[173] While the literature has recognised the investigatory challenges surrounding ML and TF as well as the threats to civil liberties the AML/CTF legislation poses to societies, there is little research appraising how the Bahraini government has addressed this challenge.

Furthermore, the ever-evolving tactics and criminal versatility exhibited by perpetrators contribute to the complexity of TF investigations. To explain, criminals continually adapt and improve their techniques to avoid detection, as well as utilise various approaches to raise funds, often exploiting legitimate financial systems to conceal their illicit transactions.[174] This can be achieved by depositing illegally gained proceeds into the financial system, concealing the origins of these proceeds, or creating a legal origin for them, the overall goal being to disguise asset ownership and use.[175] Moreover, preventing suspicious transactions is a difficult task that requires dedicated and continuous risk assessments by all public institutions and private organisations that could be victims of TF attempts, as criminals continuously refine their techniques to make transactions appear legitimate, thus detecting non-obvious or subtle red flags in financial transactions requires advanced analytical tools, expertise and time.[176] However, this approach relies heavily on having access to accurate and timely data; however, the absence of reliable data sources, inaccurate or incomplete information and the minimal information exchange between private entities and public institutions can hinder the assessment and management of risks linked to TF.[177] Identifying the proper risk that terrorism financing poses to societies both in the Middle East and Europe is a fundamental challenge to many researchers and practitioners, as the question is still not extensively explored in the current scholarly debate.

[172] Girlado and Harold n(156)
[173] Parkman and Gill n(131)
[174] Scott N Romaniuk, Christian Kaunert and Amparo Pamela H Fabe (eds) *Countering Terrorist and Criminal Financing: Theory and Practice* (CRC Press, 2024).
[175] Abdul Rafay, *Money Laundering and Terrorism Financing in Global Financial Systems* (IGI Global, 2021).
[176] Chatain and others n(124)
[177] Campbell n(121)

Furthermore, many of those participating in TF may lack extensive criminal records, rendering it more challenging to identify and target them using conventional law enforcement strategies.[178] Adding to this difficulty is the lack of an organisational culture that requires timely reporting of suspicious activities. The FATF Recommendations urge individuals, businesses and financial institutions to report suspicious activities in a timely manner, as it plays a pivotal role in early prevention and intervention efforts; however, challenges arise due to a lack of awareness, concern or a reluctance to report discrepancies, further hindering investigations.[179] Even once this social barrier is dismantled, distinguishing between lawful and unlawful financial activities is still a challenging operation, and investigators are compelled to construct robust cases, compiling an abundance of evidence over the course of a long period.[180] In parallel, criminals work outside of such national and regional bureaucratic barriers, developing criminal strategies at a faster rate than national and international entities attempting to develop regulations to counteract these illegal activities.[181] Adding to this difficult process of identifying illicit transactions is the utilisation of informal or unregulated financial systems, including new financial technologies such as Hawala or cryptocurrency trading platforms, which presents a unique challenge for investigators, as these systems operate outside conventional financial regulations and can be difficult to access and monitor.[182] Another less-known challenge met by investigators who manage to overcome the above barriers relates to the legal defences and loopholes employed by legal defence teams attempting to leverage existing laws to protect clients accused of TF, thereby increasing the difficulty of achieving successful prosecutions.[183]

Thirdly, the human aspect of investigating TF presents additional challenges that investigators and law enforcement agencies must contend with. To start, investigators confront complex motivations among those involved in these illicit activities. Understanding these motivations, whether driven by ideology, political beliefs, financial gain or other causes, is essential not only for building

[178] Ryder (n 20)
[179] FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations' (2023). <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf> accessed 17 January 2024.
[180] Girlado and Trinkunas n(156)
[181] See Chatain and others n(124)
[182] Eray Arda Akartuna, Shane D. Johnson and Amy E. Thornton, 'The money laundering and terrorist financing risks of new and disruptive technologies: a futures-oriented scoping review' (2022) 36 Secur J 615, 615.
[183] See Esoimeme n(133)

effective cases but also for identifying patterns that can be used to predict and, therefore, diminish the likelihood of such activities reoccurring.[184] For instance, one such recurring pattern is the presence of insider threats within financial institutions or government agencies in the form of corrupt officials and politicians, complicit or negligent employees, and even data breaches.[185] These insiders either intentionally or unintentionally aid criminal activities, demanding heightened vigilance and robust internal controls to detect and address such threats. While the literature has recognised the threat emanating from the likelihood of terrorist organisations penetrating the state and financial structure, much less is known about how the state must reform its legislation to adequately protect vulnerable entities and how it can prevent more and more organisations from becoming complicit to terrorist financing.

Another pertinent example is related to terrorist recruitment and radicalisation, as the process of luring individuals into TF often involves manipulation, coercion or incentivising susceptible individuals.[186] This presents a challenge in the form of identifying such individuals, including employees and intervening before they engage in illegal activities.[187] Another challenge for investigations is the secrecy and compartmentalisation that occurs within criminal organisations.[188] Specifically, TF groups operate with high levels of secrecy, limiting access to critical information and making it challenging for investigators to trace money trails and networks, as typically only a few individuals have access to critical information. Simply put, capturing one criminal is almost never sufficient to guarantee the operations stop, while whistle-blowers are rare due to the fear of retaliation from the organisations they were a part of or due to the legal consequences that may discourage potential informants from cooperating.[189] Indeed, striking the right balance between the need for effective investigations, transparent collaboration, and ethical standards presents a continuous challenge in such cases.[190] For these reasons, ensuring the safety of witnesses and informants is a critical aspect of the investigative process, while establishing

[184] See Wittig n(128)
[185] Ibid.
[186] Colin P Clarke, *Terrorism, Inc: The Financing of Terrorism, Insurgency, and Irregular Warfare* (Praeger Security International, 2015).
[187] Rafay n(176)
[188] Esoimeme n(133)
[189] Ridley n(140)
[190] Rébé n(167)

effective witness protection programs should become paramount for securing cooperation with all stakeholders in order to ensure the success of national and international CTF activities.[191]

This study uncovered that there are many limitations to investigating TF, notably taking into account the cross-jurisdictional nature of these crimes and the limited access to information across jurisdictions, accounting for any potential diplomatic tensions, the lacking local legislation and limited local resources, as well as the abundance of unique human factors that are inherently difficult to trace without crossing the privacy boundaries of innocents. To further bridge this gap, this research considers the various local investigative challenges experienced by the UK and Bahrain specifically.

2.2.3. Legislative and Regulatory Challenges

The final theme extracted from the literature review highlights the legal and regulatory hurdles associated with combating TF, given that creating effective laws and regulations on CTF is a complex endeavour marked by numerous challenges that must be carefully navigated.

Even from the start, two foundational issues that need to be clearly expressed are the agreed-upon definition of terrorism and the classification of TF activities, as divergent interpretations exist across different countries and jurisdictions, making the task of harmonising CTF laws on a global scale formidable.[192] This challenge underscores the necessity for international collaboration via information sharing and consensus-building among key actors to establish a common understanding of terrorism, which can then be applied at a national level.[193] This necessity is further driven by the fact that TF often transcends borders and involves intricate cross-border transactions; thus, successfully prosecuting such cases poses a unique set of difficulties that require the coordination of international efforts to combat this issue.[194] These issues are crucial in the context of double criminality, a main principle in extradition law that requires an act to be considered a criminal offence in both the requesting and requested jurisdictions for extradition to take place.[195] This point is particularly of note in cases such as TF, as many countries lag in

[191] K E, Boon Huq A and Lovelace D C, *Terrorist Financing and Money-Laundering* (OUP, 2010).
[192] Campbell n(121)
[193] Khoury n(160)
[194] Romaniuk and others n(175)
[195] Schott n(116)

implementing legislation pertaining to cyber offences.[196] Some studies have examined the consequences stemming from the requirement of double criminality to prosecute perpetrators of terrorism financing in cross-border investigations effectively,[197] but what is missing from the literature is a comprehensive analysis of how inconsistent definitions and legal frameworks surrounding terrorism financing (TF) are impacting the investigatory work. Few studies have delved deeply into the complexities introduced by divergent national approaches to defining TF and cyber-related crimes.

Additionally, staying ahead of technological advancements and innovative financial tools used by terrorists presents a significant challenge, requiring legal and regulatory adaptability to understand and address new payment methods, cryptocurrencies and digital platforms that facilitate TF.[198] Terrorists have increasingly turned to financial innovations, which demand that CTF legislation adapt in order to address these new frontiers without stifling innovation or imposing overly restrictive measures on financial service providers.[199] It is important to consider that the financial sector already faces a significant regulatory compliance burden, leading to high operational costs for businesses.[200] Indeed, the poor allocation of resources within both public and private institutions emerges as a critical challenge for CTF efforts, as without the necessary funding and manpower, the process of implementing and enforcing CTF laws becomes challenging.[201] Moreover, the global nature of TF further emphasises the need for international cooperation and resource sharing, as resource limitations can also impede the development and enforcement of CTF laws and regulations, particularly in certain countries and regions that lack the trained personnel and technology necessary for CTF activities.[202] These budgetary constraints are further exacerbated by the need to introduce ongoing monitoring, evaluation and amendment efforts for CTF legislation to assess the applicability and validity of specific sections, articles, provisions, and directives.[203]

---

[196] Clarke above, n(187)
[197] Koh n (129)
[198] Kiran Sood and others, *Big Data: A Game Changer for Insurance Companies* (Howard House, 2022).
[199] Paul Beckett, *Ownership, Financial Accountability and the Law: Transparency Strategies and the Law: Transparency Strategies and Counter-initiatives* (Routledge, 2019).
[200] See Muller n(127)
[201] Wittig n(128)
[202] Campbell n(121)
[203] Rébé n(167)

As such, laws must take into account the diversity of TF sources, including state sponsorship and various legal and illegal activities associated with TF.[204] However, terrorists seek to obfuscate their financial transactions by exploiting informal banking systems that operate outside traditional banking regulations, adding another layer of complexity to the legal landscape.[205] Because of these concerns, balancing the need to monitor charitable donations for potential abuse without discouraging legitimate giving is a nuanced challenge that affects lawmakers and regulators globally.[206] With this in mind, there is a need to guard CTF efforts from the risk of political influence from corrupt policymakers, government officials or political leaders, who prioritise their own financial interests or political agendas in order to get public support or protect diplomatic relationships over the broader objectives of CTF.[207] Indeed, monitoring and evaluation are vital for CTF regulation to ensure that objectivity, accountability and integrity among stakeholders are maintained throughout the entire process.[208]

Related to this, ensuring that banking institutions uphold compliance and reporting requirements may pose additional regulatory challenges. Most jurisdictions, such as the UK,[209] have clear expectations that are mandated by law with regard to customer due diligence, suspicious activity reporting and adherence to sanctions lists, all while ensuring that internal controls within regulated entities effectively identify and report suspicious transactions.[210] Another good approach to diminishing the threat of suspicious transactions is de-banking[211] or de-risking,[212] or the practice taken by financial institutions to terminate relationships with high-risk clients or to restrict

[204] M Freeman *Financing Terrorism*: Case Studies (Ashgate, 2012).
[205] Schott n(116)
[206] Romaniuk and others n(175)
[207] Ridley above, n 17.
[208] Rébé n(167).
[209] Hereafter, MLRs 2017. The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 <https://www.legislation.gov.uk/uksi/2017/692/part/3/made> accessed 22 November 2023.
[210] Goldbarsht n(141)
[211] Debanking refers to the practice of financial institutions closing or restricting accounts to mitigate risks associated with money laundering, terrorism financing, or regulatory non-compliance. Banks may debank individuals, businesses, or even entire industries deemed high-risk due to insufficient transparency, suspicious transactions, or inadequate anti-money laundering (AML) controls.
[212] De-risking refers to the practice where financial institutions terminate or restrict business relationships with clients, sectors, or entire regions perceived as high-risk for illicit financial activities. This often occurs due to AML and CTF regulations, high compliance costs, or potential reputational damage. While intended to reduce exposure to financial crime, de-risking can unintentionally exclude legitimate businesses, non-profits, and individuals from the financial system, leading to financial exclusion and pushing transactions into less-regulated channels, which paradoxically increases money laundering risks rather than mitigating them.

transactions from certain regions, which can be regulated via the introduction of specific risk management practices within such institutions.[213] The literature examining the risks of TF for the banking sector is extensive; however, most of the studies have focused on how the formal banking institutions have responded to the threats that TF poses to their operations. There is a gap in the literature on how the states have tried to address the risks of TF in economies where informal banking institutions are getting more and more popular among the population.

Another intricate aspect of crafting effective CTF legislation is the importance of not only having strong and clear legal measures in place but also ensuring that these measures are aligned with ethical principles to diminish the chance of abusing legal lacunae.[214] Thus, there is a need to consider international human rights and data protection acts so that new laws and regulations do not infringe upon basic freedoms and rights, including the right to free speech and the right to privacy.[215] Indeed, the risk of either public or private organisations infringing upon citizens' privacy raises concerns about surveillance and excessive data collection, which need to be considered prior to legal deliberations.[216] The abuse of a possible *non-liquet* that neither prevents nor punishes such actions could inadvertently result in discrimination against vulnerable individuals and areas and may even flag innocent people and organisations for suspicious activities without justification.[217] This, therefore, highlights the importance of ensuring that CTF laws and regulations are not formulated solely to encourage de-risking but rather to encourage financial institutions to adopt, implement and oversee robust risk management practices.[218] Considering that the regulatory challenges regarding CTF primarily centre around the interpretation and implementation of CTF laws, the development of guidelines, directives, frameworks and procedures is mandatory to ensure practical compliance by financial institutions and other relevant entities.[219] Consequently, CTF laws should also incorporate legal safeguards to protect individuals

[213] Chatain and others, n(124)
[214] Nathanael Tilahun Ali, *Regulatory Counter-Terrorism: A Critical Appraisal of Proactive Global Governance* (Routledge, 2018).
[215] Téwodros Workneh and Paul Haridakis, *Counter-Terrorism Laws and Freedom of Expression: Global Perspectives* (Lexington Books, 2021).
[216] Ibid.
[217] Ali n(215)
[218] Chatain and others n(124)
[219] Girlado and Trinkunas n(156)

and entities from wrongful actions, including account terminations, accusations or asset freezes, to ensure due process.[220]

To illustrate, investigative efforts are encumbered by poor national definitions and classifications of keywords and conditions – which results in differences in interpretations, the lack of banking and third sector regulations, the lack of or slow adoption of innovative CTF techniques and technologies, as well as by the lack of oversight in ensuring these regulations are enforced.[221] This thesis bridges this gap by examining the development of the money laundering and CFT legislation in the UK and of Bahrain and subsequently comparing the two regimes to identify which states have implemented a more effective approach to combat ML and TF and to propose practical approaches to address emerging challenges.

2.3. Regulatory Framework and International Evaluation

The regulation of TF is a multifaceted effort comprising international and national measures to safeguard the global financial system from abuse by preventing, detecting and addressing the financing of terrorist activities.[222] At the international level, the FATF sets global standards and recommendations, encouraging countries to adopt and implement them, while at a national level, the legislation criminalises TF and provides legal mechanisms for investigation and prosecution.[223] As a result, financial institutions are typically subject to rigorous regulations, including Customer Due Diligence (CDD) requirements, transaction monitoring and reporting of suspicious activities, with certain reporting obligations extending to professionals in various sectors.[224] Regulatory authorities, such as Financial Intelligence Units (FIUs), play a pivotal role in identifying and disrupting TF activities, and reports from these units may result in sanctions, including asset freezes and travel bans on individuals and entities involved in TF.[225] Oversight of the non-profit sector, risk assessments, capacity building, adherence to international agreements and conventions,

[220] Beckett n(200)
[221] P Sproat, 'Counter-terrorist finance in the UK: a quantitative and qualitative commentary based on open-source materials', (2010) 13 Journal of Money Laundering Control, 315-335.
[222] Rébé n(167)
[223] FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations' (2023). <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf> accessed 17 January 2024
[224] Chatain and others n(124) at 206, 245.
[225] Muller n(127)

supervision, enforcement, adaptability and fostering public-private partnerships all further strengthen TF regulation, emphasising the need for continuous vigilance and collaborative approaches to combat TF, both domestically and cross-border effectively.[226] However, in order to do so, an objective, standardised tool such as the Mutual Evaluation Report must be employed to assess these efforts.[227] The purpose of this thesis is to address the gap in the literature and to provide a comprehensive framework for counter-terrorism financing based on the experience of both the UK and Bahrain.

2.3.1. The Mutual Evaluation Report

The Mutual Evaluation Report (MER) is a crucial component of the global efforts to combat TF, as it is an in-depth evaluation and assessment of a country's CTF systems.[228] Conducted by an international body, often the FATF or a regional FATF-style body, in cooperation with the country being evaluated, MERs are used to assess a country's efforts in these areas and to ensure that they align with international standards and recommendations for CTF efforts, particularly those established by the FATF.[229] Thus, the importance of MERs lies in their role as a critical tool for measuring a country's commitment to combat TF on an international scale, as they provide a comprehensive overview of a country's legal and regulatory framework, its enforcement efforts, its financial sector's compliance, as well as its overall effectiveness in detecting and preventing illicit financial activities.[230] Despite their significance in providing recommendations to states on how to update their CTF legislation, there is not enough literature examining how both the UK and Bahrain have responded to FATF recommendations and the findings of the MER reports and whether the FATF has been able to promote a positive and manful change to the counter-terrorism legislation of both states, which is an issue that is going to be addressed in this project.

---

[226] May and Curwell above, n 38.
[227] Anne Imobersteg Harvey, *Anti-money Laundering and Counter-terrorism Financing Law and Policy* (Brill Nijhoff, 2019).
[228] Nkechikwu Valerie Azinge-Egbiri, *Regulating and Combating Money Laundering and Terrorist Financing: The Law in Emerging Economies* (Routledge, 2021).
[229] FATF, 'Mutual Evaluations' (2023) <https://www.fatf-gafi.org/en/publications/Mutualevaluations/More-about-mutual-evaluations.html#:~:text=The%20mutual%20evaluation%20report%20is,designated%20terrorists%20or%20terrorist%20organisations.> accessed 10 January 2024.
[230] Khoury n(160)

By design, MERs offer valuable insights into identifying weaknesses and vulnerabilities within a country's CTF framework, facilitating targeted reforms and system-strengthening efforts.[231] Additionally, these reports include risk assessments, aiding in the prioritisation of resources and efforts to address the most significant threats, and as such, researchers and policymakers may rely on these reports to gauge a nation's commitment to and capacity to combat TF and effectively.[232] Furthermore, the use of MERs allows for comparative analysis, enabling researchers to assess how various jurisdictions address CTF challenges, as well as how to identify best practices or areas requiring international cooperation.[233] Even more so, MERs often feature policy recommendations that researchers and policymakers can use as guidance for enhancing their national strategies in the fight against TF.[234] With this in mind, reports from countries with robust CTF measures, such as the UK, are particularly valuable in understanding and setting global benchmarks for effective CTF efforts. Lastly, MERs can also serve as a tool for global accountability, as researchers can track progress and hold governments accountable through these reports.[235] Thus, countries that do not comply with international standards can face reputational damage and may be subject to sanctions or restrictions in the international financial system.[236]

2.4.Research gap

The literature review illustrates that most of the literature on the subject has been in the form of policy prescriptions that are based on international experience and do not reflect the changes in TF legislation in both the UK and Bahrain. There is even less literature appraising the efforts of both countries in fighting those forms of terrorist financing that involve cryptocurrencies. The literature has acknowledged that the states use a modernised version of their ALM and CTF approaches to combat the growing propensity of terrorist organisations to use cryptocurrencies to finance their operations.[237] However, those appraisals have missed exploring the specific way the AML and CTF legislation has been modernised and updated to fit contemporary regulatory needs. Furthermore, most of the existing literature explores the risks of terrorist financing and

[231] Harvey n(228)
[232] Koh n (129)
[233] Azinge-Egbiri n(229)
[234] Harvey n(228)
[235] Beckett n(200)
[236] Azinge-Egbiri n(229)
[237] Akartuna et al, above n 63.

cryptocurrency use for TF purposes[238]instead of delving into the challenges that arise from this specific setting. More specifically, while there are studies that examine the sources and victims of TF, few focus on the use of cryptocurrencies specifically and how these further affect these existing TF practices.[239] There is also little literature that attempts to appraise the investigative, legal and regulatory responses to combatting TF through cryptocurrencies,[240] with limited research focusing on the challenges arising in investigating, legislating and regulating the use of these new types of currencies and the difficulties in examining such transactions.[241] This literary gap is particularly noticeable in comparative studies, as the vast majority of the existing literature focuses on a single jurisdiction instead of taking a comparative angle. Related to this, there is a lack of research comparing the UK with Bahrain specifically, neither seeking to explore how these countries address TF and ML, and especially, there is no such study taking into account the use of cryptocurrencies for TF purposes in these two specific jurisdictions.

The present study is significant because it addresses all of the above-identified gaps in the literature. First, this thesis makes an original contribution to knowledge by focusing on the ML and TF response in Bahrain and the UK. These two jurisdictions have not been extensively in the spotlight of the TF research, and particularly noting that this comparison specifically receives no attention in TF research. Second, unlike most of the studies on the topic, which explore the risks of TF and the investigatory challenges encountered in the process of detecting TF offences, this study focuses on a very specific risk that has been insufficiently explored in academia, namely the proliferation of cryptocurrencies and the growing propensity of a terrorist group to use those cryptocurrencies to finance their operations. The link between TF and cryptocurrencies is a narrow focus that has not been commonly explored in the literature on the subject, as there are many gaps concerning the threat of TF, specifically regarding the abundance of sources and victims, as well as discussing the investigative, legislative and regulatory challenges surrounding the different approaches to TF. Third, the project has a distinct comparative angle, and it aims to uncover both

[238] Christopher Whyte 'Cryptoterrorism: Assessing the utility of blockchain technologies for terrorist enterprise' (2023) 46 Studies in Conflict & Terrorism, 1126-1149.
[239] Donald Rebovich and James M Byrne (eds) *The New Technology of Financial Crime: New Crime Commission Technology, New Victims, New Offenders, and New Strategies for Prevention and Control* (Routledge, 2023).
[240] Aleksander Essex, Shin'ichiro Matuo, Oksana Kulyk, Lewis Gudgeon, Ariah Klages-Mundt, Daniel Perez, Sam Werner, Andrea Bracciali and Geoff Goodell (eds) *Financial Cryptography and Data Security: FC 2023 International Workshops* (Springer, 2024).
[241] Jelena Madir (ed) *Fintech: Law and Regulation* (2nd edn, Elgar Financial Law and Practice, 2021).

the strengths and weaknesses of the counter-terrorist financing and anti-money laundering legal frameworks in the UK and Bahrain and offer recommendations on how those frameworks are to be revised to ensure that both countries follow a modern and informed approach in the area. Considering the unique use of these two case studies and the many issues that have been identified as gaps and which are addressed throughout this thesis, the current research makes a significant and original contribution to knowledge by bridging these research gaps.

2.5. Methodology

The study relies on three methodological approaches: the black letter approach, the socio-legal approach and comparative analysis, examining and comparing two case studies (i.e. the UK and Bahrain).

The black letter research, as a hermeneutic discipline, emphasises the necessity for legal practitioners to scrutinise legal texts and materials to determine their application to legal scenarios. Black letter research aims to understand the law from no more than a thorough examination of a finite and relatively fixed universe of authoritative texts.[242] Advocates of doctrinal research posit that the law is grounded in a set of fundamental principles found within legal texts, cases, and their interpretations.[243] These principles are to be correctly apprehended and shall serve as the starting point for legal analysis. Doctrinal research aims to provide a logical response to logical arguments, operating under the assumption that by employing local and rational methods to extrapolate legal principles to cases, one can arrive at resolutions to disputes untainted by political or moral ideologies.[244]

However, the doctrinal approach is not interested in the factors that influence the external reality in which the legal norms develop, nor are they capable of producing an informed analysis of why the rules in the different legal systems differ.[245] Schwartz himself notes that the only way for the black letter (doctrinal) methods to remain relevant to contemporary legal realities is to constantly readjust itself by embracing the results and the insights of the other external methodologies. Adding external (non-doctrinal insights) to the legal study produces "new reasons more fitted with

[242] V Douglas, Interdisciplinarity and the Discipline of Law'[2004] 31 Journal of Law and society 178
[243] M V Hoecke (ed.) Methodologies of Legal Research (Oxford, Hart Publishing 2011), 1-18.
[244] E H Tiller and F B Cross, 'What is Legal Doctrine?', (2006) 100 Northwestern University Law Review 517
[245] Hoecke n(244(

time"[246] that enable the doctrinal research methodologies to remain relevant. This means that doctrinal methods are not capable of effectively studying the transformation of social realities, not only because they are narrowly framed to examine how the law applies (rather than how the law should and must change) but also because they rely on the established rules and precedents and do not attempt to question them. For that reason, the black letter analysis in this study is supplemented with socio-legal and comparative analysis.

The socio-legal approach is utilised due to its ability to examine the interplay between law and society, focusing on how legal rules and institutions impact and are influenced by social, cultural, political and economic factors.[247] Socio-legal research is highly diverse and difficult to define; however, Jolly describes it as research that investigates law in action and thereby 'transcends exclusively doctrinal analysis of supposedly authoritative legal texts'.[248] To examine the practical application of the law and its social implications, the socio-legal approach employs a variety of methods also to investigate data beyond the text of the law.[249] It entails a review of how doctrines, legal decisions, legal rules, practices and institutional culture operate together to form the reality of the law in action,[250] typically by making use of case study methodology to pinpoint existing operations and issues.[251] In effect, case study research is best employed when the studied phenomena cannot be adequately separated from their context, indicating that the phenomena as observed could not exist similarly under different circumstances.[252]

Thus, the advantage of the socio-legal approach is its capacity for deep insights into the interplay between legal systems and their broader social, cultural and political contexts.[253] By examining these contexts, this approach provides a holistic understanding of how laws are perceived and implemented by individuals and institutions, allowing for a comprehensive exploration of legal phenomena.[254] Moreover, findings from socio-legal research often carry direct policy relevance,

[246] Schwartz, RL, 'Internal and External Method in the Study of Law' (1992) 11Law and Philosophy 179
[247] Reza Banakar and Max Travers *Theory and Method in Socio-Legal Research* (Hart Publishing, 2005).
[248] D Jolly *Exploring the 'Socio' of Socio-legal Studies* (Palgrave Macmillan, 2013) 5.
[249] Naomi Creutzfeldt, Marc Mason and Kirsten McConnachie *Routledge Handbook of Socio-Legal Theory and Methods* (Glasshouse, 2020).
[250] Mike McConville and Wing Hong Chui *Research Methods for Law* (2nd edn, EUP, 2017).
[251] Aikaterini Argyrou, "Making the Case for Case Studies in Empirical Legal Research" (2017) 13 Utrecht Law Review 95-113.
[252] Robert K Yin, *Case Study Research and Applications: Design and Methods* (6th edn, SAGE, 2018).
[253] Dermot Feenan *Exploring the 'Socio' of Socio-legal Studies* (Palgrave, 2013).
[254] David Cowan and Daniel Wincott *Exploring the 'Legal' in Socio-legal Studies* (Palgrave, 2016).

making it an indispensable tool for informing policy-making and contributing to the development of laws and regulations that are not only legally sound but also contextually relevant.[255] However, compared to doctrinal research, which is precise and objective, one potential drawback of the socio-legal approach is its inherent subjectivity and the potential for researcher bias.[256] More specifically, researchers may introduce subjective interpretations and judgments into their analyses due to the intricate interplay of the social, cultural and legal factors examined.[257]

Considering these factors, the socio-legal approach is particularly well-suited to this research because it allows for the consideration of how CTF laws and regulations operate in practice within the unique socio-political contexts of the UK and Bahrain. Employing this approach considers how historical, cultural and political factors shape the CTF legal framework in both countries, notably considering the impact of cultural and social norms on current financial practices. Furthermore, socio-legal research helps assess the real-world impact of CTF measures on individuals, businesses and civil liberties, thus making it possible to examine how these measures affect financial institutions, non-profit organisations and the broader society.[258] Unlike doctrinal research, which may offer a limited or incomplete view of how laws are enforced or whether they can address emergent threats,[259] employing the socio-legal approach can thus help reveal how legal systems adapt to evolving CTF challenges and whether the laws align with international standards while considering local nuances. In effect, employing the socio-legal approach allows the examination of the intended and unintended consequences of CTF measures, the compliance levels and the enforcement practices related to CTF within the socio-legal contexts of both the UK and Bahrain.

Furthermore, this thesis makes use of comparative analysis, which involves the systematic examination of similarities and differences between two or more legal systems.[260] Comparative analysis examines how an issue manifests and is addressed under various legal systems or contexts.[261] The comparative method also excels at highlighting variations in legal or regulatory

[255] Ibid.
[256] Reza Travers n(248)
[257] McConville and Chui n(251)
[258] Burke Uğur Başaranel and Umut Türkşen, *Counter-Terrorist Financing Law and Policy: An Analysis of Turkey* (Routledge, 2019).
[259] Creutzfeldt n(250)
[260] George Mousourakis, *Comparative Law and Legal Traditions: Historical and Contemporary Perspectives* (Springer 2019).
[261] Mathias Reimann and Reinhard Zimmermann, *The Oxford Handbook of Comparative Law* (2nd edn, OUP 2019).

approaches, allowing for an in-depth exploration of policies, procedures and their implications by helping pinpoint factors contributing to differences in effectiveness.[262] Adding to the complexity offered by the use of the socio-legal approach, the comparative analysis examines diverse legal contexts, helping to identify successful patterns, strategies or approaches in one jurisdiction that can be transplanted into another.[263] In doing so, comparative analysis promotes knowledge sharing and the cross-pollination of ideas, as policymakers can draw from these insights to enhance their own CTF efforts. Moreover, comparative analysis can shed light on shared challenges faced by both countries and unique challenges specific to each jurisdiction, this insight being instrumental in developing well-informed policy recommendations.[264]

However, comparative analysis presents its own set of challenges. One complexity lies in the in-depth understanding required of the legal systems and regulatory frameworks in both countries, with researchers having to possess comprehensive knowledge and expertise of the subject matter to conduct effective cross-country comparisons.[265] Related to this, another potential limitation is data availability and comparability.[266] More specifically, obtaining relevant, reliable and comparable data for both the UK and Bahrain can be challenging, as data sources, formats, quality and quantity may vary. Moreover, a comparative analysis may not fully capture cultural nuances unique to each context; however, the decision to complement the comparative analysis with contextual insights gained from the socio-legal approach was specifically made to address this limitation.

This study makes a comparative analysis of the legal frameworks, policies, and practices in the UK and Bahrain, and it helps identify the differences in their approaches to CTF. Considering the functional equivalence method, which assumes that certain institutions fulfil analogous functions in spite of the disparities in legal systems,[267] the comparison focuses on the intended purpose and utility of the CTF strategies of both countries. Effectively, this method allows the assessment of the effectiveness of CTF measures in each country, making it possible to evaluate which strategies

[262] Geoffrey Samuel, *An Introduction to Comparative Law Theory and Method* (Hart Publishing 2014).
[263] Mark Van Hoecke *Epistemology and Methodology of Comparative Law* (Hart Publishing 2004) 172.
[264] Mousourakis above n.261
[265] Roberto Scarciglia, *Methods and Legal Comparison: Challenges for Methodological Pluralism* (Edward Elgar Publishing 2023).
[266] Pier Giuseppe Monateri *Methods of Comparative Law* (Edward Elgar 2012) 310-311.
[267] Reimann and Zimmermann n(262).

or regulatory frameworks are more successful in achieving their objectives by understanding the successful strategies employed in one jurisdiction and which may be applicable or adaptable to the other.[268] Thus, comparative law has been adopted so that the thesis does not focus the research questions on comparing legal systems but rather uses this approach to assess the efficacy of the profit-driven reporting model in detecting financial flows linked to terrorism. This approach facilitates the comparison of how the selected jurisdictions differ in their approaches to counter terrorist financing in relation to the international legal framework set out by the UN, the EU and the FATF. For comparison, the UK and Bahrain were selected as case studies based on the diverging characteristics of the two countries, with reference to the general legal frameworks and specific CTF measures. The thesis employs a diverse array of analytical methodologies to explore the evolution of regulatory frameworks in the UK, encompassing aspects such as the 4th and 5th Anti-Money Laundering Directives (4AMLD and 5AMLD). In addition, for the UK this thesis reviews the Proceeds of Crime Act 2002, various Financial Services and Markets Acts including FSMA 2000, FSMA 2001, FSMA 2005, the Financial Services Act 2012 and 2021, The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 and its Amended Regulation MLR 2019, Policy Statements such as PS 20/10 and PS 19/22, the Sanctions and Anti-Money Laundering Act 2018, to name a few. For Bahrain, this study reviewed various articles of the Bahrain Constitution, as well as the Central Bank of Bahrain (CBB) and Financial Institutions Law, including Law No. (54) of 2006, Law No. (25) of 2013 and Law No. (36) of 2017, Decrees No. (4) of 2001, (64) of 2006 and (29) of 2020, Ministerial Orders such as (102) of 2001, (9) of 2007, (17) of 2017, (173) of 2017, (108) of 2018 and Decisions including No. 18 of 2002, several articles from the Penal Code 1976 and sections from the GCC Customs Law, among others. This comparative exploration aims to illuminate the pathways through which Bahrain can adapt or enhance its own measures similarly or more effectively than those of the UK. Additionally, the successes and shortcomings observed within the UK's regulatory frameworks will be scrutinised, with the objective of enabling Bahrain to develop a framework that circumvents potential pitfalls and shortcomings.

Finally, considering that the thesis investigates CTF practices in the UK and Bahrain, ethical considerations play a pivotal role. Transparency, data accuracy, integrity and accountability are

[268] Van Hoecke n(264)

some of the key elements for sound research methodology,[269] and these were pursued to uphold ethical standards throughout the entire research. Plagiarism is another critical ethical concern in legal research, and to avoid plagiarism, the researcher ensures proper citation and attribution of all ideas and concepts to their sources.[270] At the same time, ensuring the privacy and confidentiality of individuals and organisations involved in CTF activities is paramount;[271] thus, the researcher diligently followed the ethical guidelines regarding data protection and confidentiality. The researcher also maintained objectivity and integrity while avoiding conflicts of interest, as there are no financial or personal relationships that could affect the research. Furthermore, this research sought to strike a balance between advocacy for policy recommendations and maintaining impartiality, while adherence to human rights standards was perceived as a vital ethical consideration.

2.5.1 Rationale for selecting Bahrain and the UK as case studies for the research

Bahrain and the United Kingdom were chosen as case studies for this thesis. While there is a scarcity of research on Bahrain and the UK's efforts in combating TF through crypto-currencies, the UK has one of the most advanced legal frameworks for money laundering and terrorism financing that serves as a blueprint for other countries on how to develop their AML and TF responses.[272] With a well-established financial system supported by robust legal frameworks, the UK has been addressing terrorist financing since the 19th century, employing comprehensive measures and penalties for violations under the Terrorism Act 2000 and other regulations.[273] Its mature CTF framework aims to protect regional economic stability and is recognised for compliance and effective financial reporting, as evidenced by positive FATF evaluations.[274] As a

[269] Geoffrey C Hazard and Angelo Dondi, *Legal Ethics: A Comparative Study* (SUP 2004).
[270] Camille Yip, Nian-Lin Reena Han and Ban Leong Sng, 'Legal and ethical issues in research' (2016) 60 Indian J Anaesth 684.
[271] *Ibid*.
[272] Hynes, Paul, Nathaniel Rudolf, and Richard Furlong, *International money laundering and terrorist financing: a UK perspective*. (Sweet And Maxwell 2016)
[273] N Ryder, *The Financial War on Terrorism: A Review of Counter-Terrorist Financing Strategies Since 2001* (Routledge, 2015). K Harrison and N Ryder, *The Law Relating to Financial Crime in the United Kingdom* (Routledge: 2016) at 60.
[274] For a recent analysis on the UK's compatibility with the international CTF standards see Financial Action Task Force Anti-money laundering and counter-terrorist financing measures United Kingdom Mutual Evaluation Report (Financial Action Task Force: 2018).

leading UN and FATF member, the UK significantly influences global counter-terrorism financing decisions and best practices.[275]

In contrast, Bahrain, situated in a region known for Islamic terrorism origins, has less exposure to terrorism but faces significant risks in TF. Its counter-terrorism financing legislation, starting in 2006,[276] is influenced by Islamic Sharia, which presents challenges in adopting FATF-established frameworks. With only 50 years of independence, Bahrain lacks the UK's experience and institutional resilience, although it models much of its CTF legislation on Western frameworks.[277] Even so, FATF-MENAFATF reports suggest Bahrain has only moderately recognised TF and ML risks, highlighting the need for learning from the UK's successful approaches.[278] Still, Bahrain was chosen for this research as it has far more progressive legislation in relation to ML and TF than its Gulf neighbours.[279] The country has been very proactive in passing legislation to update its ML framework, and this legal activism cannot be found in the other countries in the Gulf.[280] Still, there is a need to question whether the reforms that were conducted are sound and whether the country is following the most relevant advice from the international community on how the ALM and TF legislation should be written. Furthermore, there is little research tracing how Bahrain has responded to the exorbitant growth of ML attempts in cryptoassets, which further spurred the author's interest in the area.

Thus, a comparison between a state with advanced ALM legislation (such as the UK) and a country with an ALM framework still in development (such as Bahrain) will provide lessons for policy transplant and help uncover gaps in the current ALM and TF framework in Bahrain. Furthermore, the research will provide insights on how the UK AML and TF framework is to be strengthened by analysing the areas and aspects in which Bahrain has performed comparatively better.

---

[275] Clarke n(187)

[276] B E Whitaker, "Exporting the Patriot Act? Democracy and the 'War on Terror' in the Third World." (2007) 28 Third World Quarterly, 1017-032.

[277] C L Yordan, Enacting Counter Terrorism Financing Laws in the UAE and Bahrain: The Fusion of Global Pressures, Regional Dynamics, and Local Interests (March 1, 2008).

[278] FATF-MENA *FATF , Anti-money laundering and counter-terrorist financing measures -Bahrain, Fourth Round Mutual Evaluation Report, (*FATF 2018) <http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-bahrain-2018.html>

[279] IMF Country Report, 'Kingdom of Bahrain: Detailed Assessment on Anti-Money Laundering and Combating the Financing of Terrorism' (IMF 2007), <https://www.imf.org/external/pubs/ft/scr/2007/cr07134.pdf> accessed 14 February 2023

[280] AAlmutawa, 'Terrorism measures in Bahrain, proportionality and the interplay between security, civil liberties and political stability. (2018).The International Journal of Human Rights, 1–17.

Additionally, the thesis will explore the impacts of anti-terror financing laws on human rights, identifying potential areas for Bahrain to improve, especially in human rights protection, by comparing socio-legal approaches and learning from the UK's experiences to enhance CTF practices and compliance amidst evolving threats.

All things considered, the lack of literature exploring in sufficient detail the English and Bahraini responses to combatting ML and TF is surprising for a number of reasons. First, both states are international financial hubs and have significant international influence, which exacerbates their vulnerability to TF and ML. Thus, comprehending the strategies and approaches employed by both countries is necessary to appraise the current developments and the broader trends in the area. Secondly, the growing popularity of cryptoassets as a means for facilitating ML and TF seems to have eluded scholarly attention. While researchers have recognised that traditional legal and regulatory response might be insufficient to counter the complexity of ML and TF, there has been little interest in appraising the new methodologies used for preventing, investigating and prosecuting these crimes in both the UK and Bahrain, which is also the focus of the present research. Thirdly, one must also acknowledge that there are regional variations in the responses to TF and the proliferation of cryptoassets. By studying ML responses in a country from Europe and a country from the Middle East, this research will acknowledge those regional variations and attempt to bridge the divide between the European and Middle Eastern responses to terrorist financing.

Chapter III: The history and evolution of terrorism financing: a conceptual overview

3.1 Introduction

This chapter reveals how counter-terror financing (CTF) measures are designed to balance the dual-purpose regime of depriving terrorists of the funds necessary to finance their operations while relying on financial intelligence for detection and disruption of the network of terrorists. The discussion reveals that the development of CTF measures is an event-driven process, with rapid expansion precipitated by particular events.[1] Furthermore, the discussion will also indicate that the effectiveness of CTF measures has often proven to be a precipitant of the innovation of new measures as terrorists design workarounds and alternative measures. As a result, the utility of any strategy is limited by time and space, with the objective of the government institutions being to do as much damage as possible before the terrorists innovate. A clear appreciation of terrorism financing (TF) is integral in counter-terrorism (CT) strategies since it enables governments to confront, weaken and ultimately suppress terrorists without a confrontation. With the emergence of the new terrorism models whereby the individual terrorists and groups are nondescript, TF remains the only evidence of their existence. The chapter aims to address the following three subsidiary research questions. First, how has TF evolved since the 2001 terrorist attacks in the United States of America (US)? Secondly, how have terrorists embraced new forms of technology? Thirdly, do terrorists use cryptocurrencies to fund acts of terrorism?

3.1 The Evolution of Terrorism Financing

This section focuses on factors that drive TF, including key political events that lead to disenfranchisement, changes in technology, the multiplicity of AML/CTF strategies, and changes in the social, cultural, economic, and political environments. The analysis focuses on the primary drivers that explain the proliferation of terrorism financing starting from the late 19th century and moving on to contemporary times.

[1] Y Heng, and M Ken, 'The Other War on Terror Revealed: Global Governmentality and the Financial Action Task Force's Campaign against Terrorist Financing.' (2008) 34 Review of International Studies, 3, 553

3.1.1 The Anarchists

Terrorism in the 19th century started with anarchists, who were part of the anti-establishment movement. Although they were spread across Asia, Europe, the US and the Balkans, they were essentially domestic terror groups with their attacks planned and implemented domestically. In the United Kingdom (UK), the anarchist movement emerged in 1880 and sought to challenge state control, capitalism, conformity and social hierarchy.[2] The attacks by the anarchists were deployed through targeted political assassinations, which were carefully planned to avoid collateral damage, to avoid criminal liability, and to create a code of honour among the potential and current supporters. In addition to the use of bombs,[3] the anarchists used stabbings and shootings to achieve their objectives.[4] Technology played an integral role in the role of anarchical terrorism since it was possible to achieve a broader audience through the improvement in print media.[5]

3.1.2 Terrorism Financing in the 19th Century

The convergence in their ideology, coupled with the simplicity of their attacks, explains why terrorists in this era had limited budgets. TF was limited to mechanisms that could be justified under the revolutionary ideology. However, there is evidence that anarchists targeted wealthy individuals in their illegal TF activities since this fits the profile of their objectives.[6] Using the example of the Galleanists[7], the Italian group utilised terror strategies and tactics that were later adopted and improved on by al Qaeda (AQ). By using existing social systems[8] to mask their activities, these anarchists established an intricate operational strategy aimed at forcing political change. Similarly, rather than engage in TF, they utilised the available resources for the various

[2] H Shpayer-Makov, Anarchism in British Public Opinion 1880-1914." (1988), 31 Victorian Studies,: 489, indicates that the movement bore diverse ideological inclinations, institutional frameworks and ethnic groupings.
[3] R Jensen, 'Daggers, Rifles and Dynamite: Anarchist Terrorism in Nineteenth Century Europe' (2004) 16 Terrorism and Political Violence 134 indicates that at the height of anarchy, the extensive use of dynamite for assassinations and other forms of terror attacks deviated from the original targeted attacks and assassinations by the original anarchists.
[4] Ibid, 119, who cites a number of stabbings targeting prominent people across Europe.
[5] Ibid at 121, the assassination of Alexander II came at a time when the telegram-based communication was efficient, and in the process, resulted to emergence of similar anarchist movements in other locations.
[6] M Freeman, Financing Terrorism*: Case Studies* (Ashgate, 2012) 63.
[7] J D Simon, 'The Forgotten Terrorists: Lessons from the History of Terrorism'. (2008) 20 Terrorism and Political Violence, 2, 195
[8] Ibid, just like Al Qaeda who used mosques for meeting and recruiting, the Anarchists met in the workplaces and used the infrastructure to plan and implement attacks without being seen.

attacks.[9] This form of self-financing led to limited resources available for each attack, although this did not limit the impact of their actions.[10] The role of technology is also apparent in the TF strategies. The innovation of dynamite as a weapon for targeted assassinations as well as to spread terror among the masses came at a time when mass communication and transportation media were introduced.[11] Technological developments such as the advance of cryptography have played an important role in those who attempted to finance terrorist organisations in those early days as they have provided perpetrators with the means to avoid detection by the police and local security agencies.

3.1. 3 The 1920 anti-colonists

The end of the terrorist acts of the Anarchists culminated in the creation of the League of Nations.[12] Due to the increased wave of colonisation by European countries, anti-colonial groups set out to object to this rule through large-scale compliance violence, which targeted the structures utilised by the colonialists. This targeted approach to terrorism established a clear enemy, with the perpetrators recruited from the victims of colonisation.[13] Although they are not essentially considered territory-controlling groups, the anti-colonialists utilised their awareness of their country and the people there to plan and execute attacks. The financing of anti-colonial movements often relied on local support and international solidarity, with the main sources of funds coming from grassroots fundraising and sympathetic external actors. By analysing historical funding mechanisms, one can understand how these movements sustained their operations and how such strategies have influenced contemporary terrorism financing methods.

[9] H Costa and J Baños, 'Bioterrorism in the literature of the nineteenth century: The case of Wells and The Stolen Bacillus', (2016) 3 Cogent Arts & Humanities, 1, 1, who theorised that terrorists presented an existential threat, with the possibility of holding biological and nuclear weapons, based his projections on the fact that some individuals had shown increasing abilities to acquire and use such weapons.

[10] The assassination of the Archduke of Austria in 1914, led to a domino effect that ended in the First World War, which fit into the objectives of the anarchists' ideology.

[11] K Zimmer, "Propaganda by the Deed." In Immanuel Ness (ed) *The International Encyclopaedia of Revolution and Protest*. (Blackwell, 2009), who indicates that the mass communication and transport media offered the anarchists additional opportunities to achieve their goals. Through print media, their acts could reach the millions, while the new transport infrastructure enabled people to more fluidly.

[12] S Kumar, ''Terrorism' or the Illegitimacy of Politics in Colonial India." (2016) 44, Social Scientist 43, who indicated that the League of Nations was established in 1920 to bind nations together, and in the process, the dissatisfaction led to motivations for the anti-colonists.

[13] B Stora, *Algeria, 1830–2000: A Short History*. (Cornell University Press, 2004) 36 uses the example of the National Liberation Front (FLN), which was organised as a nationalist entity in Algeria. By controlling most of the rural areas and with the exceptional familiarity with the country, the FLN, much like other entities, are known to have used the peasants to plan and implement their attacks.

3.1.4 Anti-Colonial Terrorists

The anti-colonialists used a multiplicity of TF strategies, most of which were established around mutually beneficial and symbiotic relationships with the members of the society in which they operated. Since most were guided by the Marxist-Leninist ideology,[14] the nationalists, who sought to reclaim their countries, drew their financing from activities that were justified on the backend benefits of self-governance. Similarly, the groups benefited from their ability to utilise the infrastructure and systems in their native lands to facilitate the attacks.[15] Furthermore, some groups exploited the available resources to further their criminal activities.[16] The nationalists also presented themselves as liberators, thus giving them the power and freedom to utilise the resources within the community to finance their activities.[17] Although the anti-colonial movement was global, each group relied on domestic funding since the goals of their activities were primarily national.[18]

3.1.5 The Irish Republican Army (IRA)

In the late 20th century, terrorist groups, specifically the IRA, relied on violent campaigns to achieve their objectives of keeping Ireland unstable to frustrate the British colonialists. Just like past groups, the extensive committed to ideological purity, the groups shunned illegal and crime-related TF activities to preserve their reputation. Furthermore, changes in the legal frameworks imposed stringent punitive measures for certain criminal activities, thereby leading to increased

[14] Roth and Sever noted that the PKK to explain how the ideology behind the group influenced the financing strategies. M Roth, and M Sever, "The Kurdish Workers Party (PKK) as Criminal Syndicate: Funding Terrorism through Organized Crime, A Case Study," (2007) 30 Studies in Conflict and Terrorism, 905.

[15] These included ability to communicate easily and covertly with the members of society as compared to the foreigners, as well as the ability to blend into society as and when needed.

[16] The PKK, which had access to over 5,000 miles of coastal land, exploited the shipping lands, as a transit point into Europe, where heroin purchased at US$1000 could be sold at a wholesale value of US$20,000-80,000 and a street value of US200,00. See F S Sahin, 'Case Studies in Terrorism-Drug Connection: The Kurdistan Workers' Party, the Liberation Tigers of Tamil Elam, and the Shining Path' (MA Thesis University of North Texas, 2001) p. 41), who indicates that the PKK made as much as 56M Marks in 1993.

[17] There are similarities in the actions of anti-colonialists, including the Mau Mau from Kenya by *H Bennett, 'Fighting the Mau Mau: The British Army and Counter-Insurgency in the Kenya Emergency'*. (Cambridge University Press 2014). *p. 147.)*

[18] S F Dale 'Religious Suicide in Islamic Asia: Anticolonial Terrorism in India, Indonesia, and the Philippines' (1988), 32 The Journal of Conflict Resolution, 39, who indicated that cross-border financing for anti-colonial terrorism did occur in the second half of the 20th century, following the defeat of most of the colonial powers. These forms of assistance were aimed at enabling countries that were still oppressed to achieve independence, and this occurred as late as the 1970s, with South Africa receiving assistance as late as the 1990s.

surveillance by law enforcement agencies.[19] This explains why one offshoot of the IRA, the Provisional IRA, is credited with creating a sophisticated network for financing terrorist activities.[20] The most intricate form of support for the IRA originates from its pseudo-legal activities, most financed through diaspora support, with institutions such as Noraid.[21] The IRA thrived on legal businesses, normally acquired by the group through illegally acquired funds, then exploited and ran into bankruptcy.

However, the IRA has shelved the violent campaigns in preference of political engagement for security political influence.[22] The change resonates with the transition from illegal TF activities such as theft, kidnappings and drug trade since these actions have been criminalised, besides the criminalisation of supporting terrorist groups.[23] Similarly, several changes in TF are observed with the IRA due to the increased surveillance on the purchase of the materials for implementing attacks, such as weapons.[24] Ultimately, the IRA was forced to focus on homemade weapons, whereby the terrorists relied on readily available materials to create improved explosive devices.

In that respect, Horgan and Taylor observe that the income-generating activities of the Provisional Irish Republican Army (PIRA) are not much different from the ones employed by other terrorist organisations; however, they could be deemed more sophisticated and specialised.[25] Nevertheless, unlike most other terrorist organisations, PIRA was, at its peak, heavily embedded in Irish society, which made it possible for PIRA to purchase legitimate businesses through illegal proceeds and subsequently launder money through those businesses.[26] The interest of PIRA in legitimate

[19] M Jonsson and S Cornell, 'Countering Terrorist Financing: Lessons from Europe' (2007) 8 Georgetown Journal of International Affairs, 69, who indicates that the IRA stopped kidnap for ransom after a failed kidnapping of D Tidey, a British national, which ended in a fire fight with law enforcement agencies and led to loss of reputation of the IRA and backlash from the Irish community.
[20] *Ibid*
[21] Diaspora support formed 50% of the funding for the IRA between 1970 and 1980. See Jonsson and Cornell above, n 19.
[22] This approach was also adopted by the Palestine Liberation Organisation (PLO), which is a former terror group that denounced its past activities. Although violent and dissident elements of PLO and IRA still exist, their mainstream agenda has been transformed to primary focus on legitimate political endeavours.
[23] The IRA is more focused on TF activities that relate to victimless crimes, as well as the less-risky TF activities, since these are more cost effective. One of the key considerations is the cost of supporting.
[24] J Horgan and M Taylor, 'Playing the "Green Card" -financing the provisional IRA: (1999) 2 Terrorism and Political Violence who cites Operation Silo, implemented in 1992 to impede the ability of the PIRA to acquire weapons, mainly from the Middle East, and led to recovery of 60% of the weapons acquired by the PIRA from the Middle East.
[25] *Ibid*.
[26] Horgan and Taylor n(24).

business activities is not surprising, considering that it was far less costly for the organisation to run a business than it was for it to organise armed robbery and subsequently pay for the family of the perpetrators if something goes wrong.[27] What was also notable in the PIRA's case was that the organisation employed a flexible operational structure; this is not the case for the department that was overseeing IRA's financial operations, as control and organisation of the financial activities were entrusted to a few selected individuals.[28] There are a number of reasons why PIRA was so successful in its financial operations. First, the funding activities were organised; second, the funding activities were task-specialised as the organisations had different units and personnel specialised in specific money-generating activities.[29] Third, unlike many other terrorist groups that rely on financing activities to enrich the high-ranking members of the organisations, the PIRA financing was solely directed towards ensuring the organisational survival of the group and enabling it to continue with its insurgency activity.[30] What also enabled PIRA to succeed in its financing activities was able to create a network of individuals from the non-terrorist world to support the organisation in obtaining and concealing the proceeds of crime[31] Furthermore, PIRA financing operations were flexible and adaptable to the context and the external circumstances in which the organisation was operating. Thus, the organisation become very opportunistic in exploiting the financing opportunities. While the PIRA had a diversified source of income, it could not tap into all the resources traditionally available to terrorist organisations. For example, there is evidence that PIRA stayed away from drug trafficking and drug selling because its leaders believed that involvement in the drug trade would compromise the relationship with the local community.[32] All of this suggests that terrorist financing is a complex operation, the success of which depends on the capability of the organisation to funnel illegal proceeds of crime to legitimate businesses and to diversify the sources from which it obtains its revenue. PIRA ML and TF activities are devoid of the technological sophistication that is present in the modern TF methodology; the PIRA experiences showcase how important it is for the terrorist organisation to establish itself as a legitimate political actor to support its financing operation. The PIRA experience is important for

[27] *Ibid*
[28] *Ibid*.
[29] *Ibid*.
[30] *Ibid*.
[31] *Ibid*
[32] *Ibid*

researchers interested in TF in the Middle East, where many terrorist organisations are as well embedded in the fabric of the society in the same manner as PIRA was and the methods that the police and security forces used to prevent TF can inform contemporary responses in Middle Eastern societies, and Bahrain in particular.

3.2 The Hybrid-Terror Organisations of the Mid and Late 20th Century

The successes and failures of the anti-colonialists, coupled with the changes in the political, social and economic environment in the mid and late-20th century, led to the emergence of hybrid terrorist groups. The motivation behind the hybridised approach includes the ability to utilise violence and terror as and when needed, as well as banking on political goodwill to further their objectives.

There are direct and indirect motivations associated with TF for hybridising the operations of terror groups. On the one hand, the ability to combine illegal and legal TF activities is increased under the hybrid institutionalisation of terror groups. This is achieved by having decentralised operations, with the ability of the group to justify the distinction between the violent and non-violent entities, even though they both have similar goals. However, different groups have utilised the hybrid approach in different ways. Most of the hybrid-terrorist organisation's literature relates to the activities of Islamic Hezbollah,[33] which is fundamentally comprised of two entities, the paramilitary[34] and the political wing.[35] The group, which started as a resistance movement, has reinvented itself as a multifaceted entity that can seamlessly transform into a resistance, political and religious entity.[36] Through a process commonly termed the Lebanonisation of Hezbollah[37] gave the organisation the ability to influence policy in the country while bestowing upon the leadership the ability to command respect from foreign nations interested in compromising the

[33] E Azani, 'The Hybrid Terrorist Organisation: Hezbollah as a Case Study' (2013) 36, Studies in Conflict and Terrorism, 11, 899, who indicates that which was formed in 1985 in Lebanon, is a political and militant group affiliated with Shia Islamists.

[34] *Ibid* Hezbollah's paramilitary wing, the Jihad Council, is a designated terrorist groups in most countries and regions across the globe, including the EU and the Arab League

[35] Azani n(33)

[36] M Rudner, 'Hizbullah Terrorism Finance: Fund-Raising and Money-Laundering', (2010) 33 Studies in Conflict & Terrorism, 8, 700.

[37] D O Shaw, 'Beyond necessity: Hezbollah and the intersection of state-sponsored terrorism with organised crime'. (2019) 3 Critical Studies on Terrorism, who indicates that its budget it used for a multiplicity of purposes, including economic and social services, inter-terror cooperation with other groups such as Hamas, Marty's charity, religious institutions for supporting the spread of Islam, media and propaganda, armed militia such as recruitment, weapons and other logistics, administrative purposes and to fund political campaigns.

sovereignty of Lebanon.[38] It can be argued that Hezbollah has been one of the key groups that has revolutionised money laundering and terrorism financing. The experience of the Lebanonisation of Hezbollah in Lebanon shows how easy it is for a terrorist group to establish itself as a legitimate political actor whose financial operations should not be scrutinised or considered as a potential sponsor of terrorist activities. Recognising whether remittances to Lebanon are used to support terrorist groups is also one of the key challenges the governments in the Middle East still struggle to address. Technological sophistication and the adoption of new technologies, including cryptocurrency payments, have defined Hezbollah's approach to terrorism financing in the past few years due to the decline of Iranian funding for the organisation.[39] Unlike many other terrorist organisations, Hezbollah has branches in many countries throughout the world, including Europe, Latin America, and the Middle East, and crytoassets provide a convenient medium for the organisation to facilitate the movement of ill-gotten funds. [40] Understanding how Hezbollah has utilised technology and cryptocurrency is of importance for this project, as terrorist financing through Hezbollah is a major threat that the Bahraini government must respond to.

3.3 Traditional TF Methods

These criteria reveal that the choice of a TF approach involves a trade-off, with the identification of the preferred methodology involving a complex decision-making process. Since terror groups have to change their financing approaches based on the circumstances, the groups must focus on efficiency and effectiveness based on the criteria. TF occurs in four main ways, as explained under the opportunity-based[41] and necessity-based theories.[42]

[38] Rudner n(36)
[39] M Fawzy, Muhammad, Iran and Hezbollah: A Very Special Relationship. (2016) 44 Annals of the Faculty of Arts, Ain Shams University, 447-502.
[40] C Dion-Schwarz, B Manheim, and P B Johnston, *Terrorist Use of Cryptocurrencies: Technical and Organisational Barriers and Future Threats (*RAND Corporation, 2019)
[41] See K Hausken and D K Gupta. 'Determining the Ideological Orientation of Terrorist Organisations: The Effects of Government Repression and Organised Crime' (2016) 12 International Journal of Public Policy 1, 75, who defines opportunity-based theory of TF as the political and economic factors that influence the TF activities of a group, such as opportunities to engage in kidnap for ransom, which can only be done when the opportunity presents itself.
[42] *Ibid*

3.3.1 State-Sponsorship

State-sponsored terrorism has significantly reduced over the years, having been common during the Cold War era.[43] The reduction is attributable to the changes in the foreign policies and international relations goals in those nation-states. However, several countries are still involved in state-sponsored terrorism, and the approaches have changed.[44] These include Iran, which is accused of state sponsorship of Hezbollah,[45] and Pakistan, which sponsors the Taliban of Afghanistan. Based on this example, it is apparent that rather than an actual reduction in the involvement of states in sponsoring terrorist groups, state sponsors of terrorism have been less willing to acknowledge their actions. State sponsorship is a preferred source of funds since terror groups can enjoy a multiplicity of forms of support, including financial, material and legitimacy. With most countries operating with obscure military budgets, it is easy for a country to provide the necessary support for a terror group without raising suspicions. The reliability of funds from this approach to the terror groups is high since most state sponsors rely on the groups to further their foreign policy options. This explains why groups like the Taliban and Hezbollah have remained active.[46]

However, state sponsorship comes with strings attached, thus limiting the ability of the terror group to determine its objectives and operations. While, in the past few decades, there has been a notable decrease in the state sponsorship of terrorism, the threat should not be underestimated. As evidenced during the terrorist attacks conducted on October 7 in Israel, Hamas is not a weakened terrorist organisation but one that can conduct sophisticated terrorist attacks at multiple venues.[47]

---

[43] See Freeman n(6) who cites the state sponsorship of Marxist groups supported by Cuba and the Soviet Union. Also see S. Claire, *The Terror Network: The Secret War of International Terrorism* (Holt, Rinehart, and Winston, 1981) and A James, *The Financing of Terror* (New English Library, 1986)

[44] The changes to the approaches and strategies can be attributed to the six-point criteria by Freeman n(6) and the interplay between the choices by the terror groups and the state-sponsors.

[45] Iran finances 50% of the US$200M budget for Hezbollah, which also receives material support from Syria in the form of weapons and safe havens to operate.

[46] On the contrary, the dynamics of international relations and foreign policies also make state-sponsored terrorism an unreliable source of finances in the long-term. Keatinge and Keen refer to the collapse of Libya, which was a state sponsor of terrorism, as part of the reason groups lost significant financing. The collapse of the Soviet Union in the 1990s led to loss of funding and collapse of numerous Marxist groups such as the Contras. See T Keatinge and F Keen, 'Social Media and (Counter) Terrorist Finance: A Fund-Raising and Disruption Tool (2018) Studies in Conflict & Terrorism, 15.

[47] Human Rights Council, 'Detailed findings on attacks carried out on and after 7 October 2023 in Israel' < https://www.ohchr.org/sites/default/files/documents/hrbodies/hrcouncil/sessions-regular/session56/a-hrc-56-crp-3.pdf> accessed 11 July 2024

The Iranian role in the attack was visible. Back in 2010, researchers estimated that Iran is the primary financier of Hamas, as Iran has contributed between 20 and 30 million USD in operation support to Hamas.[48] Such financial assistance reduced the independence of Hamas and made it a proxy of the Iranian regime, and there is also evidence that the Iranian support for Hamas has increased ever since, as current estimates suggest that in 2023 Hamas obtained nearly 100 million USD in direct support from the Islamic republic [49] According to Smyth It is highly likely that Iran was surprised by the sheer operational success of October 7 terrorist attacks; however, there is little doubt that, the assistance it provided to Hamas and other terrorist groups in the region to structure their operations and become more effective armed factions and provision of weaponry had directly enabled the October 7 attacks to succeed.[50] Indeed, according to a report from the Wall Street Journal, Iranian military officials not only helped Hamas in planning the October 7 attacks but also gave a green light to Hamas to conduct it[51] While such reports might have exaggerated the Iranian day-to-day involvement in the Hamas operational planning, Iran is organising an axis of resistance against Israel and is currently recruiting guerrilla fighters to fight in Gaza [52] Further direct financial assistance to Hamas is also expected to guarantee the survival of the organisation during the heightened presence of Israeli army in Gaza. All of this suggests that state sponsorship of terrorism significantly affects the modus operandi of terrorist groups in the Middle East, as a terrorist insurgency in the region is used as a proxy war between the main regional players. Understanding the impact of state sponsorship on the modus operandi of terrorist groups is important for this project as the methods of TF differ significantly on whether the group can rely on support from the state or needs to find resources to support its operations independently of the state. Terrorist organisations, relying on state funding do not necessitate the same level of technological sophistication for their fundraising activities, as financial assistance can be provided

[48] Josef Federman, "Israel: Slain Hamas leader smuggled Iranian arms' < https://www.newsday.com/news/world/israel-slain-hamas-leader-smuggled-iranian-arms-c04868> Accessed 11 July 2024.

[49] Angus Berwick and Ian Talley, "Hamas Needed a New Way to Get Money From Iran. It Turned to Crypto," (*Wall Street Journal* 2023) < https://www.wsj.com/world/middle-east/hamas-needed-a-new-way-to-get-money-from-iran-it-turned-to-crypto-739619aa> accessed 11 July 2024

[50] Phillip Smyth, "The Path to October 7: How Iran Built Up and Managed a Palestinian 'Axis of Resistance' Financial Action Task Force-Style Regional Body" <https://ctc.westpoint.edu/the-path-to-october-7-how-iran-built-up-and-managed-a-palestinian-axis-of-resistance/> accessed 11th July 2024

[51] Summer Said, "Iran Helped Plot Attack on Israel Over Several Weeks" (*The Wall Street Journal*, 2023) < https://www.wsj.com/world/middle-east/iran-israel-hamas-strike-planning-bbe07b25 > accessed 11th July 2024

[52] Giorgio Cafiero, "Iran's Stakes in the Hamas-Israel Conflict" <https://carnegieendowment.org/sada/2023/10/irans-stakes-in-the-hamas-israel-conflict?lang=en> accessed 11th July 2024

in cash, often through established and functional networks.[53] Terrorist organisations sponsored by the states, however, have attempted to diversify their sources of funding as the state assistance can come with conditionality that the group does not want to adhere to.[54] Understanding the legislative responses that the government of Bahrain has undertaken in the past few years to update its legislation against TF must also appraise that Bahrain has to deal with hostile actors that have access to state funding and come up with a progressive agenda for countering the alternative channels through which terrorist organisation can access new resources.

3.3.2 Illegal Activities

The multiplicity of illegal activities[55] that a terror group can rely on to fund its operations makes this option highly lucrative. Terrorist groups have relied on illegal activities with their options determined by their characteristics, with the earliest instance of terrorists relying on crime to finance their activities reported in the 1980s.[56] The crime-terror nexus is often viewed as being necessitated by the reduction in the state-sponsorship of terrorism, especially following the end of the Cold War. This occurs in two ways.[57] Territory-controlling groups have found it lucrative to impose revolutionary taxes on people living in the areas where they control.[58] Control over territories enables terror groups to employ a multiplicity of strategies, including the threat of violence for failure to support the groups.[59] Illegal activities offer lucrative sources of funds for terrorists, thus making it possible to raise large quantities of money. Kidnapping for ransom[60] has been lucrative, especially in locations where terrorists target foreigners and wealthy individuals.

---

[53] M Jacobson and M Levitt *Combating the Financing of Transnational Threats* (Emirates Center for Strategic Studies and Research 2009)
[54] *Ibid*.
[55] Commonly referred to as the terror-crime nexus TF activities, they include revolutionary taxes, extortion, petty crime, counterfeiting of goods, pirating, smuggling, theft, smuggling and trafficking and kidnap for ransom.
[56] Roth and Sever n(14)
[57] The Crime-Terror nexus can either occur through the terrorist group getting involved in criminal activities, or when terror groups work together with criminal groups for the purpose of achieving particular goals.
[58] Since they establish a form of a pseudo-government, such groups can control trade and all operations, thus giving them a multiplicity of options in raising funds.
[59] The support can be in the form of value-creating activities, whereby institutions and individuals are forced to provide labour and services to the group. For instance, Claire indicates that the PLO collected at least US$10M from airlines in the Middle East, as well as up to US$220 from oil-exporting companies in the 1970s. In other instances, the support can be in the form of cash, which is collected over and above the illegal activities. For instance, Freeman, 7 indicates that in Ireland, the Protestant Loyalists extorted fees in the pretense of protection from businesses and advised them to claim tax deductions on those expenses. See Claire (n) 43.
[60] The Abu Sayaff Group from Philippines and Boko Haram from West Africa which are notorious for kidnapping target wealthy members of society, or foreigners, including tourists or NGOs workers, whereby the ransom paid

Terrorist groups have also shown an increasing propensity to engage in theft to finance their operations. By targeting the repositories of these valuables, such as museums and banks, terror groups rely on their willingness to use violence to acquire finances in this approach.[61] Similarly, smuggling and trafficking,[62] with most terrorist groups involved in one form of trafficking or another.[63] These criminal activities are preferred since they are repeatable and can be scaled up and down depending on the circumstances.[64] Illegal activities also enable terror groups to compromise the governance of the current government by undermining the legitimacy of the government.[65] However, illegal activities are a TF activity of the last choice since they present increased chances of exposure to both law enforcement and security agencies.[66] These activities include the following:

- Infiltrating the supply and value chains[67]
- Exploiting production and distribution chains in failed states
- Kidnap for ransom, among others.

Terrorist organisations are using a wide array of sources to finance their activities, and an effective response to counter-terrorism financing should take into account the dispersed nature of the problem. The legislative responses to terrorism must take into consideration the proliferation of

---

ends up financing terrorists' activities. see P Lewis, *Guerrillas and Generals: The "Dirty War" in Argentina'* (Praeger,2001) at 58..

[61] Freeman, n(4) p 8 cites the theft of US$600M dollars in 1976 by PLO from banks in the Middle East, the widespread theft and destruction of property by ISIS militants as part of a strategy to finance their operations. See FATF *Financing of the terrorist organisation Islamic State in Iraq and the Levant (ISIL)* (FATF 2015).

[62] Terrorist groups traffic in a multiplicity of goods, including the movement of people from one location to the other. A Grynkewich, "Welfare as Warfare: How Violent Non-State Groups Use Social Services to Attack the State" (2008),31, Studies in Conflict and Terrorism, 350, who indicates that the Taliban made a yearly profit of nearly US$400M from trafficking opium.

[63] Hezbollah trafficked in Cigarettes from North Carolina, while the IRA smuggled pigs across the Irish border, thereby making over US2M per year. Other groups like that control territories provide security for the traffickers and smugglers who pass through their territories.

[64] Similarly, terror groups can penetrate a criminal entity for the purpose of raising funds, as and when needed, thereby rely on the infrastructure of the criminal group, rather than starting upfront. However, Freeman, 10 cautions that this strategy can expose the terror group to liabilities.

[65] See H Shpayer-Makov, n(2)

[66] It has been suggested that by engaging in petty crimes, terror groups expose themselves to criminal liability. As a result, terror groups can only utilize illegal activities if those activities have not yet been criminalized or sanctioned, such as locations with poor law enforcement standards or in failed states. See H Carrapico, D Irrera and B Tupman, 'Transnational organised crime and terrorism: different peas, same pod?' (2014) 15 Global Crime, 4, 213,

[67] See F Lemieux and F Prates, 'Entrepreneurial terrorism: financial strategies, business opportunities, and ethical issues'. (2011) 12 Police Practice and Research, 378, who indicates that a Hezbollah terror cell used the differences in the cigarette taxes in North Carolina and New York and New Jersey to make over US$4M in profits, which was the substance of *United States v. Hammoud, 483* F. App'x 865 (4th Cir. 2012)

sources of terrorist financing and account that cryptoassets have become one of the key new means through which terrorist organisations could solicit external funding. As this project will examine the UK and the Bahraini approach to the regulation of cryptoassets, the research would be able to address a pertinent question, namely, are the states well equipped to deal with the challenges the technological sophistication has presented them with or the terrorist organisations are gaining the upper hand by becoming more creative in embedding technologies in their methods for terrorist financing.

3.3.3 Legal Activities

As explained by the intersection between the needs-based and opportunity-based theories,[68] TF can be achieved through supplementing or complementing the other TF activities. Legal businesses created for-profits are preferred by terrorist groups since they can be operated without interference by law enforcement agencies.[69] Legal businesses offer terrorist groups a cloak to mask their financing activities[70] while enabling the group to generate revenues from activities that are highly marketable and valuable within the locations where they operate.[71] The preference for legal businesses enables terror groups to operate without detection by law enforcement and security forces while enjoying the benefits of legality, such as protection by the state. When necessary, the terror groups rely on strawmen, who carry out the business on behalf of the terror group, but with a cloak of legality to mask their true objectives.

Certain legal businesses, such as money transfer, courier services and transport services, are preferred since they enable the terror groups to hide their TF activities more effectively. For instance, by penetrating the *hawala* system of money transfer, Al Shabaab has been able to

[68] See Freeman, n(4) 9, who indicates that the Provisional IRA has often shunned dealing in drug trade in N. Ireland, since they view the trade as being damaging to the end consumers and the economy. Furthermore, due to the profitability of the trade, they are aware that involved in the trade will result to corruption and competition for the immense resources from the trade, which can drive the members to deviate from the objectives of the groups. On the contrary, M Levitt, 'Going to the Source: Why Al Qaeda's Financial Network Is Likely to Withstand the Current War on Terrorist Financing' (2004) 27, Studies in Conflict and Terrorism, 3, 169, who states that Islamic Jihad groups have shown increasing willingness to engage in activities that are considered immoral, if the purpose is to achieve the objectives of the group.

[69] According to J Burke, *Al-Qaeda: The True Story of Radical Islam* (I.B. Tauris, 2003) 145, Al Qaeda operated numerous legal businesses in Sudan between 1992 and 1996. See also Freeman n(4) 10, who indicates that the IRA, Hezbollah and Hamas has engaged in legal businesses in their various jurisdictions.

[70] Commonly known as front companies, these entities are established to enable terrorist groups or criminals to engage in ML, or to create an infrastructure through which planning, and implementation of terror activities can be conducted.

[71] Legal businesses are profitable since most individuals within communities consume the products and services from those businesses. See Lemieux and Prates n(67), 368.

generate finance from the charges and channel donations masked as money transfers to legitimate individuals.[72] However, it is challenging to divert the funds to terror activities since most processes associated with remaining legal reveal such activities.[73] Legal businesses also require industry-specific knowledge and management skills and are subject to fluctuations in the lifecycle phases. To avoid some of the challenges associated with legal businesses, terror groups preferred charities. Due to the simplicity of establishing and running charities, terror groups preferred this form of institution due to the limited oversight by government institutions and the fact that their operational requirements were less stringent.[74] Furthermore, charities rely on donations, which are subjected to the same rigour as the revenues from business operations.[75] The most widely used legal businesses include the following:

- Charities
- Stock exchanges
- Essential services

These legal avenues to TF represent the increased ability of terror groups to structurally transform their financing activities and take advantage of opportunities to generate revenues from globalised trade.[76] Most researchers indicate that terror groups utilise both licit and illicit activities to finance their activities, as and when required, since most groups have found it possible to utilise these two sources of finance with ease.[77] There is, however, a disparity in the theorisation of the dynamics of the crime-terror nexus. On the one hand, based on the logic of realism, both criminal entities and terror groups interact in a rational and commensurate manner to achieve their rational

[72] Ibid, 378.
[73] See ibid, 2, who indicates that the oversight placed upon legal businesses limits the ability of terrorist groups to operate in a clandestine manner. However, Roth and Sever indicated that due to the disparities in the oversight over businesses in different regions, it is common for terrorist groups to find ways of operating legally within their jurisdiction, even if such activities might be considered suspicious elsewhere. Roth and Sever n(14) at 59.
[74] As early as 2002, FATF indicated that Al Qaeda relied on donations, which were essentially funds originally aimed to finance terror that were donated to registered charities as their primary source of funds. Since the source and destination of donations are rarely monitored, terror groups have found this approach highly lucrative. FATF, *Global Money Laundering &Terrorist Financing Threat Assessment* (FATF, 2010).
[75] See A Acharya, *Targeting terrorist Financing: International cooperation and new regimes,* (Routledge, 2009), who indicates that donations to charities from all members of society, including wealthy donors is a common practice among Muslims, and it is done for the purpose of helping the poor, and to support the spread of Islam.
[76] T Clancy, "Theory of an Emerging-State Actor: The Islamic State of Iraq and Syria (ISIS) Case " (2018) 6 Systems 16, who indicates that ISIS made billions annually from trading in oil, gems and art, sometimes with parties who were not aware that they were dealing with a terrorist group.
[77] J T Picarelli, 'The Turbulent Nexus of Transnational Organised Crime and Terrorism: A Theory of Malevolent International Relations', (2006) 7 Global Crime, 1, 1.

goals. However, from past evidence, the irrational nature of the two actors leads to infighting, with the challenge of public goods coordination.[78]

The proceeds of crime continue to be part and parcel of the terrorist economy. Terrorist groups have found innovative ways to utilise drug trafficking,[79] racketeering, kidnapping for ransom, human trafficking, illegal trade in precious items and antiques, arms trafficking and theft to finance their activities. Certain terror groups have specialised in particular criminal activities[80] , and Terrorist organisations have relied on criminal activities such as drug trafficking. Understanding how legal activities are used to support terrorism financing is central to the answer to the first research question of this study, which aims to explore the responses of the state to terrorism financing, which must include not only the criminalisation of illegal activities but also a closer regulation of legal activities that can be used to conceal proceeds of crime.

3.4 The 'New Model' Terrorism

The 9/11 attack [81] laid the foundation for the ability of terror groups to draw members from different nation-states[82] for a single purpose. The network model utilised by Al-Qaida involved separate cells that operate at arm's length from the central organisation, with the ability to coordinate and support one another for one or more terror attacks. This form of organisation makes it challenging to detect and track the activities of either the cells or the central organisation since they can morph into society. This 'new model' of terrorism is characterised by the intersection between the extant literature on TF and the emergent literature and knowledge on terrorist innovation. One challenge with this field of study is the propensity of the literature to be more

[78] See R Bossong, *Public good theory and the 'added value' of the EU's counterterrorism policy*. (Economics of Security Working Paper 42 2011), who indicates that the crime-terror nexus is complicated by the lack of enforcement mechanisms, since either party can withdraw from the relationship without any consequences,

[79] Common referred to as Narco-terrorist groups, these include Taliban, Hamas, FARC

[80] E Price, 'Literature on the Financing of Terrorism' (2013) 7 Perspectives on Terrorism. 4: 115, who indicates that in some cases, the terrorist groups partner with or take over the criminal entities, since the criminal group has no recourse but to capitulate.

[81] H Tofangsaz, 'Rethinking terrorist financing; where does all this lead'. (2015) 18. J of ML Ctrl, 1, 112, who indicated that the attack, which cost US$500,000 to implement, led to US$40B in direct costs, and trillions of dollars in response under the war on terror.

[82] F Schneider and R Caruso, 'The (Hidden) Financial Flows of Terrorist and Transnational Crime Organisations: A Literature Review and Some Preliminary Empirical Results' (2011) https://www.econstor.eu/bitstream/10419/119378/1/diw_econsec0052.pdf accessed 29 January 2021, who indicates that the 9/11 attacks were directly implemented by 26 co-conspirators from seven countries.

descriptive while primarily focusing on taxonomising and categorising the existing funding methods and the trajectory of innovation.

Furthermore, groups like AQ and ISIS have a more gradualist strategy, which enables them to utilise a completely different TF approach.[83] The gradualist approach lays down the foundation for present and future TF activities since they have convinced Muslims and other individuals that it is necessary to join in and support the movement by taking up arms and providing financial support to emancipate themselves.[84]

3.4.1 Structure

'New Style' terror groups have shown an increasing preference for horizontal structures with higher parity in the power and influence of the different cells. Unlike the hierarchical structures used by Al Qaida,[85] the horizontal structures amplify the input of each group. As observed under ISIL, the creation of horizontal structures arises from open-ended affiliations, including Al-Shabab, Boko Haram, and the multiplicity of offshoot lone ranger attackers who profess alliance to the group.[86]

New model terror groups rely on a combination of domestic and international ties, which go beyond what past terror groups used.[87] In addition to outsourcing manpower[88] and acquiring artificial notoriety,[89] the groups can attract sympathisers who offer value-creation capabilities to facilitate the planning and execution of attacks. The measures can be traced to the strategies of the IRA, which drew part of its finances from donations by Irish countrymen in the US.[90] Rather than

[83] The gradualist strategy by Al Qaeda and ISIS, whereby they popularized their ideology of Jihad for agitational purposes, while achieving enforcement objectives that is common among established political systems.
[84] Keatinge and Keen n (46)
[85] P Neumann, *Old and New Style Terrorism*, (1st Edn, Polity Press 2009) uses the example of Al-Qaida, where decision making was centralised under Osama Bin Laden, who organised the activities of the group around his vision.
[86] This form of evolution results to increased fluidity in the identification of targets, communication, and most importantly, the approaches to financing of attacks.
[87] See Schneider and Caruso n (82)
[88] B M Jenkins, *The New Age of Terrorism* (Rand Corporation 2006) indicated that large terrorist organisations have shown increasing ability to institutionalise their operations, including the decentralisation of certain functions, such as recruitment, training, intelligence, reconnaissance, planning, logistics, finance, propaganda, and social service. These functional specialisation leads to hierarchies and bureaucratic tendencies, which have implications on the management of finances.
[89] Emergent terror groups affiliate with the most prominent terror entity, with most of the groups that aligned with AQ having moved towards associated with ISIS.
[90] See Tofangsaz, n(81)

relying on financial support, modern-day terrorists draw upon the support of a broader range of individuals within society, some of whom assist unknowingly.

New model terrorism is also designed to defeat a multiplicity of the AML/CTF measures put in place. One of the primary objectives is to identify weak links in the measures put in place within the legal and policy frameworks.[91] Groups like Al Shabaab and ISIS[92] were effective in defeating the existing procedures and governance within a country to establish themselves as the authority in the region. ISIS utilised a highly intricate institutionalised governance infrastructure through which the generation, storage, movement and use of finances resembled a nation-state.[93]

3.4.2 Novel targets

Second, the groups have a new target.[94] Unlike past terror groups, new model terrorists target 'soft targets', including civilians, based on the premise that civilians support the political systems, which is the basis of the dissident status of those terror groups. Since they have a global outlook, the soft targets are individuals and socio-cultural systems which exist in locations that the terrorists view as enemies. This differs sharply from contemporary terrorist violence, which was historically directed towards targets with optimal symbolic value to society. The selective approach through which adversaries are identified and targeted by terrorists bore semblance to an apparent moral code, which focused on the minimal loss of the lives of non-combatants.[95] These decisions were based on the fact that terror groups relied heavily on the support of the general public, and this indiscriminate carnage was antithetical to such an outcome. However, under the new model, terror groups rely on a different and highly dynamic moral code, signified by asymmetrical warfare, both domestically and internationally.[96] The new model of terrorism, which

[91] For instance, the lack of uniformity in the adoption and implementation of the propositions under FATF and other regional and international legal frameworks makes it easy for terror

[92] See Clancy, n(76) who describes ISIS as an emerging state actor, whereby a number of conditions have to be made, including control over territory, presence of valuable resources in the territory, ability to coerce the population to support the group, exploit local grievances, and attract foreign fighters.

[93] Documents found in ISIS compounds revealed intricate records regarding its financial and military operations, with blueprints from the future of the terror groups, featuring civil service structures, taxation models, regional government institutions and a monitoring system for control and oversight.

[94] By targeting new targets, which are more diverse.See Schneider and Caruso n(82)

[95] M M Nia, 'From old to new terrorism: The changing nature of international security'. (2010) 18 Global Studies Journal, who reports that even when terrorist used high-yield weapons against indiscriminate targets, their primary objective was to avoid mass civilian casualties.

[96] L K Donohue, 'Anti-Terrorist Finance in the United Kingdom and United States' (2006) 27 MICH.J. INT'LL. 2, 303, attributed the use of asymmetrical warfare to the need to disrupt the traditional and new security measures,

prioritises an indiscriminate targeting of civilians, has also led to a paradigm shift in terrorism financing. While previously terrorists could rely on like-minder civilians to support their operations, the mass civilian casualties contemporary terrorist attacks have produced have made it more difficult for terrorist organisations to find like-minded supporters among the general population. However, it has not led to the demise of terrorism; instead, the technological revolution has made it incredibly easy to radicalise an individual at the other end of the globe, as the experience of Andres Breivik has demonstrated.[97] As more and more terrorist attacks were perpetrated by lone wolves who operate independently and finance their activities independently from the terrorist organisations, their methods for TF have relied on technological solutions to obtain funds remotely.[98] This research is going to examine how terrorist groups have adapted to the new models of terrorism by considering not only the changes in their modus operandi but also the new methodologies that are being used for finding new sources of funding.

The novel targets under the new model of terrorism rely on the creation of fault lines through discriminative targeting. Following in the line of Al-Qaida, most Islamic terrorist groups have embedded religion as the primary motivator for their actions. Within this terrorist environment, the activities are loosely modelled around Islam as a religion to boost the success and acceptability of their agenda.[99] In addition to obtaining extensive publicity from their actions, the terror groups seek to deter challenges to their legitimacy since they can shift back and forth from the religious standpoint to the extent that it fits their objectives.[100] The primary outcome of the new target selection strategies is the emergence of novel political fault lines arising from the social, cultural, governance and economic norms. By antagonising elements of the social fabric, the new terror groups have created a highly volatile and partisan climate where each decision, action and reaction results in an escalation of the confrontation.[101] The shift to targeting "soft targets" by modern terrorist groups has significant implications for terrorism financing. Firstly, the reliance on a dynamic moral code and asymmetrical warfare means that terrorist groups can adapt their funding strategies, making it harder for authorities to track and intercept financial flows. Secondly, the use of religion as a primary motivator complicates efforts to combat terrorism financing, as it requires a nuanced approach that addresses both ideological and financial aspects. Lastly, the creation of

[97] J Kenyon, C Baker-Beall, and J Binder, ';Lone-actor terrorism–a systematic literature review.' (2023) 46 Studies in Conflict & Terrorism 2038-2065.
[98] M Tierney, 'Spotting the lone actor: combating lone wolf terrorism through financial investigations.' (2017) 24 Journal of Financial Crime 637-642.
[99] See Nia, n(95)
[100] G Martin, *Understanding terrorism: Challenges, perspectives, and issues.* (Sage Publications, 2016), 3.
[101] Donohue, n(96), 307.

political fault lines through selective targeting can lead to increased funding from sympathisers who support the group's socio-political agenda, further complicating efforts to disrupt these financial networks. This project will examine how the Bahraini and UK governments have responded to the sophistication of terrorism financing approaches and whether their regulatory frameworks have financial intelligence capabilities that have been effective in combatting the use of illicit channels such as money laundering, cryptocurrencies, and cross-border transactions.

3.4.3 Diverse Objectives

Third, the terror groups have unique ends and objectives, over and above the use of violence to cause loss of life and disrupt economic activities. Religious fundamentalists have sought to impose their ideological norms on their subjects. ISIL,[102] According to FATF,

> "ISIL's operations are distinct from those of most other terrorist organisations...Unlike some AQ[al-Qaeda] associated organisations, most of ISIL's funding is not currently derived from external donations but is generated within the territory in Iraq and Syria where it currently operates."[103]

Evidence of the transformation exists in the fact that rather than adopt the hybrid approach, these groups are committed to using violence to create a new world order.[104] Unlike the hybrid terror groups, which seek to engage in TF activities while maintaining political goodwill within the established political systems,[105] the new model terrorists[106] focus on goals that are so radical that there is a need for the overhaul of the entire system.[107]

Despite the multiplicity of objectives targeted by these groups, they tend to embed their objectives to the defeat of Western civilisation by unleashing a global jihad. The narrative established by these terror groups, with justifications from the religious teachings under Islam, offers a broad

---

[102] Whose objective was to create an Islamic caliphate, sought to change the social, cultural, economic and political systems into the caliphate-style governance.
[103] FATF, "Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)" (FATF/OECD, 2015).< http://www.fatf- gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organisation-ISIL.pdf.>Accessed on 29 January 2021
[104] K Petrich, 'Cows, Charcoal, and Cocaine: Al-Shabaab's Criminal Activities in the Horn of Africa', (2022). 22 Studies in Conflict & Terrorism,
[105] Although they use violence, Hezbollah and the IRA have ended up conforming to the existing political systems.
[106] Boko Haram of West Africa, ISIS in Syria, and Al-Shabaab in the Horn of Africa have all shown increased willingness and propensity to destroy social structures and systems, even target Muslims, even though they identify as terror groups with affiliation to Islam as a religion.
[107] Roth and Sever, n (14), 59..

range of individuals and institutions the reasons to provide support to the terror groups, thus establishing a highly intricate network of supporters willing to provide finance and other forms of value-creating goods and services.[108] Technology plays an important role in the global jihad by providing terrorist groups with a global outreach that they could not enjoy before the advent of the digital age. [109] As Saltman acknowledges, nothing binds a community together as much as the two-way communication that the new technologies provide, as the Internet has offered a means for terrorist groups to influence public opinion even if their military capacities are low.[110] "Indeed, the Internet has come to serve as a choice means of communications outreach on the part of al-Qaeda and its regional affiliates, for its pronounced, digitalised multiplier effects on jihadist consciousness-raising, recruitment, training, fund-raising, and operational activities".[111]

3.5 TF Under the 'New Model' Terrorism

Existing literature points towards the existence of causation and correlation between the implementation of AML/CTF strategies and the innovativeness of terrorist groups in engaging in ML/TF activities. However, there are contradictions in the views of whether the interventions by the various jurisdictions stimulate the changes in ML/TF activities or whether the AML/CTF strategies are in response to the innovations by terrorist groups. The historical review focusing on the four waves of terrorism offers limited disambiguation of the relationship between the two phenomena. A review of the objectives and principles of FATF and FSRBs(Financial Action Task

[108] Petrich n(104), 10 who indicates that TF has been reinvented under the 'New Model' terrorism, whereby different parties contribute in different ways, with the terror groups and the ideology of terrorism being utilized to create a symbiotic relationship that benefits the terror groups, the attackers, the individuals involved in facilitating the terror groups, as well as other auxiliary beneficiaries.
[109] S Saltman, 'The Global Jihad Network: Why and How Al-Qaeda Uses Computer Technology to Wage Jihad.' (2008) 1 Journal of Global Change and Governance, 2-10.
[110] *Ibid.*
[111] Martin Rudner, '"Electronic Jihad": The Internet as al-Qaeda's Catalyst for Global Terror' (2016) 29 Studies in Conflict & Terrorism 1.

Force-Style Regional Body)[112] reveals that the most tenable explanation for the innovations can be attributed to the interventions within the jurisdictions.[113]

In this review, the analysis will reveal the extent to which TF under 'New Model' terrorism resembles the activities under the previous waves of terrorism, including the high degree of responsiveness to incentives. Theories on terrorism in general, which can be applied to the aspect of TF, predict that moderate terror groups tend to turn more radical following a government crackdown.[114] Similarly, changes in the ideology of a terrorist group lead to splitting into factions, and this can affect the choices and capabilities of TF.

3.5.1 Diversified Criteria for Choosing the Financing Portfolio

Terror groups require money to finance their operations.[115] With the possibility of one financing source facilitating the success of another, terrorist groups have found it necessary to rely on more than one of the generic financing approaches. The choice of the portfolio of financing approaches is based on six factors, as shown hereunder. Quantity: since terror groups can do more damage with more finances, they prefer financing approaches that deliver the largest quantities of money. Security, due to the clandestine nature of terrorist operations, is critical as the potential for hiding the financing activities from the CTF institutions is integral in obscuring how the terror groups are organised and how they plan, recruit, and train their members. Secure financing approaches help terrorists steer clear of the radar of the security forces by warding off unwanted attention and raising no suspicion. Simplicity is essential for efficiency, as terrorist groups rely on

[112] The FATF-style Regional Bodies include the following Asia/Pacific Group on combating money laundering (APG), Caribbean Financial Action Task Force (CFATF), Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism of the Council of Europe (MONEYVAL), Eurasian Group (EAG), Eastern and South African Anti Money Laundering Group (ESAAMLG), Financial Action Task Force on Latin America (GAFILAT), Inter-Governmental Action Group against Money Laundering in West Africa (GIABA), Middle East & North Africa Financial Action Task Force (MENAFATF) and Task Force on Money Laundering in Central Africa (GABAC)

[113] FATF 'High-Level Principles for the relationship between the FATF and the FATF-style regional bodies, updated February 2019'(FATF 2019), which identifies the objectives, including setting of standards, technical assistance, promoting autonomy, sharing similar objectives and operating in partnerships, reciprocating the actions of one another, and establishing common interests in order to promote the FATF ideology.

[114] See P Rosendorff and T Sandler, 'Too Much of a Good Thing? The Proactive Response Dilemma (2004) 48 Journal of Conflict Resolution, 657 and R De Figueirdo, and B. Weingast, 'Vicious Cycles: Endogenous Political Extremism and Political Violence' (2001) Institute of Governmental Studies Working Paper, 2001-9.

[115] M Freeman, 'The Sources of Terrorist Financing: Theory and Typology (2011) 34 Studies in Conflict & Terrorism, 461 indicates that whereas most studies only focus on the finances that end up being used to fund attacks, terrorist groups require much more for administrative costs as an institution.

simple financing methodologies where the skills and efforts required are limited.[116] The reduction in the inherent cost of financing is key to control and reliability. Control, the nexus between power/influence and money, is integral in the choice of financing approaches.[117] Normally, terror groups select a financing approach that leads to the retention of power in their leadership to avoid unwanted influence. External sponsorships, which have preconditions, may limit the options of the terror groups, while financing approaches reliant on individuals other than the heads of the groups may lead to a shift in the balance of power within the group. Reliability ensures a consistent and predictable stream of revenues for various operations.[118] For instance, financing through the drug trade is dependent on there being a reliable group of users and producers of the drugs, while taxation is dependent on efficiency in operating businesses in the location. Legitimacy results in more support from the parties involved in the financing activities.[119] Legitimacy is affected by the use of financing approaches that are antithetical to the social, cultural, religious, or political views of the supporters of the terror groups. Legitimacy is also adversely affected by the wrong use of the funds, such as for personal enrichment, corruption, or inequality in the distribution of the finances within the group.[120]

3.5.2 The Establishment of Terrorism Financing Systems

Understanding TF under the 'New Model' terrorism, it is imperative to appreciate the changes in the terrorist financing systems based on how they are created and how they have changed. The multiplicity of measures under the AML/CTF strategies makes it challenging for terrorist groups to rely on one financing approach.[121] The establishment of financing systems enables the terror group to establish causal links between their every action and the ability to raise, move and store funds. One key strategy is exemplified in the utilisation of transnational terror attacks for laying down the foundation for TF, as exemplified by one key similarity between some

[116] This explains why terrorist groups prefer raising funds through crimes such as theft and kidnap for ransom, rather than the multi-actor and multi-stage financing operations such as drug trade.
[117] See Roth and Sever, n(14), 914
[118] M Freeman, 'The Sources of Terrorist Financing: Theory and Typology' (2011) 34 Studies in Conflict & Terrorism, 6, 464
[119] P Williams, "Terrorist Financing and Organized Crime: Nexus, Appropriation, or Transformation?" in Thomas Biersteker and Sue Eckert (eds) *Countering the Financing of Terrorism* (New York: Routledge, 2008).
[120] Azani, n(33)
[121] K Laura, and L K Donohue, 'Anti-Terrorist Finance in the United Kingdom and United States' (2006), 27 MICH.J. INT'LL. 2, 303 who indicates that terror groups rely on various sources of funds, store their resources in various locations and ways, and move the funds in different ways. By so doing, in case, there is exposure of one financing strategy, the rest of the activities are protected.

of the most brazen attacks, such as the 9/11 attacks in the US in 2001, the London Bombings of 2005, Mumbai attacks in 2008, and more recently the Westgate attacks in 2013 in Nairobi, the October 7 attacks in Israel and the Moscow Concert Hall attack on 9 April 2024 is the application of a simple yet effective approach to planning and implementing attacks:

- Select a target in a functioning and healthy democracy.[122]
- Select a location that is known globally.[123]
- Plan the attack in a manner that leads to maximum damage within the shortest time possible.[124]

The combined effect of these outcomes is the increased ability to defeat the existing AML/CTF strategies in place. The approach also enables the terror groups to sow chaos within societies in a manner that only the terror groups can benefit from, primarily through territory control. These groups establish political and administrative control of large areas over extended durations by excluding other entities, such as democratically elected governments, as well as competing terrorist groups. Control over these territories provides access to a multiplicity of resources that assure the survival of the terror group, with the primary sources of finance being the natural and human resources within the area. The control also leads to a high degree of self-sufficiency while creating a haven that limits the need for reliance on external assistance. However, different groups utilise territory control for TF purposes in different ways. For instance, at the peak of its territorial control, ISIS earned between US$1 billion and $2 billion through a highly efficient taxation system[125] designed to complement and supplement its revenues from trading in oil and other resources available in the region under the caliphate. Al-Shabaab, which is loosely affiliated with Al-Qaeda and ISIS, operate a quasi-government in Somalia.[126]

---

[122] F Schneider, 'The (Hidden) Financial Flows of Terrorist and Organized Crime Organisations: A Literature Review and Some Preliminary Empirical Results' (2010) < https://core.ac.uk/download/pdf/6482945.pdf> accessed 21 February 2021 which ensures the presence of a free and effective press, meaning that the news of the event will be spread beyond the national borders.

[123] Ibid, 5.

[124] C E Humud, R Pirog, and L Rosen, '*Islamic State Financing and U.S. Policy Approaches'* (Congressional Research Service 2015).

[125] See V Salama, "As Territory Shrinks, ISIS Looks for New Money Sources," (*Seattle Times*,2016) <https://www.seattletimes.com/nation-world/as-territory-shrinks-is-group-looks-for-new-money-sources/> accessed 14 February 2022 who reports that ISIS collected over US4M per month in taxes?

[126] T Keatinge, 'The Role of Finance in Defeating Al-Shabaab. Whitehall Report, 2-14' (*RUSI*, 2014)https://rusi.org/sites/default/files/201412_whr_2-14_keatinge_web_0.pdf accessed on January 29, 2021.who indicates that Al Shabaab has shown exceeding abilities to exploit the chaos it has created in the country.

The design of the 'New Model' terrorism, specifically Islamist terrorism, blends cynical calculations and skewed promises of heroism under Jihad.[127] The group benefits from the destruction caused by the terror attacks, thereby getting value for money from their activities, while the highly motivated attackers participate in terrorism for goals not related to financial gain. In this new framework, the payoff from participation in the terrorist attacks is a key consideration, thereby highlighting the extent to which terror groups rely on financial and economic analysis in their decision-making.[128]

Under the new model, the establishment of horizontal networks has led to the increased ability of individuals and offshoot groups, which are essentially not willing to participate directly in attacks, to engage in fundraising for the group.[129] This is because they support the cause but are not willing to participate actively in the terrorists' activities [130] These mutually beneficial relationships are integral to the financing of groups such as ISIS and Al-Shabaab. In the case of Al-Shabaab, by facilitating the activities of pirates in the Indian Ocean, the group was able to raise funds that were redirected to other TF activities.[131]

TF under the 'New Model', and in some of the past, terrorist typologies occur at operational and strategic levels.[132] Operational levels, which entail short-term financing approaches, are utilised within the 'means justify the ends' scenario.[133] The task-oriented approach results in soft-financing outcomes. At the strategic level,[134] TF is done with long-term objectives and perspectives in mind.

[127] The formation of the ideology of this form of terrorism occurs in the minds of a few analysers, which is them strategies for attacks planned by zealous individuals with extensive training in military strategies, and then implemented by terrorists who are radicalised by the masterminds.
[128] Lemieux and Prates above, n (67), 370.
[129] I Levy and A Yusuf, 'How Do Terrorist Organisations Make Money? Terrorist Funding and Innovation in the Case of al-Shabaab' (2021) 44 Studies in Conflict & Terrorism, 1–23.
[130] Shaw n(37)
[131] UN 'Report of the Monitoring Group on Somalia and Eritrea 2012: Somalia', (2013), which further indicates that Al-Shabaab involved itself in a multiplicity of supply and value chains in the region.
[132] Lemieux and Prates, n(67)
[133] These approaches require limited sophistication, involving low profile activities that are not detectable. A contrary view is provided by Azani, n (33), 900.
[134] Strategic financing activities are designed to support the going-concern activities that terrorist groups engage in, including training, recruitment, provision of social services and other amenities that New Model terror groups maintain to acquire and retain power within the locations where they operate. In contrast, see Lemieux and Prates above n (67), 375.

Finally, these terrorist financing systems focus on the cost-effectiveness of their activities. Through the use of their finances to create different forms of value within the organisation, these groups have managed to cut down the costs of attacks while retaining the impact of those attacks for the intended purposes. Cost-effectiveness makes low-value transactions a very viable strategy in TF activities, even though this approach is normally employed for ML.[135] Furthermore, as experienced during the 9/11 attacks, the adoption of cost-effective approaches to terrorism, as well as the strategies involving low-value transactions in TF, limits the viability of SARs.[136]

3.5.3 Reliance on both Domestic and Foreign Sources

The criteria for choosing a funding source, as provided by Freeman,[137] reveals why most terror groups target multiple funding sources. Although there are preferred approaches, terrorist groups under the 'New Model' of terrorism, on account of their institutionalised operational strategies, understand the fact that any amount of support is integral to achieving the various goals.[138] The diversification of TF activities is unique depending on the terrorist group. For AQ, the financial network established by Osama bin Laden was based on the model created by the US to finance the Mujahedeen during the Afghanistan-Soviet war.[139] In the case of Al Shabaab, the focus on foreign sources of finance is based on the fact that the remittances from the diaspora, which are estimated at US$1.2B, provide a more lucrative source of funds as compared to other potential sources such as international trade (US$516M), foreign direct investment, (US$101M), international aid (US$800M). Despite the diminishing attractiveness of state sponsorship as a

[135] Law Commission, *Anti-Money Laundering: the SARS Regime Consultation Paper* (2018) which argues that low-value transactions tend to fly under the radar of the established AML/CTF measures. Furthermore, due to the cost of complying with AML/CTF measures by regulatory institutions, financial and non-financial institution are often incapable of monitoring all transactions

[136] The SAR regime is only effective for large transactions, otherwise it is impossible to monitor and investigate millions of transactions effectively. N Ryder, "A false sense of security? An analysis of legislative approaches towards the prevention of terrorist finance in the United States and the United Kingdom." [2007] Journal of Business Law, p 849 gave the example of the fact that one of the suicide bombers was mentioned in an SAR but was only noticed after the event.

[137] Freeman n(4) p 23.

[138] For instance, whereas Al Shabaab appreciates the fact that foreign cash flows are unreliable, inconsistent and precarious, they have maintained a considerable strategic operation for attracting this form of financing, while also focusing on the more consistent domestic financing sources.

[139] J Waszak, The Obstacles to Suppressing Radical Islamic Terrorist Financing, (2004) 36 Case W. Res. J. Int'l L.673, who indicates that Al Qaeda relied on a diversity of sources to raise and channel funds to support the struggle by the Muslims against the soviet invasion.

source of TF, New Model terrorist groups have been deployed by state sponsors to achieve covert international relations goals.[140]

3.5.4 The Use of Non-Financial Resources for TF

The extensive focus on financial resources TF has led terrorist groups to focus on non-financial forms of value in furthering some of their goals. The measures can be traced to old models of terrorism that were used by the anti-colonialists. Under the new model, non-financial resources mostly include Foreign terrorist fighters (FTFs). The FATF report on emerging threats to TF reveals that FTFs are primarily a non-financial resource to terror groups.[141] FTFs are a major threat to AML/CTF measures due to the diversity of ways through which they can assist terror groups. Similarly, since they are individuals who sometimes have no past ties to terrorism, their involvement can occur without the awareness of the monitoring mechanisms established by counter-terrorist institutions.[142]

FTFs join or are recruited to terrorist groups on account of their potential contribution to the cause.[143] The involvement of FTFs places a challenge on AML/CTF strategies since these FTFs can overcome most of the measures for controlling TF. For instance, by self-financing an attack,[144] FTFs can defeat the CTF measures, which focus on preventing the raising and storing of resources that eventually end up being used to finance terror attacks. Since the contribution to terrorism by FTFs may have occurred Before the emergence of 'New Terrorism' by ISIL and Al Nusra Front,

---

[140] T Keatinge, The Role of Finance in Defeating Al-Shabaab. (*Whitehall Report* 2014). <https://rusi.org/sites/default/files/201412_whr_2-14_keatinge_web_0.pdf> Accessed January 29, 2021. 24, who cites the case of Eritrea supporting Al Shabaab in early 2010s until international pressure forced it to scale back, while M. Burton, "The Challenges of ISIS and the Modern Nation-State" (2016) cites the case of the US and Russia supporting different factions involved in the fight against ISIS, some of which were essentially terrorist groups.

[141] FATF, *Emerging Terrorist Financing Risks* (FATF, 2015), which indicates that although FTFs do not contribute through financial resources, they facilitate the operations of terror groups by providing human resources. See also *R v Yahya Rashid* [2016] EWCA Crim 568, where a student utilised his student loan and other grants to finance his travel to join ISIS.

[142] See H Yalcinkaya, 'Turkey's Struggle Against the Foreign Terrorist Fighters of Daesh', (2016) 21 Perceptions, 29, who indicates that the diversity of ways through which FTFs are recruited and how they assist the terror groups is so broad that it has been challenging for AML/CTF institutions to develop a learning curve on how to deal with the threat.

[143] FATF, n(141), which indicates that FTFs offer human resources services to terror groups based on their specialisations, while others facilitate terror attacks on foreign lands, thus limiting the need for terrorist groups to organise for cross-border logistics.

[144] Ibid, whereby 90% of the case studies by the FATF among terror cells in Western Europe reveals that the TF was done through personal savings, loans taken by individuals involved in suicide attacks, or funds raised from legitimate businesses, but diverted to terrorist attacks.

FTFs were not considered a threat under terrorism.[145] Similarly, in some isolated cases, the FTFs end up supporting terrorism without knowing it.[146] A comparison between AQ during the 9/11 attacks and the ISIS terror networks reveals that the involvement of foreign fighters has diversified the abilities of terror groups to plan and execute their attacks.

The FATF has raised concerns regarding the returning FTFs who lead TF and terrorist activities in their countries. Through their proactive approach to CTF, the FATF has raised concerns that these returning FTFs can exploit the existing systems to raise money to finance terrorist attacks in their countries. [147] The involvement of Foreign Terrorist Fighters (FTFs) presents significant challenges to terrorism financing (TF) and state responses to combating terrorism financing (CTF). Firstly, FTFs, as non-financial resources, can bypass traditional AML/CTF measures and self-financing attacks without raising suspicion. Secondly, their diverse methods of support complicate monitoring, making it difficult for counter-terrorist institutions to detect and prevent their activities. Thirdly, returning FTFs can exploit existing financial systems to fund terrorist activities, undermining domestic security efforts. Lastly, the evolution from traditional terrorism to "New Terrorism" by groups like ISIL and Al Nusra Front, which heavily involve FTFs, has diversified the operational capabilities of terror groups, complicating state CTF strategies.

3.5.5 Highly Developed Social Media Capabilities

Web 2.0 tools have provided new model terrorist groups with the ability to engage in TF through a more effective approach than under previous waves. These multifaceted communication tools offer a highly integrated platform for terror groups to communicate and interact with a broader range of individuals, thus expanding their base of supporters and sympathisers while

[145] Yalcinkaya, n(142), 27 S See, "Returning Foreign Terrorist Fighters: A Catalyst for Recidivism Among Disengaged Terrorists." (2018) 10 Counter Terrorist Trends and Analyses, 6, 11.

[146] C Davies, 'ISIS Suspect Jack Letts' parents Found Guilty of Funding Terrorism (2019) whereby the parents of an FTF, who send him £223 after the parents were made to believe that he was stuck in Syria. See also V. Edwards, 'Indiana mother married to ISIS extremist who moved her young family to Syria is sentenced to six and a half years in prison for providing $30,000', whereby a woman married to an individual who ended up as an FTF travelled to Syria with valuables worth $30,000, which were eventually used to finance terrorists' activities.

[147] FATF, n(141) indicates that the returning FTFs utilise the skills they have acquired in the terrorist camps to engage in fraudulent activities, by targeting beneficiaries of social services, some of whom lack knowledge on how the financial system can be exploited.

promoting their ideology.[148] Ultimately, social media tools have been used to bypass the measures designed to control the flow of information by directly broadcasting their messages and activities on online platforms. Through the internet, terrorist groups have been able to communicate with a broader audience, thus increasing the number and diversity of potential recruits, sympathisers and supporters cost-effectively and efficiently.[149] Most foreign terrorist fighters are recruited through these social media platforms, where people who are disenfranchised within their societies can be radicalised and used to implement attacks.[150]

Social media platforms offer terrorist groups the ability to engage in TF since they enable the group to raise, store, transfer, and use the resources in a manner that meets most of the six elements of the criteria set by Freeman.[151] A multiplicity of case studies by MENAFATF reveal that terror groups relied on social media platforms, including Facebook, Twitter, YouTube, Telegram, WhatsApp, Instagram and Snapchat, for covert and overt communication purposes. First, social media platforms are used to coordinate fundraising activities. Terrorist groups such as ISIS have achieved significant success, much the same way AQ relied on donations through charities.[152] To mask the true purpose of the funds, these groups advertise the fundraising campaigns using appealing language without mention of terrorism or similar purposes.[153]

---

[148] MENA FATF, 'Social Media and terrorism Financing' (MENA FATF 2019) <<http://menafatf.org/sites/default/files/FINAL-TM-SF-en.pdf >Accessed on January 29, 2021 found that social media platforms facilitate TF through social networking services (whereby individuals meet and interact about a variety of topics), content hosting services (individuals host content for generating funds, or promoting certain information), crowdfunding services (where users present their project so that the users can contribute to its success), and internet communication services (two or more users communicate through voice, text and video).

[149] Keatinge and Keen, n(46),15. They indicates that to recruit operates, AQ had to rely on face-to-face contact, which was time consuming and risky. However, groups like ISIS now recruit through online platforms through micro-targeted and personalized messages, whereby interested persons can then be targeted through one-to-one encrypted communications platforms, such as WhatsApp or Telegram.

[150] M Burton, 'The Challenges of ISIS and the Modern Nation-State' (BA Thesis Union College 20161), <https://digitalworks.union.edu/theses/126 > accessed 29 January 2021 who indicates that ISIS has utilised social media and other online platforms to publicise their attacks to impressionable youths who are prone to violence, and in the process, create novel belief systems that can be exploited for finances or other forms of support.

[151] These include anonymity, ease of access, security due to encryption, widespread availability with the increased internet penetration, real-time access, reliability due to continuous generation of funds, ease of modification in case of crackdown, and ability to influence the public through propaganda.

[152] FATF, n(141) indicates that fund raising through social media by terrorist groups is normally masked in order to hide the true purpose of the

[153] Ibid, , who indicates that although the terrorist groups hide the purpose of the funds, they can also indicate that the funds are to be used for humanitarian purposes in the locations where terrorists operate, thus increasing the possibility that well-wishes will contribute. Similarly, due to the increased surveillance for such messages on social media, the groups use images, whereby the information embedded therein cannot be identified through the automated monitoring systems installed by social media networks.

Individuals also use the platforms to help the donors defeat the AML/CTF measures in place through the provision of guidance on how to transfer the funds. The instantaneous communication facilities also enable terror groups to move funds from one account to another as soon as they are transferred, thus defeating the measures in place to freeze the accounts or confiscate those resources. With the possibility of social media platforms to create money transfer facilities for users in the group, the potential for misuse has been widely discussed.

3.5.6 Adoption of New Technologies for TF

Emergent technologies are often discussed, focusing on the risks they present to terrorism finance. Some of the predictions have materialised, such as the Law Commission using the example of a lone actor who relied on the existing financial system and social media to plan and implement an attack.[154] Other predictions failed to materialise, such as the 20th-century predictions about the possibility of terrorists using biological agents in their attacks.[155] A number of the emergent technologies used in TF have played a role in successful attacks, with the ability of terror groups to raise, store, move and use funds. First, the use of prepaid cards has enabled terror groups to move funds from one point to another, as well as to raise funds through fraudulent schemes. Prepaid cards are primarily used by the bearer and can either be used to withdraw money from an ATM or redeemed for their value in particular outlets. Since the data on the prepaid card can be stored remotely and loaded onto the card easily through activation, terrorist groups have found this approach highly reliable since access to the funds is instantaneous and anonymous,[156] just like some crime groups did decades ago.[157]

Second, the use of online payment methods is also challenging despite the multiplicity of due diligence measures put in place. FATF Recommendation 8 recognises the specific risks

[154] Law Commission, above, n(135) who cites the case of Ahmed Hassan, who planned an attack on a district line tube train in September 2017, using materials purchased through gift cards and assembling them through instructions provided through social media platforms by ISIS recruiters.
[155] Costa and Baños, (n_ 9.
[156] FATF, *Money Laundering using New Payment Methods* (FATF 2010)', which indcates that anonymity can be achieved through the use of anonymous products where the customer details are not provided, or indirectly, such as through stolen identities or fake details.
[157] K R Choo, "Money Laundering and Terrorism Financing Risks of Prepaid Card Instruments' (2009) 4 Asian Criminology, 11, who indcated that prepaid cards are preferred due to the fact that they can be transported physically across borders and masked as something else, and used elsewhere without the awareness of the regulatory and monitoring institutions.

associated with online business transactions which do not involve face-to-face interactions.[158] Due to the increased utilisation of these means, terror groups have inserted themselves into the value and supply chains of the transactions and are known to exploit the facilities to generate, store, move and utilise funds for terror purposes. Internet-based payment services are an extension of traditional banking, and their design and characteristics are still novel within most jurisdictions.[159] The ability of banking institutions to monitor the use of these services is complicated by the multiplicity of third-party entities involved in the fulfilment of the service. For individuals who are not privy to how technology can be exploited, online payment services present a key threat to AML/CTF activities. An online payment system has been utilised to purchase materials for planning attacks. Due to the utility of online payments, and the ability to transform them from one form of currency to another, the risk from these payment methods is high. Terror groups are known to move money electronically from one bank or institution to another, thus limiting the traceability through audit trail means.

Third, the creation of commercial websites provides terror groups with the opportunity to generate revenues by offering certain services, after which the funds can be utilised to plan and implement attacks. The viability of this approach to generate funds was demonstrated by individuals who utilised the era of information weaponisation under Fake News to generate hundreds of thousands.[160] The risk is widely recognised by FATF, whereby commercial websites that are ultimately used for classified advertisements are utilised for fundraising activities.[161] Terror groups such as ISIS have shown an increased ability to exploit the demand and supply scenarios in most industries, with the most recent being the sale of fake PPEs during the COVID-19 pandemic to finance its terrorist activities.[162] The combination of commercial websites and

[158] FATF, n(156), 8.
[159] S W Laksmi, 'Terrorism Financing and The Risk of Internet-Based Payment Services In Indonesia'. (2017) 9 Counter Terrorist Trends and Analyses, 2, 21.
[160] A Smith and B Vladimir, 'Fake News: How a Partying Macedonian Teen Earns Thousands Publishing Lies' (*NBC news* 2016) <https://www.nbcnews.com/news/world/fake-news-how-partying-macedonian-teen-earns-thousands-publishing-lies-n692451> accessed 29 January 2021 and E J Kirby, 'The City Getting Rich From Fake News' (*BBC* 2016)< https://www.bbc.com/news/magazine-38168281> accessed 29 January 2021 who idncate that numerous individuals created websites and published news with extensive appeal in order to atrtact views and earn from advertising fees from both Google and Facebook.
[161] FATF, '*Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems* (FATF 2008)
[162] C Herridge, 'ISIS Accused of Selling Fake PPEs Online to Finance Terrorism'. (CBS News 2020) https://www.cbsnews.com/news/isis-accused-of-selling-fake-ppe-online-to-finance-terrorism/ Accessed 29 January 2021. who indcated that the group was peddling fake N-95 masks and others PPEs through online platforms.

online payment methods creates a multiplicity of risks that represent TF opportunities; the FATF Report[163] identifies exit scamming and the sale of non-existent products as an avenue for TF.

Fourth, the risks associated with new forms of currencies that are outside the control of traditional banking institutions have also been researched. The risk from virtual assets[164] such as crypto-currencies differs from that related to internet payment systems because the value of cryptoassets and virtual currencies is based on a different philosophy.[165] Since they are not issued by any government, the demand and supply of crypto-currencies are outside the control of most governments involved in AML/CTF activities.[166] Over time, the emergence of altcoins designed as alternatives to Bitcoins diversifies the types of risks for TF since each of these forms of cryptocurrencies has vulnerabilities for misuse for ML/CT.

Despite the lack of empirical evidence, emergent research pivots towards the potential for terror groups adopting cryptocurrencies to raise, store, move and use resources for planning and implementing attacks.[167] These studies focus on the possibility of terror groups using the cryptoassets to raise, store, move and use resources for terrorism activities through the forward-looking approach.[168] Criminals have thrived through the use of cryptocurrencies such as Bitcoin, with the example of Silk Road being the most prominent marketplace for a diversity of illegal products and services.[169] TF activities can be achieved in several ways, including the following.

---

[163] Ibid, 17

[164] FATF, '*FATF Report to the G20,* (FATF 2020) defines virtual assets as digital representation of value that can be traded, transferred or used for payment on digital platforms.

[165] Whereas internet payment means facilitate payment of traditional currencies, virtual currencies have a different missing text here.

[166] C Dion-Schwatz, D Manheim and PB Johnston, 'Terrorist Use of Cryptocurrencies: Technical and Organisational Barriers and Future Threats'. (*Rand* 2019). <https://www.rand.org/content/dam/rand/pubs/research_reports/RR3000/RR3026/RAND_RR3026.pdf > Accessed 29 January2021.who indicates that although the main crypto currencies have predictable market values, in terms of quantity and value, the fact that no central banks controls these aspects increase the risks asscaited with their use in ML/TF

[167] I. Salami, 'Terrorism Financing with Virtual Currencies: Can Regulatory Technology Solutions Combat This?', (2018) 41 Studies in Conflict & Terrorism, 1–22 and P Carroll, and J Windle, 'Cyber as an enabler of terrorism financing, now and in the future' (2018) 13, Journal of Policing, Intelligence and Counter Terrorism, 285, all who recognise the potential threats for use of cryptoassets for TF, based on how well they have been deployed for use by terrorist groups.

[168] G Pavlidis, 'International regulation of virtual assets under FATF's new standards', (2020) 21 Journal of Investment Compliance, 1, 1, indicated that the FATF created Recommendation No 15 under the 2018 report, to cover the risks associated with ML/TF from virtual assets.

[169] T Keatinge, D Carlisle, and F Keen, *Virtual currencies and terrorist financing: assessing the risks and evaluating responses* (European Parliament, 2018) <https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf> accessed

- The launching of initial coin offerings (ICOs)[170]
- Purchase of cryptoassets for transfer or store of value[171]
- Using cryptoassets to purchase products and services on the darknet[172]

Cryptoassets are a secure and reliable tool for the transfer of wealth, with the potential for generating revenues in the process. As a result, it is challenging to seize or confiscate physical resources such as cash or property. With the potential for gaining value, cryptoassets provide terrorists with an opportunity for speculative investing.[173] Although the process of dealing with cryptoassets requires technical knowledge, the globalisation of terrorism makes it possible for terror groups to access the knowledge easily. Furthermore, with the increased usage of the darknet in most of the failed states as a way of sidestepping the limitations to access the internet, most individuals have become proficient in these technologies.

Several challenges associated with these new payment methods, such as prepaid cards, mobile money, and internet payment, are that not all jurisdictions require the identification of the users.[174] Even in locations where identification is required, the ability to monitor all transactions is challenging, as reported for the Dusit D2 attack by Al Shabaab.[175]

3.6 Conclusion

The scale and scope of TF have changed. The definition of TF in both jurisdictions has transitioned to cover additional dimensions, over and above the generic TF definition revolving around raising, storing and moving funds. In the more recent legislative frameworks, the two jurisdictions recognise the need to understand how terrorists create value from the funds, as well as how they raise, use, move, store, and obscure the TF activities based on the situation.

---

21 January 2021 who indicates that Silkroad was a marketplace created to facilitate the trade in illicit products and services, with the primary currency used being Bitcoin.

[170] C Whyte, 'Cryptoterrorism: Assessing the Utility of Blockchain Technologies for Terrorist Enterprise' (2019) 46 Studies in Conflict & Terrorism, 13, who indicated that ICOs are created for raising funds, thus giving terrorist groups the ability to raise, store, move and use funds. See also F M J Teichmann, 'Financing terrorism through cryptocurrencies – a danger for Europe? (2018) 21 Journal of Money Laundering Control, 4, 515, who indicated that terror groups can work with rogue nations which face financial sanctions in order to facilitate the ICOs, which essentially presents an opportunity for next frontier in state-sponsorship of terrorist.

[171] Salami, n(167) at, 15.

[172] Windle above, n (167) at 290.

[173] See Whyte above, n(170)

[174] FATF, n(156)

[175] Ibid.

The differences in TF definitions reveal the challenges associated with the highly anticipated global CT structure, which is integral in global governmentality.[176] The objectives of these definitions, as well as the involvement of different institutions culminating in the establishment of FATF-style frameworks, have reshaped international relations for CT, both in explicit and implicit ways. As a result, although the various institutions have unique structures, objectives, and jurisdictions, they all contribute to the broadening of governmentality for CTF purposes.

The difference in TF definitions is also attributable to the fact that the responsibility for implementing the countermeasures lies with different institutions. Each agency or department has unique characteristics, motivations, powers and capabilities. The challenge arises in that the process of establishing terrorist associations relies on less concrete associations than other existing laws. In most cases, LEAs deal with cases where there is no apparent intent while relying on secret evidence and conducting *ex-parte* hearings. The impact of these actions is evident in the changes in the health of democratic governance since the fight against terror started, with the practical consequences of failure to consider the rights of certain individuals evident. One of the most evident effects arises from the alienation of domestic and international parties, which bears significant negative connotations to the prevention of terror threats. Ultimately, the credibility of the institutions and governments that promote such measures has been called into question. The situation is worsened by the fact that governments such as the UK have failed to allow for public scrutiny of the processes for implementation of some of the measures, such as the creation of blocklists. The potential for real or perceived misuse of such strategies is often counterproductive.

The introduction of institutional frameworks such as the FATF, FIUs and the entities designed to fulfil the goals of the financial war on terrorism has driven terrorist groups towards innovation as they seek ways to avoid the intricate AML/CTF regimes. Although the existence of a correlation does not imply causation, the emergent TF approaches under the New Model of terrorism are complex and fundamentally designed to enable the terrorist groups to achieve their goals, regardless of the countermeasures within the various jurisdictions. The differences in the

[176] Governmentality involves emphasis on the governing of the conduct of people through positive approaches, rather than the imposition of sovereign power based on formulated legal frameworks.

utilisation of the various TF approaches in various jurisdictions, vis-à-vis the present AML/CTF, indicate the fact that jurisdictions ought to enhance their AML/CTF in order to achieve parity.

Chapter IV: International CTF Legislation on Cryptoassets

4.1 Introduction

The globalisation of terrorist threats has necessitated the introduction of a commensurate international counter-terrorism financing (CTF) legislative framework. The response to these emergent threats, as highlighted in Chapter Three, has made the regulation and monitoring of cryptoassets a key priority. The concerns about the risks associated with cryptoassets arise from the fact that they enable cyber-dependent criminal activities and establish opportunities for terrorists to raise funds that can ultimately be used to finance terror-related activities.[1] The majority of the provisions in the legal frameworks bear semblance to the traditional anti-money laundering/counter-terror financing (AML/CTF) policies; cryptoassets have introduced new dimensions of risks that necessitate specific considerations within the legislative, regulatory and monitoring strategies. Emergent[2] and extant[3] literature concur on the fact that online systems provide loopholes to the existing regulatory frameworks.[4] One of the often-overlooked challenges associated with the regulation of cryptoassets is the lack of robust accounting and reporting standards.[5] These reporting standards enable institutions to provide reliable information that can be used as legally binding evidence in case illegal activities are suspected.[6] The legal concerns associated with cryptoassets focus on the activities of crypto exchanges since these are the

[1] J B Delston, 'The Criminalisation of Money Laundering and Terrorism in Global Contexts: A Hybrid Solution. (2014) Journal of Global Ethics 10, 326.

[2] M M Abdeldayem and S H Aldulaimi, 'Cryptocurrency in The GCC Economy' (2020) 9 International Journal of Scientific & Technology Research. who argued that entry of crypto currencies in the GCC region presents a unique set of challenges, thus explaining why the majority, 85% of the countries have not taken up either Ethereum or Bitcoin.

[3] D Sonderegger 'A regulatory and economic perplexity: bitcoin needs just a bit of regulation' (2015) 47 Wash. Univ. J. Law. Policy 47:175–216

[4] O Marian, 'A conceptual framework for the regulation of Cryptoassets' (2015) 82 Univ. Chi. Law who indicated that the regulation of crypto currencies must consider the unique characteristics of these instruments to ensure effectiveness. Also see H Deng and others, 'The regulation of initial coin offerings in China: problems, prognoses and prospects' (2018) 19 Eur. Bus. Org. Law. Rev, 470 and A Brookes, 'U.S. regulation of block chain currencies: a policy overview' (2018) 9 Am. Univ. Intell. Prop. Brief., 80

[5] See CPA Canada, 'Audit Considerations Related to Cryptocurrency Assets and Transactions' (CAP Canada 2018), < CPA Canada, 'Audit Considerations Related to Cryptocurrency Assets and Transactions'. (2018)> accessed 22 February 2022 who indicates that accounting and reporting standards, such as the International Accounting Standards, which were replaced by the International Financial Reporting Standards (IFRS). These accounting standards enable firms, and individuals, who participate in the creation, ownership and transactions associated with cryptoassets to provide reliable qualitative and quantitative information on the characteristics of the crypto market at any point in time.

[6] D Jayasuriya, "Money laundering and terrorist financing: the role of capital market regulators" (2002) 10 Journal of Financial Crime, 30

institutions which are directly involved in the supply and demand of cryptoassets.[7] The illegal activities associated with cryptoassets include money laundering and financing of illegal activities, including terrorism, the purchase and disposal of cryptoassets, goods and services in the dark web marketplaces, evasion of controls on the movement of capital and foreign currencies and payment of ransom, among others.[8] Over the last 10 years, the dominance of Bitcoins as the primary crypto asset has been challenged due to two circumstances. First, the emergence of private 'tokens',[9] some of which are created through ICOs, has led to the number of cryptoassets in the market. Second, the creation of digital currencies by several central banks has led to the emergence of stablecoins.[10]

Therefore, in this chapter, the international CTF legislation is reviewed, focusing on four main aspects. First, a general overview of the international legislative frameworks on cryptoassets is provided, focusing on the regulatory and oversight activities by institutions such as the UN, the EU and the FATF. In the second section, the principles that guide the regulation of cryptoassets are provided, with a specific focus on five key principles. In the third and fourth sections, a review of the crypto asset standards in Bahrain and the UK are reviewed, focusing on the institutions involved in the regulatory processes, the performance based on the most recent review by FATF, and the apparent weaknesses in the current regulatory perimeter. Finally, recommendations shall be provided based on the weaknesses in the regulatory frameworks in the International CTF standards. In doing so, the chapter aims to address the following research sub-questions: The first subsidiary question is whether the international legal framework applies to cryptoassets. The second question is, does the financial war on terrorism re-tackle the concept of terrorism financing?

---

[7] R Houben and A Snyers ‘‘Cryptoassets: Key Developments, Regulatory Concerns and Responses’ (2020). https://www.blockchainwg.eu/wp-content/uploads/2020/05/IPOL_STU2020648779_EN.pdf accessed 22 February 2022 who indicated that crypto asset exchanges are targeted through measures involving licensing and registration, and they have provided most countries with a reliable pathway to controlling the misuse of cryptoassets.

[8] FATF *Virtual Assets and Virtual Asset Service Providers: Guidance for a Risk-based Approach* (FATF, 2019).

[9] FCA, ‘Guidance on Cryptoassets Feedback and Final Guidance to CP 19/3’ < https://www.fca.org.uk/publication/policy/ps19-22.pdf> accessed 22 February 2022 on consultation under the UK Crypto Asset Task Force Report (CATF), Exchange tokens: Cryptoassets not backed or issued by a specific central authority and are designed and intended to be used as a medium of exchange, Utility tokens: Cryptoassets that grant the holders access to current or future products or services, but are not specifically investments and Security tokens: Cryptoassets with particular characteristics through which they specify the rights and obligations with reference to a particular investment. These resemble shares or debt instruments.

[10] I Chiu, ‘Pathways to European Policy and Regulation in the Crypto Economy (2019) 10 European Journal of Risk Regulation who argues that These changes have captured the interest of regulatory institutions, legal scholars, and institutions involved in the establishment of industry standards, specifically regarding the broadening of the definition of crypto-assets, and scrutiny of the previously perceived or actual risks and opportunities within the global marketplace.

The third sub-question is whether the UN counter-terrorism financing provisions after 9/11 address this new form of TF. The fourth question is does the FATF cover this? If so, what does that entail? The last subsidiary question is how the UK and Bahraini governments are responding to the challenges surrounding the regulation of cryptoassets? In addressing these questions, this chapter will be able to advance the academic discourse on the international legal framework on cryptoassets and address the second research question of the study, which aims to identify the relevant international and national frameworks that regulate efforts against cryptocurrency use in terrorism financing in general, as well as in Bahrain and the UK.

4.2 General Overview CT Legislation on Cryptoassets

Extant and emergent literature presents conflicting conclusions on the link between terrorism and cryptoassets. One strand of the literature suggests that terror groups have little interest in cryptoassets due to the challenges associated with their use in conflict zones.[11] A different strand of literature posits that digital currencies are a gold mine for criminal enterprises, as can be seen in the literature review chapter of this study. In addition to the ease of transfer and lack of oversight on their use and exchange, these currencies provide a viable way to acquire, transfer and use assets.[12] The regulatory frameworks at the national level have focused on one or all the following dimensions:

- Tax treatment
- Implications of anti-money laundering/ counter-terrorism financing (AML/CFT)
- Requirements for reporting and registration
- Requirements for cybersecurity and fraud
- Regulation of the financial entities involved in the cryptoassets and
- Permitted usage, ownership and creation[13]

[11] L Borlini and F Montanaro, 'The Evolution of the EU Law Against Criminal Finance: The Hardening of FATF Standards within the EU. (2017) Georgetown Journal of International Law See also W A Tupman, 'Ten Myths About Terrorist Financing' (2009) 12 Journal of Money Laundering Control 12, 189.

[12] E Howden, 'The Crypto-Currency Conundrum: Regulating an Uncertain Future' (2015) *29 Emory International Law Review.* who argued that the dichotomy of views surrounding crypto currencies can be summarised into two views. On one hand, the increase in value is indicative of a bubble, and the fact it is suitable for nefarious activities means that is should be controlled or outlawed.

[13] See European Central Bank, *Crypto-assets: Implications for financial stability, monetary policy, and payments and market infrastructures*" (Occasional Paper Series No. 223 2019) and House of Commons, *Government and Financial Conduct Authority Responses to the Committee's Twenty-Second Report: Crypto-assets*' (House of Commons, 2019).

Despite the diversity of concerns, countries are inclined to focus on a limited scope of these dimensions since there is an overlap in the impact of each regulatory dimension identified above.[14] For instance, most regulatory institutions focus on cryptoasset exchanges since they act as a link between the cryptoassets market and the traditional financial sector.[15] Similarly, by targeting exchanges, most countries can prevent the most prevalent forms of malpractices, including price manipulation[16] and wash-trading.[17] A different approach is proposed by Bullmann *et al.,*[18] who indicated that the regulation of the creators of the cryptoassets lays the foundation for effective regulation by creating stablecoins.

The regulations surrounding cryptoassets from different countries differ in terms of the degrees of control, from laissez-faire oversight to the legalisation of possession and use. The patchwork of state-level regulations exists on a spectrum, with one set of countries imposing total restrictions[19] while others promote their adoption and utilisation. Despite these differences, these countries are faced with the challenge arising from the fact that although the use, ownership and creation of the assets occur at a global level, regulation is currently limited to the national boundaries.[20] The application of different definitions and nomenclatures of these cryptoassets magnify the challenges associated with tackling the varied policy and legal questions that often arise. This is why some countries actively foster the development and use of cryptoassets,[21] while others have restricted or outrightly banned crypto-assets.[22] Some countries have adopted an optimistic approach to the

[14] Sonderegger, n(3) who who indicated that comprehensive regulation of cryptoassets has adverse effects, since it drives individuals and entities in the crypto market to seek loopholes.
[15] Houben and Snyers n(7) at 6.
[16] N Gandal, and others, 'Price Manipulation in the Bitcoin Ecosystem' (2018) 95 Journal of Monetary Economics. who cites the case of Mt. GOX, whereby trading bots were used to fake transactions to create non-existent demand, and, to increase the price of Bitcoin, one of the earliest cryptoassets.
[17] D R Deakin, 'Study Declares 95% of Reported Bitcoin Trading is Fake.' (2019) <https://www.notebookcheck.net/Study-declares-95-of-reported-bitcoin-trading-is-fake.414981.0.html accessed 29 January 2021 who concluded that out of the 81 crypto asset exchanges with the highest volumes of trading, 71 reported misleading information. Out of the US$6B in bitcoin volumes trades, only US$273M were legitimate trade, with the remaining volume comprised of unverifiable trades designed to move the prices.
[18] D Bullmann, J Klemm and A Pinna, 'In search for stability in crypto-assets: are stable coins the solution?' (ECB 2018). https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf accessed 29 January 2021.
[19] China (which has banned its financial institutions from using crypto currencies, banned the ICOs and restricted the creation of crypto asset exchanges); South Korea (banned ICOs),
[20] See R M Nelson, 'Examining Regulatory Frameworks for Digital Currencies and Blockchain' (2019) <https://crsreports.congress.gov/product/pdf/TE/TE10034 > accessed 19 February 2024 Even among countries who operate in regional unions such as the EU and the GCC, any of the international treaties relating to cryptoassets are designed and implemented at the national level.
[21] Including Switzerland, Malta and Singapore.
[22] Houben and Snyers n(7), 6

regulation of cryptoassets by establishing balanced regulation regimes.[23] There are several reasons given for this position, including the evolution of the prevailing legal frameworks around cryptoassets and the fact that there are difficulties in achieving consensus on regulation by the different government institutions that are involved in oversight.[24]

The philosophical and intellectual shift in the functioning of financial markets has led to two main conclusions. First, the establishment of different rules for different countries does not necessarily culminate in a regulatory quagmire.[25] However, a customised approach offers the best solution to enable cryptoassets to enjoy the same level of trust as other mainstream fiat currencies. Second, heavy-handedness and bulky directives have the unintended impact of sparking innovations designed to circumvent the controls and promote the development of different cryptoassets, thereby reducing the demand and utility of the existing assets and harming the international economic and financial systems.[26] Third, piecemeal regulations fail to prevent speculative attacks.[27] Speculative attacks are viewed as a risk under ML/TF objectives,[28] whereby a powerful marketplace engages in aggressive buying or selling of cryptoassets to achieve certain objectives that may compromise the stability of the country's national currency.

Despite the sharp differences in the national patchwork of regulations, it is apparent that these regulations can be fit into two main domains: the financialised and the product dimensions.[29] The potential advantages of these technologies include the fact that Distributed Ledger Technologies (DLT) provide new business models based on peer-to-peer platforms, which has caused disruptive innovations in key sectors such as the energy industry.[30] The disintermediation of these sectors has created value for the end-consumers by increasing the mobility of products and services, thereby ushering in a new economic society. Under these technologies, the democratisation of transaction

[23] Averie Brookes, US Regulation of Blockchain Currencies: A Policy Overview' (2018) 9 Am U Intell Prop Brief 75
[24] Sonderegger n(3) 15.
[25] Howden n(12) at 29
[26] Ibid. 12.
[27] S Azgad-Tromer, 'Crypto securities: on the risks of investments in blockchain-based assets and the dilemmas of securities regulation' (2018) 68 Am. Univ. Law. Rev, who defines a speculative attack as the implementation of transactions, such as buying or selling of cryptoassets to achieve certain supply and demand outcomes that serve an ulterior motive.
[28] Ibid, 78.
[29] Ibid, 50
[30] T Morstyn and others, 'Using Peer-To-Peer Energy-Trading Platforms to Incentivize Prosumers to Form Federated Power Plants' (2018) 3 Nature Energy

verification has introduced novel challenges to a system that relies on arbitrary and systematic decision-making under highly institutionalised systems.

The political, social, economic, and environmental implications of these innovations explain why there is an increased interest among multinationals in limiting the risks associated with this new variable in the AML/CTF policies. These changes raise the question of whether global actors, such as the UN and, to an extent, regional entities, such as the EU, are obligated to participate in the prevention of terrorism and whether they are mandated to consult and gain consensus from other parties in their actions.[31]

4.2.1 United Nations

The involvement of the UN in ML/TF policies arises from the fact that the multinational entity offers a viable institutional framework for the implementation of the international legislative framework. The involvement of the UN can be traced to the signing of the UN Convention against Transnational Organised Crime (UNTOC) under Resolution 55/25, which came into force in 2003.[32] The measures were aimed at drawing countries together to prevent these cross-border criminal activities and entities. In addition to engaging in one or more vices, these establishments tended to cooperate in the furtherance of emergent criminal activities. For instance, criminal entities involved in human trafficking were capable of transitioning to arms trafficking in the facilitation of terrorism. Resolution 2462,[33] designed for combating and criminalising the financing of terrorists and their activities, introduced binding resolutions on all member states, a decision which implies that the UN can impose sanctions for countries found to engage in such activities. Resolution 2462 is intricately linked to UN Security Council Resolution 1373,[34] which was introduced following the 9/11 attacks in the US, whereby terror financing policies focused on the 'follow the money' approach, in addition to other strategies.[35]

---

[31] Delston n(1)

[32] United Nations Convention Against Transnational Organised Crime and the Protocols Thereto. ((adopted on 15 November 2000, entered into force on 29 September 2003) which covered activities such as human trafficking, smuggling of migrants by land, sea or air, and the manufacture and trafficking of illicit arms, components and ammunition, among others.

[33] F Cyrille, 'Transnational Crime and the Role of the United Nations in Its Containment through International Cooperation: A Challenge for the 21st Century' (200) 8 EUR. J. CRIME CRIM. L. & CRIM. JUST.

[34] Ibid, 5.

[35] Whereby the UK acquired the mandate to target specific entities and individuals who are viewed as high risk, with reference to money laundering and terror financing.

The UN has shown extensive interest in DLTs, primarily due to the potential advantages of their application in solving a multiplicity of challenges.[36] The United Nations Research Institute for Social Development concluded that blockchain technologies enable countries to facilitate the remittance of resources, enhance financial inclusion and promote structures for cooperation, all of which further the objectives of social development by the UN.[37] In response to these opportunities, UNICEF established a $6B crypto fund in 2019, whereby donations in the form of cryptoassets are provided to the agency.

The involvement of the UN in the regulation and oversight of cryptoassets arises from the fact that international criminal establishments have shown growing creativity in the use of cryptoassets in furtherance of their actions. The involvement of the UN is also attributable to the classification of money laundering as a criminal offence under the Vienna Convention.[38] The involvement of signatories to the UN treaties[39] has enabled the regulatory mandate to adopt a follow-the-money approach when targeting criminal and illegal activities associated with cryptoassets.

The involvement of the UN in the regulation of cryptoassets has the potential to introduce a new tool in the form of economic sanctions that are designed to punish or encourage the actions of nation-states.[40] At this level of regulation and monitoring, the UN provides a robust system through which state-sponsored actors in the crypto market can be influenced to prevent misuse. However, several reports indicate that the level of involvement of the UN in the crypto market is negligible.[41] This lack of oversight by the UN is attributable to the fact that crypto-assets are decentralised. Since they are created and used outside the scope of control of the UN and at the sovereign state level, most of these cryptoassets lie outside the regulatory environment of the UN. Similarly, the fact that most nation-states have not taken measures to harmonise their responses to the regulation

[36] United Nations, 'Blockchain-What does it Mean for the UN' (UN, 2018) <https://unite.un.org/sites/unite.un.org/files/emerging-tech-series-blockchain.pdf > accessed 6 November 2024, indicates that DLT promotes the administrative abilities of the UN, such as the deployment of international law, elections among member states, and dispatch of humanitarian assistance. It also lays down the foundation for peace building, disarmament, and achievement of human rights goals.

[37] B Scott, 'How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance? (United Nations Research Institute for Social Development, 2016).

[38] According to S Durrant., Understanding the Nexus between Cryptocurrencies and Transnational Crime Operations. (MA Thesis, CUNY John Jay College 2018. UN classified money laundering as a criminal offense in 1988, under the United Nations Convention Against Illicit Traffic in Narcotic Drugs and psychotropic Substances.

[39] See Cyrille (n 33), 5

[40] T Clautice, "Nation State Involvement in Cryptocurrency and the Impact to Economic Sanctions" (2019). Economic Crime Forensics Capstones. 43.

[41] Compared to the involvement in the traditional banking and financial services sector.

of cryptoassets has limited the ability of the UN to get involved, over and above its mandate, in money laundering and other international criminal activities.

Despite the limited involvement of the UN in the regulation of the crypto market, there is evidence of its interventions in some instances. Through the activities of the Office of Foreign Assets Control, a US agency, the UN can influence the responsible exchange of cryptoassets by screening for compliance concerning every transaction that involves the use of the US dollar. The mandate provided by the US enables the UN to monitor all wallet addresses that transact using the dollar proactively. However, there is evidence that most players in the crypto market have found workarounds to avoid regulatory oversight by the US.[42] The involvement of the UN cryptoassets offers an understanding of how international measures influence national legislative responses, such as those in the UK and Bahrain, to terrorism financing. The UN's binding resolutions, like Resolution 2462, highlight the importance of pursuing global efforts, which can inform Bahrain's strategy for regulating digital currencies. The challenges posed by decentralised cryptoassets offer interesting insights into the potential difficulties Bahrain might have in mitigating systemic risks to its financial systems. Additionally, the UN's efforts illustrate potential areas for enhancing legal frameworks, providing a basis for recommendations to improve AML and CTF measures in the UK and Bahrain concerning digital currency-based terror finance.

4.2.2 The Financial Action Task Force (FATF)

The involvement of the FATF[43] in the regulation of cryptoassets arises from the fact that its primary mandate is to prevent and mitigate risks and threats to the global financial sector.[44] Since 2014, the FATF has been actively involved in the development of standards for the regulation of cryptoassets, starting with the *'Virtual Currencies: Key Definitions and Potential AML/CFT Risks'*[45] in 2014 and a later report, '*Guidance for a Risk-based Approach to Virtual Currencies*' in 2015.[46] The FATF enjoys a global reach through cooperation with countries affiliated with the G20. Its most recent guidelines focus on the dynamic environment through which Cryptoassets are

[42] See Brookes n(24) 4.
[43] An intergovernmental organisation created in 1989 to combat money laundering but diversified its portfolio of activities to include anti-terrorism financing in 2001.
[44] See FATF (n 8)
[45] FATF Report, 'Virtual Currencies: Key Definitions and Potential AML/CFT Risks' (FATF2014).
[46] *Ibid*, 5.

developed, acquired and used,[47] especially due to the risks of the application of money laundering techniques and the potential use of such assets for terror financing. FATF utilises most of the measures applied in the contemporary financial sector when designing frameworks for controlling the handling of virtual assets.

The FATF offered new guidelines in response to emerging threats and measures for increased efficiency in the mitigation of risks and opportunities associated with the crypto market.[48] These include the following. First, diversification of the nomenclature of domains under its purview to include virtual assets (VA), which is a term that is more inclusive than cryptoassets. These virtual assets are a broader definition, including cryptoassets, tokens and other forms of digital value representation, since they cover all products and services that were previously categorised as cryptoassets.[49] Second, the FATF reinforced its recommendations on the utilisation of a risk-based approach in the activities by VASPs concerning VAs.[50] Third, assisting national institutions, both public and private entities, in understanding the risk-based approach specific to VAs and VASPs. The regulatory concerns regarding cryptoassets have focused on different dimensions based on the type of legislative systems in focus.

The lack of harmonised legislative frameworks can be attributed to the fact that cryptoassets were, until recently, considered a small constituent of the financial sector. Using the example of Bitcoin, its most significant price increase was reported in 2010, when it changed from US$0.0008 to US$0.08.[51] However, this value pales in comparison to the current price per coin, which is estimated at US$23,000[52] and is projected to increase to US$1M in the future. Due to the small size of the outstanding cryptoassets, concerns such as the protection of investors, anti-money laundering and risks of use in terror finance were overlooked. However, when the combined impact

[47] FATF Annual Report, 'Financial Action Task Force-Annual Report 2019-2020. (FATF, 2020).
[48] FATF, FATF Focus on Virtual Assets. (FATF, 2020).
[49] European Parliament. 'Virtual Money: How Much Do cryptoassets Alter the Fundamental Functions of Money? (EP, 2019) Furthermore, the categorisation as VAs reduces the confusion as to whether the elements are currency (money) or commodities. The VAs are provided by virtual assets service provides (VASPs). The diversified and comprehensive nomenclature increases the efficiency with which extant and emergent AML/CFT measures, such as registration/ licensing and monitoring/ supervision can be deployed.
[50] See Chiu n(10) K Braddick, A Bailey, and D Ramsden, 'Cryptoassets Task Force: Final Report'. (2018) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/crypto_assets_taskforce_final_report_final_web.pdf accessed 22 February 2022
[51] R Browne, 'Bitcoin Hits New All-time High Above $23,000, Extending its Wild 2020 Rally' (*CNBC News* 2020)<https://www.cnbc.com/2020/12/17/bitcoin-btc-price-hits-new-all-time-high-above-23000.html accessed 19 February 2022
[52] *Ibid*

of the widespread use of cryptoassets in multiple avenues is considered, the potential for transmission of the risk into mainstream channels of financial systems increases due to the integration of the international financial system. The involvement of the FATF in preventing ML through the cryptoassets industry underscores the importance of global cooperation in addressing the systemic risks of digital currencies. FATF recommendations have directly influenced the development of AML and CTF legislation in Bahrain and the United Kingdom. By setting international standards, the FATF's guidelines provide a framework that both countries can build upon to enhance their legal frameworks for AML and CTF. Additionally, the FATF's emphasis on a risk-based approach and assisting national institutions can inform recommendations for the UK and Bahrain to mitigate better the risks of digital currencies used in terrorism financing.

4.2.3 European Union

The EU, through the European Central Bank (ECB), relies on a combination of directives and norms,[53] which provide preventive propositions to be adopted by signatories to the legislative frameworks. As shown in the previous section, the recommendations from the FATF are, at best, influential on the decisions made by the legislation within a country or a region. The changes in the recent FATF recommendations have led to the emergence of a multi- and cross-disciplinary approach in the EU AML/CFT legislation, which focuses more on prevention and addressing the most prevalent challenges in the EU legislative framework.[54] A 2015 report by the ECB on Virtual Currency Schemes (VCS) highlighted the prevalence of the use of cryptoassets, with Bitcoin transactions amounting to 69,000 per day across the globe.[55] The EU agreed on input from the FATF and other institutions,[56] whose mandate revolves around risk-management-oriented strategies. In 2019,[57] the EU diversified its oversight mandate to specifically focus on the dynamic

[53] See Borlini and Montanaro, n(11), 1009.
[54] *Ibid*
[55] European Central Bank, "Virtual currency schemes – a further analysis" (*ECB* 2015) < https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> accessed 12 February 2022 whereby updates to the European Central Bank, "Virtual currency schemes", (October 2012) propositions are provided, including the issue of VCSs, specifically how they influence monetary policy and price stability, financial stability, promoting the smooth operation of payment systems, and prudential supervision, the materialisation of these risks depends on the volume of VCS issued, their connection to the real economy.
[56] According to these institutions include the Securities and Markets Stakeholders Groups (SMSG), the European Securities and Markets Authority (ESMA).
[57] See European Central Bank n(13)

risks arising from cryptoassets, as well as the establishment of a more effective link between the regulatory and oversight frameworks to ensure a seamless link between the two functions.

Based on these inputs, the EU has two key legislative frameworks that regulate the crypto markets concerning AML/CFT. First is the Basel Committee on Banking Supervisions[58], whose obligation is to provide guidelines on the prudential treatment of cryptoassets. As of 2019, the Committee[59] was in the process of implementing the improvements to Basel III, normally referred to as Basel IV, with the main improvement being about market risk frameworks.[60] These changes are in response to the realisation that the oversight and regulation of banking institutions must consider the specific risks of volatility, money laundering and terrorist financing associated with crypto markets. Second is the Money Laundering Directive (MLDs).[61] In the First AML Directive (MLD1), EU countries had elected to prohibit rather than criminalise money laundering legislation, a decision that provided limited preventive impetus for individuals who engaged in illegal activities. In the Fourth AML Directive (MLD4),[62] the definition of a crime is broadened, including the criminalisation of activities that facilitate money laundering within or outside the EU.[63] Similarly, the threshold for regulation was set at €10,000, with member countries having the freedom to adopt lower thresholds.[64] A Supranational Risk Assessment Report (SRAR)[65] from the implementation and operationalisation of the MLD4 identified several vulnerabilities in the existing portfolio of financial products and services, which culminated in the creation of the MLD5 framework. Under the most current framework, the fifth (MLD5), the role of cryptoassets in ML/CT risk exposures is discussed widely. Directive (EU) 2018/843 under MLD5 states that

[58] An international body for setting standards pertaining cryptoassets. The Basel Committee is an authority involved in the supervision of banking institutions, which publishes guidance on the use of cryptoassets by banking institutions, with specific focus on governance, due diligence, risk management, disclosure and dialogue.
[59] Which is comprised of 45 institutions from 28 countries.
[60] KPMG, 'Beyond Basel IV: Incorporating Cryptoassets into the Basel Framework (KPMG, 2019)
[61] J Kirschenbaum and N Veron, 'A Better European Union Architecture to Fight Money Laundering (2018) Policy Contribution
[62] H Koster, Towards better implementation of the European Union's anti-money laundering and countering the financing of terrorism framework' (2020) 23 Journal of Money Laundering Control
[63] *Ibid*, 25.
[64] European Commission, 'Report from The Commission to The European Parliament and The Council' (EC, 2019),
[65] European Commission, 'Report from The Commission to The European Parliament and The Council' (EC, 2017), whereby the regulatory framework focused on risk exposures from 47 products and services offered by the financial sector, across 11 sectors in the EU.

> "Once transposed into member state legislation, will extend the list of obliged entities to virtual currency exchanges and custodian wallet providers".[66]

Additional measures under the MLD5 that target cryptoassets to limit their use in illegal activities, specifically AML/CFT activities, include the following.[67]

- Regulating the custodians of wallet providers for virtual currencies and companies providing exchange services
- Identification of all entities in the crypto market
- Ensuring that all card providers and financial institutions involved in the crypto market understand the technical nature of the industry
- Registering all other providers of services related to virtual currencies, as well as other firms that use DTLs[68]

According to the SRNA for the MLD5 framework, despite the broad scope of these provisions under the MLD5, there are sparse details on how these regulations can be implemented in practice.[69] The lack of clear statements on how the economic agents are to be involved in the process is also evident from the language of the new framework. For instance, under AML5, there are provisions:

> "that includes closer collaboration between FinCEN and the federal functional regulators and greater authority for FinCEN to establish BSA examination and enforcement priorities across these agencies and similar to control interpretations of BSA rules".[70]

Following these changes, it is expected that AML guidelines will be more responsive to the changes in the regulatory and operational frameworks that drive money laundering and terrorist financing. The involvement of the EU, particularly through the European Central Bank (ECB) and its adoption of directives influenced by FATF recommendations, highlights a potential pathway that the non-EU states can embrace to develop their AML and CTF framework. The

[66] 'Directive 2018/843 - Amendment of Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing 156 OJL
[67] *Ibid*
[68] Failure to register crypto services providers in countries like Austria attracts a fine of up to €200,000.
[69] See European Commission n(65)
[70] Kirschenbaum and Veron n(62)

implementation of Basel III and subsequent enhancements under Basel IV illustrates the EU's initiative-taking stance in adapting regulatory frameworks to mitigate risks associated with crypto markets, including volatility and illicit financial activities. Furthermore, the evolution from MLD1 to MLD5 underscores the EU's commitment to strengthening measures against money laundering and terrorist financing, particularly through stricter regulations on virtual currency exchanges and custodian wallet providers. Lastly, the EU's efforts to enhance collaboration and enforce clearer regulatory standards highlight recommendations for improving legal frameworks in both Bahrain and the UK concerning digital currency-based terror finance.

4.2.4 The Need for Harmonisation of International Regulatory Frameworks

The patchwork of state-level and regional regulations, which exists on a spectrum, creates a multiplicity of challenges in the establishment of a unified approach to the regulation of financial instruments, including cryptoassets. In a recent study, the reported effects were reported at less than 0.1% of all the criminal financing activities that can be considered money laundering.[71] Furthermore, when the costs of compliance are taken into account, the viability of the measures is found to be limited.[72] The regulatory differences create several challenges, including the regulatory race-to-the-bottom, regulatory arbitrage and under-regulation with the hope of drawing certain benefits from the loopholes that exist in the characteristics, timing and implementation efficiency across different countries. The motivation for harmonization of the controls is drawn from the successes associated with past international standards targeting the financial sector, including the shadow-banking agreements[73] and Basel Accords[74], which have streamlined the operations in the banking sector in the past. The challenges of harmonising the legislative frameworks are widely studied in past literature (see the literature review chapter). In addition to the fact that regulatory frameworks are built upon a legal system that has a particular philosophical foundation,[75] it is

[71] R F Pol, 'Anti-money laundering: The world's least effective policy experiment? Together, we can fix it,' (2020)3 Policy Design and Practice, and Tupman n(11), 189.
[72] *Ibid*
[73] Designed by G-20, the regulatory reforms were developed following the 2008-09 credit crisis.
[74] A series of three banking regulations (Basel I, II and III), which were established by the Basel Committee on Banking Supervision, which recommends banking regulations, specifically concerning operational risks, capital risks and market risks.
[75] Brookes n(24), 77. For a different view see D Siswantoro, R Handika and A F Mita 'The Requirements of Cryptocurrency for Money, an Islamic View. (2019) 6 Heliyon,

imperative to note that there are unique principles in the regulation of cryptoassets, as shown hereunder.

By reviewing the UN, FATF, and EU legislation on cryptoassets, this chapter has shown that the different jurisdictions have struggled to come forward with well-devised and relevant frameworks that could effectively regulate cryptoassets internationally. There are a number of harmonisation challenges that remain to be addressed, and more stringent regulation of cryptoassets is required to guarantee that terrorist organisations do not abuse such assets to finance terrorist networks and projects. In discussing the regulation of cryptoassets at the international level, the thesis has effectively answered the first sub-question the chapter is supposed to address, namely: does the international legal framework apply to cryptoassets?

4.3 Principles of Regulation for cryptoassets

The question of whether it is possible to normalise the regulatory policies for the crypto economy arises, especially in recognition of the contemporary conflict[76] that emerges concerning any legislative framework. The contemporary conflict arises from the fact that any regulatory policies or legislative frameworks must meet the philosophical norms in sectoral regulation[77] and the broader regulatory agendas that arise outside the financial sector, including human rights concerns, CTF and the promotion of financial innovation. In this section, the principles that inform the regulatory frameworks for cryptoassets are discussed.

4.3.1 Constructive engagement

In most jurisdictions, cryptoassets are linked to fraudulent and illegal activities.[78] A large percentage of the cryptoassets projects have failed, either for targeting goals that are too ambitious to be achieved or lacking the necessary technological infrastructure within the market, with investors losing their investments with limited recourse.[79] However, several projects have succeeded, with the results being an optimistic view of cryptoassets and a multiplicity of technological innovations.[80] As a result, regulations targeting assets should not be unduly biased

[76] See Chiu n(10), 48.
[77] In this case, the financial sector.
[78] See Azgad-Tromer (n 27), 100.
[79] See Deakin above, n(17)
[80] Howden n(12) at 12

due to the presence of bad actors. It should create a constructive methodology for systematic and logical integration of the assets into the regulatory mechanisms for existing financial systems.[81]

4.3.2 Classification

The classification of cryptoassets is a function of the regulation since it enables the various jurisdictions to operationalise their use and handling. From a functional perspective, cryptoassets can be classified as crypto-currencies, crypto-vouchers, and collective crypto investment schemes. However, there are disparities in the views regarding the classification of these cryptoassets, resulting in a lack of precision in the language.[82] Using the example of Bitcoin, cryptoassets have been classified as commodities, investment vehicles, digital assets or currencies.[83] Over the past 12 years, and due to innovation, there have been emergent cryptoassets that can be best described as alt-coins and second-generation 'cryptos'.[84] The differences in the technology that is used to create the coins present a legal challenge, including ownership, use, possession and ultimately, the contractual agreements between parties to any transaction involving the cryptoassets.

The current classifications of cryptoassets vary, but there are no differences between the various cryptoassets. However, from a legal perspective, the intrinsic characteristics have different implications on how they are treated. For instance, in the US, cryptoassets are considered commodities by the Commodities Futures Trading Commission,[85] while the Inland Revenue Services[86] treats cryptoassets as property for tax purposes, while the International Monetary Fund[87] treats bitcoins as non-financial assets. The classification determines the type of regulation that the cryptoassets are subjected to as a financial instrument. When classified as utility tokens, coupons or vouchers, the cryptoassets are viewed as representing claims on services or assets that are supplied through a network to enable the users or owners to enjoy certain forms of value from that

---

[81] O. J Mendeng, 'Basic Principles for Regulating Crypto-Assets'. (LSE 2018) https://www.lse.ac.uk/iga/assets/documents/research-and-publications/OJM-Basic-principles-for-regulating-crypto-assets.pdf , who highlights that the statement is predicated in the assumption that the existing financial regulations are prudent and suitable.

[82] M Demertzis and G B Wolff, 'The economic potential and risks of cryptoassets: is a regulatory framework needed?' Policy Contribution (2018) < https://euagenda.eu/upload/publications/untitled-176820-ea.pdf> accessed 22 February 2022 who classified cryptoassets as either cryptocurrencies (if they are used as a private means of payment) or initial coin offerings, (if they are used to fund new activities against the promise of future utilities).

[83] *Ibid*.

[84] *Ibid*, 17.

[85] CFTC, which is an intendent agency of the US government established to regulate the derivate markets, including Swaps, Futures and other types of options, in the US.

[86] IRS.

[87] IMF.

network.[88] On the other hand, security tokens designed to convey the value or stake in a particular property must be classified and regulated as securities. Finally, currency tokens, including digital currencies that serve as a medium of exchange, should be regulated at the institutional level rather than the instrument level.

To limit the exposures to the risks associated with classification for regulation, it is common for the entities that issue the cryptoassets to automatically qualify for the regulations that are widely used for financial instruments. However, for efficiency, exemptions are provided on a case-by-case basis.[89]

4.3.3 Protection of Consumers and Investors

The process of regulating cryptoassets should be linked to all principles of the financial system, including avoidance of conflict of interest, prudence, integrity, transparency, organised market conduct, and protection of the assets of clients.[90] In instances where crypto asset exchanges and issues take money from clients, the general responsibilities under fiduciary agreements have to apply, with a specific focus on CTF and AML guidelines. Cryptoasset exchanges, and to some extent, the creators of the assets, have to offer explicit and implicit provisions for price discovery, avoidance of front-running and collusion and stringent segregation of all monies from the various clients. To further protect investors and consumers, rules-based arrangements, including the decentralised autonomous entities and smart contracts,[91] must be examined to verify their applicability to the legal content under the various jurisdictions. A recent development facing cryptoassets is associated with the technical complexity of the technologies, which makes it possible for the emergence of a group of entities that controls a majority of the crypto asset. Using the example of bitcoin, an entity that controls more than 50% of the mining power or holds more than 50% of the available assets has the power to centralise control oversupply and pricing of the

[88] See G Giudici, A Milne, D Vinogradov, 'Cryptoassets: market analysis and perspectives. (2020) 47 *J. Ind. Bus. Econ.* who states that this is why some cryptoassets that exhibit features like gift vouchers or air miles should attract regulations akin to those of financial assets, even though they may function as such.
[89] Demertzis and Wolff n(82).
[90] See Azgad-Tromer n (27), 99.
[91] A smart contract is a software or computer program that governs transaction protocols that are executed automatically in order to control or document events and actions that are legally relevant. Since they are based on block chain technology, they can be sent automatically without third party interventions.

assets.[92] This highlights the need for consumers and investors to be protected in all regulatory frameworks.

4.3.4 Cryptography and technology

The complex nature of cryptoassets raises questions on whether the regulatory frameworks should extend to the underlying technologies used in the creation of the assets.[93] By regulating the technologies, it is possible to ensure that the cryptoassets that end up in the market are sufficiently transparent since there is an oversight on the technology infrastructure. However, technologies such as DLT have features that make it challenging for regulation and oversight, including the technical nature and the fact that they lack a predetermined innovation trajectory.[94] Most cryptoassets change in a manner that cannot be predicted, and the core technologies are too complex to legislate. Similarly, there are concerns that any legislation that governs the characteristics of technology is bound to limit its transformation. To ensure efficiency in the regulations, the legal frameworks should focus on the functions of the cryptoassets. This is because regulations to the underlying technologies, specifically cryptology, will have a disproportionate impact on other domains of information technology.[95]

4.3.5 Constancy

The regulations on cryptoassets and the activities related to the creation and use of the elements must be transparent, predictable and stable. Transparency in the regulations entails the involvement of all stakeholders affected by the creation, ownership and use of cryptoassets, including investors and individual and corporate users, among others.[96] The predictability of legislative frameworks is ensured through the development of judicial processes, including the specification of the institutions that make and interpret the legal frameworks, such as what is contained in FATF.[97] This includes the utilisation of legislation and case law in the process of ensuring that the provisions do not create conflicts. Finally, stability in the regulations involves

[92] Howden n(12), 4.
[93] M S Sackheim and N A Howell, *The Virtual Currency Regulation Review* (Law Business Research Ltd 2019)
[94] R Auer, and S Claessens, 'Regulating Cryptoassets: Assessing Market Reactions. (2018) BIS Quarterly Review. 57.
[95] See Giudici and others, (n88)
[96] R Robinson 'The new digital wild west: regulating the explosion of initial coin offerings' (2018) 85 Tenn. Law. Rev, 899.
[97] FATF n(48)

the creation of provisions that are not subject to unexpected changes.[98] The application of these principles solves several of the challenges identified in past research. Based on the comparison between the regulatory provisions in place in Hong Kong,[99] China,[100] the UK,[101] the US[102] and Singapore,[103] the protections which focus primarily on the protection of investors and customers differ in terms of the regulatory scope, the application of contemporary regulatory frameworks on emergent cryptoassets, and the need for promoting the development of markets while protecting the investors.[104] The discussion presented above has identified the key principles that guide the functioning of the cryptoassets and the different attempts that have been made in the different jurisdictions to regulate cryptoassets. Nonetheless, what is markedly absent in the discussion presented above is that principles in cryptoassets regulation are not capable of effectively addressing the risks that such assets pose in the context of terrorism financing. The material presented above addresses the third sub-question of this project, which is the UN counter-terrorism financing provisions after 9/11, which address this new form of TF.

4.4 Regulation of Cryptoassets

cryptoassets have become commonplace components in the global financial system. Due to an increase in the number of individuals, entities, and countries that create, use, and hold these assets, it has become necessary to standardise the definitions, technologies, and legislative frameworks related to cryptoassets. cryptoassets are like traditional currencies since they are designed as a store of value, a medium of exchange, and a unit of account.[105] Unlike traditional currencies, cryptoassets are not issued by central banks.[106] The absence of a centralised oversight institution has led to significant fluctuations in the value of the cryptoassets in the past. These fluctuations present a challenge to regulations.

[98] Houben and Snyers n(7) at 6.
[99] R. H Huang, D Yang, D. and F. F. Y Loo, 'The Development and Regulation of Crypto-assets: Hong Kong Experiences and a Comparative Analysis'. (2020). *Eur Bus Org Law Rev* 21**,** 2.
[100] The Law Library of Congress. 'Regulatory Approaches to Cryptoassets in Selected Jurisdictions. (2019), 74, which states that since the cryptoassets are not considered legal tender, financial institutions are not allowed to accept them.
[101] Ibid., at 258.
[102] Brookes n(4), 12.
[103] Law Library of Congress above, n 101.
[104] Huang and others, n 100, 2.
[105] Deng and others, n 4 at 470
[106] Brookes n(4), 81.

4.4.1 Two Competing Perspectives

The regulation of cryptoassets is faced with two competing perspectives: First, the choice problem, which arises because there are different approaches to the achievement of the AML/CFT goals in the regulation of cryptoassets, hence leading to the application of a blend of subjective and objective methodologies when selecting the most preferred approach.[107] Second, the constraint problem, which is the tendency of parties to the regulatory and legislative frameworks to rely on consent, leads to the justification of abhorrent objectives and goals.[108] It also raises the possibility that the policies that are finally consented to are too permissive of certain activities to guarantee stringency in their impacts. Due to the differences in the factors that influence choices and the experiences that determine the constraints in the type of regulations, there are six public policy concerns surrounding cryptoassets:[109]

- What potential do cryptoassets hold in the wider development and advanced financial systems?
- Which is the most suitable approach to combating the illegal activities associated with cryptoassets, including terror financing and money laundering,
- How can investor and consumer protections be ensured?
- How financially stable are these cryptoassets?
- What is the most viable approach to taxing the cryptoassets?
- How can the technology on which the cryptoassets are developed (blockchain) be embedded into the existing and emerging legal frameworks?

These public policy concerns explain the disparity in the philosophical basis and legislative structure of the regulations imposed on cryptoassets across different countries. According to Brzoska:[110]

[107] Delston n(1), 14
[108] J R, Lax, "Political Constraints on Legal Doctrine: How Hierarchy Shapes the Law." (2012) 74 The Journal of Politics 769,
[109] Demertzis and Wolff, n(82)
[110] M Brzoska, 'Consequences of Assessments of Effectiveness for Counterterrorist Financing Policy' (2014). 48 Administration and Society.

> "Past assessments have had a bias toward expanding the scope and intensity of CTF regulations and implementation because of their focus on output and outcome of measures, rather than on their impact on terrorist activity."

The propensity of countries to broaden the scope of regulation and intensify the impact of the regulations is attributable to the fact that there are emergent threats, as evidenced by the emergence of cryptoassets into the AML/CFT purview. In this section, a principle-oriented framework for the regulation of cryptoassets to achieve a balance between regulation and oversight is provided.

4.4.2 The Challenge with Widespread Acceptability

Despite the uniqueness of cryptoassets, a historical review of the emergence of 'currencies' reveals that cryptoassets faced the same catalogue of challenges as paper currencies at the turn of the Nineteenth Century. In Germany, for example, the introduction of paper money was shunned, primarily due to claims of potential challenges with regulation and the risk of excessive circulation.[111] The outcome was the preservation of the existing financial institutions and the introduction of mechanisms for transparency established on common rules. Through regulations focusing on the instruments and institutions,[112] Germany was able to achieve widespread acceptance of paper money, with peasants allowed to purchase land through borrowed money in 1850. Based on this illustration, it is possible to envisage similar widespread acceptability of cryptoassets. In fact, cryptoassets have become more and more acceptable in banking and finance. The driving force behind this acceptance can be traced back to the 2008 Global Financial Crisis, which underscored the systemic vulnerability of the traditional banking system and its lack of transparency, which undermined public confidence in the banking institutions as a whole[113]. In such an environment, cryptoassets emerged as viable alternatives offering decentralised and independent financial assets, relatively immune from the systemic risks commonly present in traditional banking. [114]Consequently, investors and the public increasingly turned to cryptoassets to diversify risk and safeguard against future financial disruptions.

---

[111] *Ibid*, 12.
[112] Mendeng above, n(81), 7..
[113] Umit Hacioglu, *Blockchain Economics and Financial Market Innovation: Financial Innovations in the Digital Age* (Springer 2019).
[114] *Ibid*.

The complex nature of the technology on which cryptoassets are built has a knock-on effect that magnifies the exclusion of individual users.[115] Most of the individual users end up failing to access the potential financial opportunities that exist in the markets. Most of the attempts to avail bitcoin to the average user have led to degradation of the usability of the cryptoassets, considering the limited trust levels between the parties to any transaction. This has contributed to the emergence of novel cryptoassets, most of which are designed to seal the flaws in bitcoin, as discussed hereunder.

4.4.3 Probability of Emergence of More Superior Cryptoassets

The dynamic nature of technology has proven that it is possible for the emergence of more superior cryptoassets. The most common improvements registered are aimed at overcoming the technical, social and environmental limitations in the existing cryptoassets. For instance, most of the early crypto-assets are designed without options for upgrading.[116] The dynamic nature of software and hardware technologies implies that crypto-assets such as bitcoin face inherent risks of becoming outdated or exposure to certain vulnerabilities due to the lack of mechanisms for upgrading.

The emergence of initial coin offerings (ICO) was an innovation in the crypto-assets markets place, whereby entrepreneurs could benefit by investing in new 'cryptoassets.' By funding the creation of crypto-assets, ICOs have been deployed for crowdfunding purposes to enable software developers to create cryptoassets that fit into the suitability criteria of a specific market. Entrepreneurs benefit from the allotment of tokens, which can be held for future value or sold in the open market at a mark-up. The proceeds from ICOs have been used for a multiplicity of purposes, including as capital for start-ups. The ICO market is described as decentralised, unregulated and disintermediated.[117] In 2018, over US$11.4B was raised through 2284 ICOs, 80% of which were later identified as scams, with only 8% of the ICOs surviving the trading phase on crypto exchanges.[118]

Evidence from across the globe reveals that in addition to the plans for current and future regulation, most countries and regions are considering investing in and launching cryptoassets that

[115] Nelson n(20)
[116] Howden n(12), 12.
[117] P Andres, and others, 'Regulatory and Market Challenges of Initial Coin Offerings' (2019) 79 International review of financial analysis, who indicated that this innovation is not insulated against the challenges facing cryptoassets
[118] Nelson n(20), 7.

are designed to fit the environment in which they operate.[119] The central banks in countries where cryptoassets are used aimed to seal the loopholes in cryptoassets, thereby mitigating the risks of misuse for ML/TF activities.

4.4.4 The Institutions Involved in Regulation

The multiplicity of operations associated with cryptoassets presents a unique set of challenges that increase the potential for online fraud.[120] In most cases, fraudulent activities are magnified by the disparity in the type of institutions involved in the oversight of the crypto markets. Most of the governments that have placed some form of restrictions on cryptoassets do so through the regulatory institutions that participate in oversight of institutions under the traditional financial sector. These include the central banks, institutions involved in oversight of banks and consumer/investor protection institutions.[121] The involvement of specialised task forces and committees has appealed to most jurisdictions since these taskforces have a broader mandate than the institution from which they are drawn.[122] The introduction of institutions such as FATF diversifies the source of inputs for the regulatory frameworks and policies specific to cryptoassets. By drawing on the inputs of professionals from different backgrounds, these institutions provide a more balanced and inclusive framework that is cognisant of the technical aspects of cryptoassets at any point in time.

The discussion presented above is an extensive answer to the second and the third research sub-questions the project is supposed to address, namely how the UN and the FATF are attempting to regulate cryptoassets. The material presented above shows that international institutions are still reactive to the growing popularity of cryptoassets and have failed to produce an effective means for their regulations. In fact, there are even debates on whether cryptoassets should be regulated by domestic and international regulatory institutions, which further highlights that the understanding of how cryptoassets are to be regulated has not advanced much. Neither the UN nor the FATF has produced a robust regime to facilitate the regulation of cryptoassets, which further highlights the numerous regulatory challenges that the relevant institutions face in their attempt to prevent terrorism financing.

[119] Estonia has plans to introduce Estcoin.
[120] I Kfir 'Cryptoassets, national security, crime and terrorism', (2020) 39 Comparative Strategy, 113
[121] O Marian n(4), 59. Sonderegger n(3), 200.
[122] Brookes, n(4)

4.5 The Cryptoassets Standards Applied in Bahrain

The country views cryptoassets as an avenue through which it can attract investors and foreign capital. Its regulatory appetite is, however, closely influenced by the opinion of some market participants who view cryptoassets as risky instruments in comparison with other instruments under the financial system. This perception has influenced the extent to which the country regulates cryptoassets. The 2006 Report, '*Financial System Stability Assessment,*'[123] concluded that despite the stability in the financial sector, exposures were originating from the actions of the regional economies. Similarly, the robust nature of the prudential regulations, specifically the modernised and comprehensive oversight mechanisms, was effective. However, there were gaps in the oversight and monitoring activities, specifically those related to the growing and sophisticated financial institutions in the sector.[124]

4.5.1 Institutions Involved: Central Bank of Bahrain

An analysis of the regulatory mechanisms in Bahrain reveals that issuers, traders and investors of cryptoassets are faced with an ambiguous regulatory regime in Bahrain.[125] Unlike other Middle Eastern countries, Bahrain has rapidly expanded the regulatory framework for cryptoassets. In 2017, the Central Bank of Bahrain introduced a Financial Technology Bay[126] and a regulatory sandbox[127] for start-ups in the crypto-assets market. As the first country in the Middle East to adopt such an approach, this regulatory strategy is driven by the fact that Bahrain seeks to establish itself as the crypto market hub in the GCC. Concerning the technology bay and regulatory sandbox, Abdeldayem and Aldulaimi stated:

> "Bahrain and Abu Dhabi are dashing to turn into the Gulf locale's driving centre point for cryptographic forms of money, decentralized computerized monetary forms that use blockchain records. Both have created digital currency administrative structures,

[123] IMF, 'Kingdom of Bahrain: Financial System Stability Assessment,' (IMF, 2006).
[124] Siswantoro and others n(76), 15.
[125] C Gunson, and B Altymulkamedov, *Crypto Asset Exchanges in the Middle East: Kingdom of Bahrain and the Abu Dhabi Global Market* (AMG, 2019)
[126] A financial technology ecosystem created through the collaboration of Singapore's Financial technology consortium and Bahrain's Economic Development Board
[127] E Prasad, 'Central Banking in a Digital Age: Stock-Taking and Preliminary Thoughts. (2018) https://www.brookings.edu/wp-content/uploads/2018/04/es_20180416_digitalcurrencies.pdf accessed 22 February 2022 who indicated that the regulatory sandbox is designed to help startups in the financial technology sector with the necessary opportunities to evaluate and experiment with different ideas, mostly related to the cryptoassets market.

authorized cryptographic money trades and businesses and put resources into digital money related to new companies."[128]

Despite the implicit ban imposed in 2017,[129] Bahrain became the first country in the region to publish a regulatory framework for cryptoassets in 2019. The Directive[130] provides guidelines on compliance, licensing, governance, capital, risk mitigation and securitisation concerning all crypto asset services. Two factors influence the extent to which Bahrain regulates the crypto market. First, in line with Islamic finance guidelines, the volatile nature of cryptoassets makes them an unreliable alternative to money.[131] Similarly, since Islamic finance only considers physical assets as money, the adoption of cryptoassets as money or assets is considered antithetical to the underlying principles. In some instances, cryptoassets are banned under Islamic law, primarily because their use is associated with unethical activities on the Dark Net. Under the new guidelines, licensing[132] is mandatory for all the regulated crypto asset services. However, the country has streamlined the process through which institutions are involved in the crypto market by offering low licence fees, estimated at US$200,000.[133] Bahrain is also a signatory to some of the treaties under the UN.[134] However, since it has not ratified a number of the treaties on human rights and democratic governance, it is not able to deploy some of the provisions under agencies that base their regulatory principles on human rights.[135]

4.5.2 The Bahrain Financial Technology (FINTECH) Sector

The FinTech sector in Bahrain is modelled around the Islamic FinTech sector, which is widely utilised in the Gulf Region.[136] The combination of the principles of Islamic finance, emergent technology such as blockchain, and Sharia law presents a complex monitoring and compliance

[128] Abdeldayem and Aldulaimi (n) 2, 17,
[129] Prasad n(128)
[130] The Central Bank of Bahrain works hand in hand with the Ministry of Industry, Commerce and Tourism
[131] Siswantoro n(75), 6.
[132] All applicants for a regulated crypto asset service license have to pay a non-refundable application fee of BHD 100, with an annual renewable fee equal to 0.25% of the annual operating expenses.
[133] Abdeldayem and Aldulaimi n(2)
[134] See Cyrille n(33) at 5
[135] United Kingdom: Foreign and Commonwealth Office, *Human Rights and Democracy Report 2017 - Bahrain*, (UNFCO, 2018) which indicates that Bahrain has failed to implement a number of human rights policies under the UN Charter, such as the 1954 and 1961 UN Conventions on Statelessness. Although this is not an indicator of its abilities to regulate the crypto market, it shows an inability by the government to standardize the protections for its citizens and financial system.
[136] M R Rabbani, S Khan and E I Thalassinos, 'FinTech, Block chain and Islamic Finance: An Extensive Literature Review, (2020). 8, Int. J. Econ. And Bus. Adm, 65.

regime that presents both opportunities and challenges. Rather than being competitors to Islamic financial institutions, these FinTech entities are treated as partners since they facilitate the achievement of the goals of the financial systems. However, due to the disparities in the penetration and adoption of technology among Gulf countries, Bahrain has found itself serving as more of a hub for FinTech in the region. A report by the Milken Institute[137] reveals that Bahrain's FinTech industry developed from the introduction of electronic funds transfer systems in 2015. In 2018, the Central Bank of Bahrain provided the first draft guidelines for platform operators for cryptoassets, with a focus primarily on supervision and licensing. Due to the increased adoption of technology in the financial sector, particularly in the banking sector, the benefits of instruments such as cryptoassets are viewed as exceeding the risks.

Furthermore, the involvement of banking institutions in the cryptoassets markets is driven by the perceived convenience of the assets as compared to other instruments. These circumstances have led to the increased propensity of financial sector institutions in Bahrain to partner with institutions from Singapore under the Singapore Fintech Consortium.[138] The partnerships have reinforced the ability of Bahrain to implement sandboxing strategies to enhance the capacity for the use of cryptoassets. The partnerships further explain the trajectory for the characteristics of the regulatory and monitoring framework for crypto in the country relative to that of other Gulf countries. Over time, Bahrain has modelled its regulatory and operational framework to certain standards from the West, including agility, aggressiveness and competitiveness.[139]

4.5.3 FATF Standards in Bahrain

The adoption of the FATF guidelines in 2018 has enhanced the risk-based approach to the regulation of cryptoassets in the country. Before the adoption of FATF standards in Bahrain, the country relied on a multifaceted regulatory framework that included ML guidelines.[140] Based on the decisions by the Shura Council,[141] citizens of the country are banned from using cryptoassets

[137] Milken Institute, 'Developing Bahrain and the UAE into FinTech Hubs'. (2019) < https://milkeninstitute.org/sites/default/files/2019-10/Developing%20Bahrain%20and%20the%20UAE%20into%20FinTech%20Hubs%20-%20A%20Timeline%20of%20Activity_FINAL.pdf> accessed 20 February 2022
[138] See Milken Institute, n(139)
[139] Rabbani and others (138)
[140] Under Decree Law 4/2001, which was developed by the Anti-Money Laundering Unit (AMLU), focused on ML offenses that included actions related to property, and focused on the persons who committed the offenses.
[141] *Ibid.*

domestically, but there are no limitations to investing or using the currency outside. The decision is based on the realisation that other countries have better regulatory frameworks regarding cryptoassets, and those regulatory frameworks create opportunities that the Bahrainis can exploit. This risk transfer approach serves to insulate the country against risks.

However, the process of ratifying the FATF standards is sub-optimal due to the limitations in legal basis and political goodwill. This explains the rationale for the performance of the country as shown hereunder. The assessment by FATF[142] reveals that Bahrain attained moderate effectiveness in the primary goals of regulating the ML/TF in 2018, as shown in Table 1 hereunder.[143] Considering that cryptoassets magnify the ML/TF risks that are normally associated with traditional financial items, it is apparent that the introduction of cryptoassets into its market is bound to amplify the potential risks associated with the crypto market.

Table 1: Effectiveness of FATF Policies in Bahrain

Outcomes	Effectiveness Rating[144]
Risk, policy and coordination	Moderate
International cooperation	Substantial
Supervision	Substantial
Preventive measures	Moderate
Legal persons and arrangements	Moderate
Use of financial intelligence	Substantial
ML Investigations and prosecutions	Moderate
Confiscation	Moderate
TF investigations and prosecution	Moderate
TF Preventive measures and financial sanctions	Moderate
PF financial sanctions	Moderate

[142] FATF-MENAFATF, 'Anti-Money Laundering and Counter-Terrorist Financing Measure-Bahrain. Fourth Round Mutual Evaluation Report (FATF, 2018)
[143] *Ibid.*
[144] The effectiveness ratings range from high, substantial, moderate and low.

A review of the level of compliance under the FAFT standards that culminate into the outcomes discussed above is provided hereunder. Although the standards are established to cover risks associated with traditional financial instruments, a review of the literature[145] reveals that the diversity of cryptoassets available within and outside Bahrain can and has been used as a complement and supplement to these financial instruments. This is why the level of technical compliance in the various standards is an indicator of the extent to which the AML/CTF policies serve to mitigate the risks against cryptoassets. The level of compliance among the 40 standards varies extensively, with the country achieving 'a largely compliant' level in 26 of the 40 standards. Bahrain has only achieved full compliance in 8 out of the 40 standards. From a qualitative perspective, the country has a long way to go to achieve comprehensive reforms since it is keen on adhering to the standards within the international frameworks and is an adopter of cryptoassets.

Table 2: Level of Technical Compliance with the FATF Standards

Standard	Level of Technical compliance[146]
Assessing risk and applying a risk-based approach	Partially compliant
National cooperation and coordination	Largely compliant
Money Laundering Offence	Largely compliant
Confiscation and provisional measures	Compliant
Terrorist financing offence	Partially compliant
Targeted financial sanctions, terrorism and terrorist financing	Partially compliant
Targeted financial sanctions-Proliferation	Partially compliant
Non-profit organisations	Largely compliant
Financial institution secrecy law	Compliant

[145] A H A Othman and others 'The impact of Cryptoassets market development on banks' deposits variability in the GCC region' (2019) 12 Journal of Financial Economic Policy, (2019),161 and S Alam, and H Noor, 'Mined and Non-Mined Crypto Currencies: A Critical Analysis from Shariah Perspective (2020) 5, Int. Journ, Inn. Sci and Res Tech. 3, 1.

[146] The level of technical compliance ranges from C-Compliant, LC-Largely Compliant, PC-Partially compliant and NC-Non-compliant.

Customer due diligence	Largely compliant
Record keeping	Compliant
Politically exposed persons	Largely compliant
Correspondent banking	Largely compliant
Money or value transfer services	Largely compliant
New technologies	Compliant
Wire transfers	Largely compliant
Reliance on third parties	Compliant
Internal controls and foreign branches and subsidiaries	Largely compliant
Higher risk countries	Largely compliant
Reporting of suspicious transactions	Largely compliant
Tipping-off and confidentiality	Largely compliant
DNFBPs[147]: Customer due diligence	Partially compliant
DNFBPs: Other measures	Partially compliant
Transparency & BO of legal persons	Largely compliant
Transparency & BO of legal arrangements	Largely compliant
Regulation and supervision of financial institutions	Largely compliant
Powers of Supervision	Largely compliant
Regulation and supervision of DNFBPs	Largely compliant
Financial intelligence units	Compliant
Responsibilities of law enforcement and investigative authorities	Compliant
Powers of law enforcement and investigative authorities	Compliant
Cash couriers	Largely compliant
Statistics	Largely compliant

[147] Designated Non-Financial Business and Professions.

Guidance and feedback	Largely compliant
Sanctions	Largely compliant
International instruments	Largely compliant
Mutual legal assistance	Largely compliant
Mutual legal assistance, freezing and confiscation	Largely compliant
Extradition	Largely compliant
Other forms of international cooperation	Largely compliant

The difference between the level of compliance with the proposed interventions and the effectiveness of the measures based on the risk concerns relating to cryptoassets in Bahrain can be attributed to several reasons. First, Bahrain has a weak history concerning counter-terrorism measures.[148] Since it has been shielded from the effects of terrorism, in comparison with other countries such as the UK and the US, the country has not experienced sufficient exposure to its systems to warrant implementing the legal and monitoring frameworks, most of which are adopted based on the existence of a need.[149] Second, Bahrain is more of an adopter of cryptoassets, rather than an inventor or creator. As compared to other countries that create these cryptoassets and hence need to establish legal and regulatory frameworks,[150] Bahrain relies on the technologies and cryptoassets that have been created elsewhere. By relying on these innovations from other countries, Bahrain has found it viable to rely on the input from the creators of these cryptoassets since the frameworks are found to be viable. Finally, Bahrain, unlike some Middle Eastern countries, has elected to modernise its systems in line with strategies from the West. Its trajectory for modernisation bears semblance to Western civilisation, even though it has retained its identity as a Gulf country. Evidence of this trajectory for modernisation includes the adoption of most elements of international law, which predispose a country to align its legal frameworks with other

[148] Legislative decree No 4 (2001) (Bahrain), which is amended by Law (25, 54 and 36, as well as Law No 58 of 2004 define terror finance as "(Illicit transfer of property across borders): A criminal act committed by any natural or legal person by any means, directly or indirectly, by the transfer of property across international borders, in case of not disclosed in violation of the public policy or if the transfer of property for the purpose of money-laundering or terrorism financing".

[149] A Almutawa, 'Terrorism Measures in Bahrain: Proportionality and the Interplay between Security, Civil Liberties and Political Stability. (2018). 22 The International Journal of Human Rights, 949.

[150] Brookes, n(4)

countries across the globe.[151] The adoption and implementation of these international legal frameworks have opened up certain systems in Bahrain to the globe, including the financial, educational, health, trade and commerce.[152] The discussion provided in this section provides an important background on the Bahraini government's approach towards the regulation of cryptocurrencies, which will be further examined in the subsequent chapters of the study. Nonetheless, the discussion provided heretofore has been helpful for addressing the last sub-question that this chapter is aiming to address, namely how the Bahraini government is approaching the regulation of cryptoassets and what are the foundational principles that influence that regulation In the next section, a review of the successes of the UK in applying the Cryptoassets is discussed so that the reader can identify how the principles surrounding the cryptocurrency regulation differ in the UK and Bahraini context.

4.6 The Cryptoassets Standards Applied in the UK

According to the BoE and the Financial Services Board (FSB), the preliminary review and position are that the risks posed by cryptoassets to the stability of the global financial sector are negligible due to the limited scope of their use.[153] In the same period, the Cryptoassets Task Force highlighted the imperativeness of awareness of the risks associated with cryptoassets. This warning, directed to consumers across the UK, was reiterated by a Treasury Select Committee,[154] which advised consumers to approach the acquisition, ownership and use of crypto-assets with a high degree of caution.[155] Despite this view, the UK has taken steps to shield itself against these minimalist risks because crypto-assets present unique risks under the ML/CT domains.

4.6.1 Institutions Involved

The UK does not have a unified legislative framework for regulating the use of cryptoassets. The decision to adopt a restrained 'wait-and-see' approach in regulating cryptoassets is attributable to the conclusions by the Bank of England that crypto-assets do not serve as money[156] or commodities. To achieve these goals, a multiplicity of regulatory institutions participate in the

[151] Almutawa, n(151), 952.
[152] Gunson and Altymulkamedov, n (126).
[153] M Dabrowski, and L Janikowski, 'Virtual Currencies and their Potential Impact on Financial Markets and Monetary Policy'. (2018) https://case-research.eu/files/?id_plik=5708 accessed 10 November 2024
[154] House of Commons, n(13)
[155] *Ibid.*
[156] House of Commons, 'Cryptoassets-Twenty-Second Report of Session 2017-19' (House of Commons: 2019).

development and oversight of cryptoassets in the UK, which is attributed to the fact that the country has involved several institutions that were previously involved in the regulation of the traditional financial system.

4.6.1.1 The Financial Conduct Authority (FCA)

The FCA is charged with the duty of regulating financial services to protect consumers.[157] The FCA has engaged in consultations on the development of guidelines for cryptoassets to provide clarity on the most suitable approaches for the various market participants. Based on the recommendations of the FCA, the HM Treasury develops the basis for legislative changes that expand the authority of the FCA concerning the regulation of cryptoassets. Past consultations by the FCA have culminated in the following outcomes. First, the FCA has defined and categorised Cryptoassets into three categories.[158] Second, the FCA has established a criterion for measuring success in its regulatory mandate while providing frequent updates based on its consultative activities in its most recent reports. The activities of the FCA have also laid down the foundation for the expansion of research into cryptoassets; the case in point is the fact that in six months, it reviewed its regulatory perimeter by increasing the range of entities under its purview.[159] To enhance its oversight activities, the FCA expanded its purview to include firms classified as financial advisers, as per the July 2019 Report. Finally, the inclusion of Financial Advisers in the more recent report highlights the expansion of the mandate of the FCA and points towards the possibility of increased oversight efficiency under this institution. This includes annual consumer surveys sandboxing working with consortiums[160] and consumer hubs that provide real-time feedback to interested parties.[161]

4.6.1.2 The Bank of England (BoE)

The BoE has been involved in a multiplicity of projects, including data-sharing initiatives such as the Digital Competition Expert Panel.[162] In response, the BoE developed a methodology for

[157] J Truby, 'Fintech and the city: Sandbox 2.0 policy and regulatory reform proposals' (2020) 34 Int. Rev. of Law, Comp. & Tech., The FCA's mandate is to protect consumers from harm, protect and enhance the integrity of the UK's financial services sector, and promote effective competition in the interest of consumers.
[158] FCA, n(9)
[159] *Ibid.* .
[160] Braddick and others n(50)
[161] FCA, n(9)
[162] Deutsche Bank, *Regulation Driving Banking Transformation* (Deutsche Bank 2019), the Export Panel seeks to rely on data to promote strategies designed for supporting digital innovations and understanding the market structure.

introducing Central Bank Digital Currencies (CBDC), which are part of the second-generation cryptoassets.[163] The involvement of BoE in the creation of CBDC is subject to the development of the right infrastructure to ensure that the functional value of the CBDC, including as a unit of account, a store of value and a medium of exchange, is reasonable, as a comparison to other traditional forms of money.

4.6.1.3 HM Treasury

The cryptoassets Taskforce outlined the UK policy towards the regulation of crypto-assets and other financial instruments and services that are developed using DLT.[164] Its broad mandate enables the regulatory objectives of the UK to include the explicit risks and implicit benefits while establishing a pathway for regulation and promotion of the technologies and products associated with cryptoassets. The involvement of the HM Treasury has led to the integration of the financial technology sector strategy, which was developed in conjunction with the BoE and FCA. The first report from the Taskforce included input from stakeholders in different industries, much like the FCA report cited earlier.

4.6.2 The Specific Standards in Place in the UK

The UK has a robust legal system that is developed with a broad-based appreciation of the risks arising from the exploitation of loopholes. As a pioneer in the AML/CTF policies utilised under the EU, UN and other multinational entities, the UK has played an integral role in the creation of frameworks for coordinating and cooperating to prevent ML/TF, domestically, regionally (EU) and globally. As a result, even before the emergence of the threat posed by cryptoassets, the standards in place were primed to achieve most of the current goals, including:

- Maintain the international reputation of the UK as a safe, secure and transparent environment for financial services,
- Establishing advanced standards for regulation of its financial markets, thereby maintaining the integrity of its financial sector,
- Protecting the domestic and international consumers from any forms of exposure,
- Guarding against the threats to the current and future financial stability of the country and

[163] Bank of England, 'Central Bank Digital Currency: Opportunities, Challenges and Design. (Bank of England, 2020).
[164] Braddick and others n(51)

- Promoting innovations in the financial technology sector to create a favourable playing field for all parties.

The UK is one of the most proactive jurisdictions when it comes to the investigation, prosecution and conviction of parties involved in a multiplicity of activities associated with the creation, ownership and use of cryptoassets.[165] The institutionalisation of the TFC under the Office of Financial Sanctions Implementation enables the UK to design robust penalties for those who breach the established policies and regulations. The objectives of the standards in the UK vary, depending on the dimensions of the crypto-asset industry targeted. First, the UK engages in financial analysis and intelligence[166] as part of the framework for overseeing and managing its involvement in the global financial systems.

4.6.2.1 AML Frameworks and Cryptoassets in the UK

The UK relies on the input of the FCA in designing frameworks and AML obligations for all institutions. Through its progressive approach, the FCA has provided a risk-based framework for the mitigation of financial crimes associated with the handling of cryptoassets. Although the UK has withdrawn from the European Union, it is cognizant of the integral nature of the AML directives under the EU, and it remains committed to adopting the fifth AML Directive, which includes the following provisions specific to cryptoassets. However, these EU-based provisions are adopted as complementary measures to the domestic AML frameworks.[167]

- Exchange services that feature multiple cryptoassets to prevent the layering of funds to disguise their anonymous origins
- Regulation of platforms that expedite the exchange of cryptoassets anonymously to prevent the unmonitored transfer of funds from one party to another.
- Cryptoasset automatic teller machines to regulate the anonymous acquisition of cryptoassets
- Non-custodian wallet providers who expedite the anonymous transfer and storage of cryptoassets.

[165] FCA n(9)
[166] *Ibid.*
[167] *Ibid.*

4.6.3 Performance under the Current FATF Standards in the UK

The performance of the UK under the current FATF standards is provided in Table 3 below. The country has achieved optimal compliance in 23 out of the 40 standards, which can be interpreted as a sufficient level of performance concerning mitigation of the risks associated with cryptoassets. A granular review of the weaknesses in compliance reveals that the UK lacks a robust risk-based approach in its AML/CTF policies,[168] which raises concerns that the introduction of cryptoassets will magnify the risk profiles of other financial instruments. The compliance challenges under this domain can be linked to the weaknesses in the establishment of sanctions targeted against TF activities and the proliferation of such activities, customer due diligence, the risk associated with correspondence banking, emergent technologies and exogenous risks.[169] These weaknesses are highlighted by the fact that although there is a harmonised AML/CTF policy under the CT legal frameworks discussed in section 1.2, the adoption and implementation of the policies differ from one country to another. As a result, exogenous risks present a challenge to countries that have reliable internal policies.

Table 3: Level of Technical Compliance with the FATF Standards

Standard	Level of Technical compliance[170]
Assessing risk and applying a risk-based approach	Largely compliant
National cooperation and coordination	Compliant
Money Laundering Offence	Compliant
Confiscation and provisional measures	Compliant
Terrorist financing offence	Compliant
Targeted financial sanctions, terrorism and terrorist financing	Largely compliant
Targeted financial sanctions-Proliferation	Largely Compliant

[168] FATF, 'Anti-Money Laundering and Counter-terrorist Financing Measures: United Kingdom-Mutual Evaluation Report' (FAT: 2018).
[169] Exogenous risks are associated with third party countries, foreign financial institutions and their subsidiaries and operations in countries with high risks.
[170] The level of technical compliance ranges from C-Compliant, LC-Largely Compliant, PC-Partially compliant and NC-Non-compliant.

Non-profit organisations	Compliant
Financial institution secrecy law	Compliant
Customer due diligence	Largely compliant
Record keeping	Compliant
Politically exposed persons	Compliant
Correspondent banking	Partially compliant
Money or value transfer services	Compliant
New technologies	Largely Compliant
Wire transfers	Compliant
Reliance on third parties	Largely compliant
Internal controls and foreign branches and subsidiaries	Largely compliant
Higher risk countries	Largely compliant
Reporting of suspicious transactions	Compliant
Tipping-off and confidentiality	Compliant
DNFBPs[171]: Customer due diligence	Largely compliant
DNFBPs: Other measures	Largely compliant
Transparency & BO[172] of legal persons	Largely compliant
Transparency & BO of legal arrangements	Compliant
Regulation and supervision of financial institutions	Compliant
Powers of Supervision	Compliant
Regulation and supervision of DNFBPs	Compliant
Financial intelligence units	Partially compliant
Responsibilities of law enforcement and investigative authorities	Compliant

[171] Designated Non-Financial Business and Professions.
[172] Beneficial ownership.

Powers of law enforcement and investigative authorities	Compliant
Cash couriers	Largely compliant
Statistics	Largely compliant
Guidance and feedback	Compliant
Sanctions	Compliant
International instruments	Compliant
Mutual legal assistance	Largely compliant
Mutual legal assistance, freezing and confiscation	Compliant
Extradition	Compliant
Other forms of international cooperation	Largely compliant

The purpose of the above discussion was to identify the main factors affecting the regulation of cryptocurrencies in the UK. The UK's approach to regulating cryptoassets involves multiple institutions, such as the Financial Conduct Authority (FCA), Bank of England (BoE), and HM Treasury, each playing distinct roles. While the Bank of England has downplayed the current risks posed by cryptoassets, the UK remains vigilant, with a focus on preventing money laundering and countering terrorist financing (ML/CTF). The UK has robust legal standards in place for AML/CTF, influenced by both domestic frameworks and EU directives, and continues to adjust its policies in response to the evolving cryptoasset landscape despite gaps in certain risk-based approaches. The discussion presented in this chapter above has addressed the last sub-questions the chapter aimed to address, which was to examine how approaches towards cryptocurrency regulation were implemented in the United Kingdom.

4.7 Propositions for Improvements on the Legislation.

The differences in the level of adoption of the propositions by domestic and international AML/CTF frameworks justify the need for improvements in the existing literature. As discussed, the link between national security and economics concerning Cryptoassets arises from the emergence of illicit financing typologies that facilitate the manipulation of markets, fraudulent activities, and the utilisation of virtual schemes to layer transactions and hide the origin and

destination of funds. These decisions are based on the propositions by umbrella entities such as the FATF, which rely on propositions by regional institutions such as the EU. However, past studies have provided empirical and theoretical evidence that most of these regulatory and legislative frameworks have achieved a suboptimal and negligible level of success.[173] This is contained in the SRAR[174], implying that most of the propositions by the regulatory institutions are not implemented effectively.

Second, the regulation should focus on the ideology of equality in contribution based on the principle of similar services, similar risks, similar rules and similar supervisory structures. This will enable the two countries to overcome the choice and constraint problems identified in chapter/section 1.4. Through the principle of neutrality in the regulation, specifically related to different business models and technological innovations. The principle should also limit regulatory arbitrage,[175], to promote integrity in the financial system. The involvement of different entities in regulating cryptoassets is justified due to the differences in their definitions, types, and functions across various jurisdictions. However, one of the categories of entities that have been lacking in participation is standard-setting organisations. The rapid globalisation of the use of Cryptoassets, coupled with the increased propensity of nations to create their coins,[176] introduces the need for the establishment of guidelines on how and when a country should start regulating a cryptoasset.

Finally, the complex and dynamic nature of Cryptoassets in the various markets implies that each creation bears unique characteristics that may nullify some or all the existing provisions in the legal frameworks. There are propositions for the use of sandboxing mechanisms[177] to enable each or all jurisdictions to determine the practicality of the regulatory frameworks in the real market. Alternatively, as was done in the case of Bahrain, a country can partner with a crypto-friendly nation[178] in the process of developing a regulatory framework.

4.8 Conclusion

[173] R K Gordon, 'Losing the War Against Dirty Money: Rethinking Global Standards on Preventing Money Laundering and Terrorism Financing" (2010) 21 Duke J. Comp. & Int'l L, 148.
[174] Ibid
[175] A scenario where an entity capitalizes on the regulatory loopholes in one system, by circumventing the unfavourable regulations.
[176] Or to select particular coins.
[177] Huang and others, n(100)
[178] Nelson n(20),

The purpose of this chapter was to provide an analysis of the international and domestic frameworks that have been introduced for the regulation of cryptoassets and to prevent their growing use for the purposes of financing terrorist activities. The material presented heretofore indicates that there are notable omissions in the approaches used for cryptoassets regulation as neither the FATF nor the United Nations and the European Union have come forward with adequate regulation frameworks capable of addressing the risks that the cryptoassets pose for the financial sector. The principles that guide the cryptoassets regulation also do not pay sufficient attention to the risks that the cryptoassets are becoming the preferable asset of new terrorist organisations, especially in the Middle East. By providing an overview of the international legal regime on the regulation of cryptoassets, this chapter has addressed the second research question of the study, which was to identify the relevant international and national frameworks that regulate efforts against cryptocurrency use in terrorism financing in general, as well as in Bahrain and the UK. The next chapter will build upon the issues identified above by examining in greater detail how the Kingdom of Bahrain has attempted to regulate cryptocurrencies and what measures it has pursued to limit terrorist financing inside its own borders.

Chapter V: Kingdom Of Bahrain

5.1 Introduction

Digital currencies have provided a novel way through which value is created and transferred between individuals. It is also evident that criminals involved in money laundering (ML)) and/or terrorist groups involved in terrorist financing (TF)have a multiplicity of options, including recruitment of individuals into their network with the singular objective of achieving their goals.[1] The discussion herein seeks to identify ways laws are developed to combat terrorist financing. As discussed in Chapter One, cryptoassets facilitate the achievement of traditional TF activities while laying down the foundation for novel risks, such as raising donations through campaigns on social media. The anonymous nature of crytoassets, the ease with which they can be moved across borders, coupled with the complexity of oversight and regulation, has necessitated the utilisation of novel and multiple legislative approaches to achieve the risk-management objectives under counter-terrorism financing (CTF).

In this chapter, a typology of the legislative approaches relevant to CTF legislation is provided, with the accompanying definitions and objectives. The discussion focuses on Bahrain's legal framework, thereby highlighting the key institutions involved in CTF in the era of digital currencies. Specific focus is given to the Central Bank of Bahrain,[2] which provides the CBB Rulebook[3] to guide all legal and natural persons in the use of digital assets within and outside Bahrain to achieve the CTF legal requirements. Several legal frameworks are reviewed, including the laws that criminalise TF in Bahrain, as well as the CTF goals which they facilitate during the era of digital currencies. Due to the steps taken by Bahrain regarding the regulation and supervision of financial technology, the discussion herein focuses on the legislative approaches employed in the establishment of the sector, as well as the motivation for regulation of the sector through Regulatory Technology.[4] The discussion then highlights the legislative approaches which facilitate the establishment of 'Rain', the first cryptocurrency exchange in Bahrain, thereby

[1] E Esoimeme, 'Identifying and Reducing the Money Laundering Risks Posed by Individuals Who Have Been Unknowingly Recruited as Money Mules' (2020) 24, Journal of Money Laundering Control, 1, 205..
[2] Hereafter 'CBB'.
[3] The Central Bank of Bahrain and Financial Institutions Law. <https://www.cbb.gov.bh/wp-content/uploads/2018/12/THE_CENTRAL_BANK_OF_BAHRAIN_AND_FINANCIALINSTITUTIONS_LAW_ENGLISH.pdf > Accessed August 30 2021
[4] Hereinafter RegTech.

indicating the measures by Bahrain to safeguard itself from TF risks arising from the institutionalisation of the exchange of digital assets by service providers. Finally, the legislative approaches behind specialised institutions, including the financial intelligence units, and frameworks, such as the FATF, are discussed in-depth since they influence the decisions for supervision, regulation and oversight of virtual assets services providers.[5] A conclusion is provided regarding the legislative approaches for CTF in Bahrain during the digital currencies era. In doing so, the chapter addresses the following research sub-questions: 1) To what extent is Bahrain compliant or not with the FATF recommendations? 2) What is the model of regulation in Bahrain towards cryptocurrencies?

5.2 Legislative Approaches: A Critical Review

The determination of what a legislative approach is concerning a particular offence is determined by the extent to which the jurisdiction targets a deliberate and systematic approach to framing its legal and policy responses.[6] The jurisdiction also has to accommodate the entire spectrum of civil and criminal exposures present to ensure a holistic approach to achieving the punitive and preventive goals.

Studies on legislative approaches have utilised a multiplicity of methodologies, including those which focus on comparison across different countries and the investigation into legislation targeting different actions, with each methodology offering unique outcomes.[7] In identifying the legislative approaches utilised in Bahrain, the chapter recognises that ML/TF risks in virtual environments are qualitatively and quantitatively higher than those in offline environments.[8] The reduced possibility for detection and increased potential for anonymity implies that criminals and terrorist groups have increased motivations to utilise virtual platforms for ML/TF activities.[9]

In discussing the legislative approaches, the chapter will recognise the fact that criminals and terrorists perceive the virtual environment as both a compliment and supplement to the offline

[5] Hereinafter VASPs.
[6] J Ayling, 'Criminalising organisations: Towards Deliberative Lawmaking. (2011) 33 Law and Policy 2, 149.
[7] M R Solanes, 'Legislative Approaches to Drought Management', (1986) 10 Natural Resources Forum, 4, 373 and J Heymann, and others 'Legislative approaches to non-discrimination at work: A comparative analysis across 13 groups in 193 countries', (2021) 40 Equality, Diversity and Inclusion: An International Journal, 2, 225.
[8] A S Irwin, J Slay, and K R Choo, 'Money Laundering and Terrorism Financing in Virtual Environments: A Feasibility Study', (2014) 17 J of ML Contrl, 1, 50.
[9] R Coelho, M Simoni, and J Prenio, 'Suptech Applications for Anti-Money Laundering', FSI Insights on Policy Implementation No. 18. (2019) <https://www.bis.org/fsi/publ/insights18.pdf> accessed 19 August 2023

and contemporary ML/TF avenues that predate the digital era.[10] Similarly, the discussion of legislative approaches will take into account the fact that emergent and extant literature is still conflicted regarding actual risks and potential for the use of virtual platforms for ML/TF activities.

The legislative approaches discussed herein reveal that Bahrain has taken measures to achieve the tenets of the *aut dedere aut judicare* principle[11] by preventing terrorism and TF activities, prosecuting the perpetrators or extraditing perpetrators to a jurisdiction willing and capable of prosecuting them. Past studies on legislative processes culminate in the development of a framework for the critical assessment of legislative approaches within a particular jurisdiction, as shown hereunder.[12]

As shown in the figure hereunder, there are five key typologies of legislative approaches based on the actors involved in the process, the activities for which the legislation is developed, the objectives of the legislation, the structures targeted by the legislation and the impact of the legislation. Drawing from the five bases, thirteen legislative approaches are identified, with the objective of those approaches including deterrence (general and specific), punishment, prevention, community safety, promotion of innovation and reassurance. The legislative approaches entail the utilisation of the bases/levers to achieve the goals based on the nature of activities.

The discussion will highlight the extent to which the deployment of risk-based and rule-based approaches in combating ML/TF risks is done and achieved, which is fundamentally determined by the legislative approach adopted. The legislative approaches have led to the adoption of a rule-based[13] and risk-based approach[14] to AML/CTF in Bahrain. The rule-based approach eliminates the role of risk assessment as a tool for decision-making, thereby establishing baseline and benchmark standards for all industry players. On the other hand, the effectiveness of the risk-based approach is dependent on the quantification and qualification of risks, access to knowledge about the outcomes of the assessment, and agreement on what risks are being

[10] Ernst and Young, "Anti-Money Laundering in the Digital Era: Building trust and ethics in AI to combat fraud and economic crimes" (2020) < https://www.accaglobal.com/content/dam/ACCA_Global/professional-insights/PUBLIC_AFFAIRS/pi-anti-money-laundering-digital-age%20v2.pdf> accessed 19 August 2023
[11] Translates to extradite or prosecute.
[12] Ayling, n (6), 154.
[13] L De Koker 'Identifying and managing low money laundering risk: perspectives on FATF's risk-based guidance', (2009) 16 J of fin crime, 4, 338.
[14] D Chaikin, 'Risk-Based Approaches to Combating Financial Crime' (2009) 8, J of Law and Fin Mgmt 2, 19.

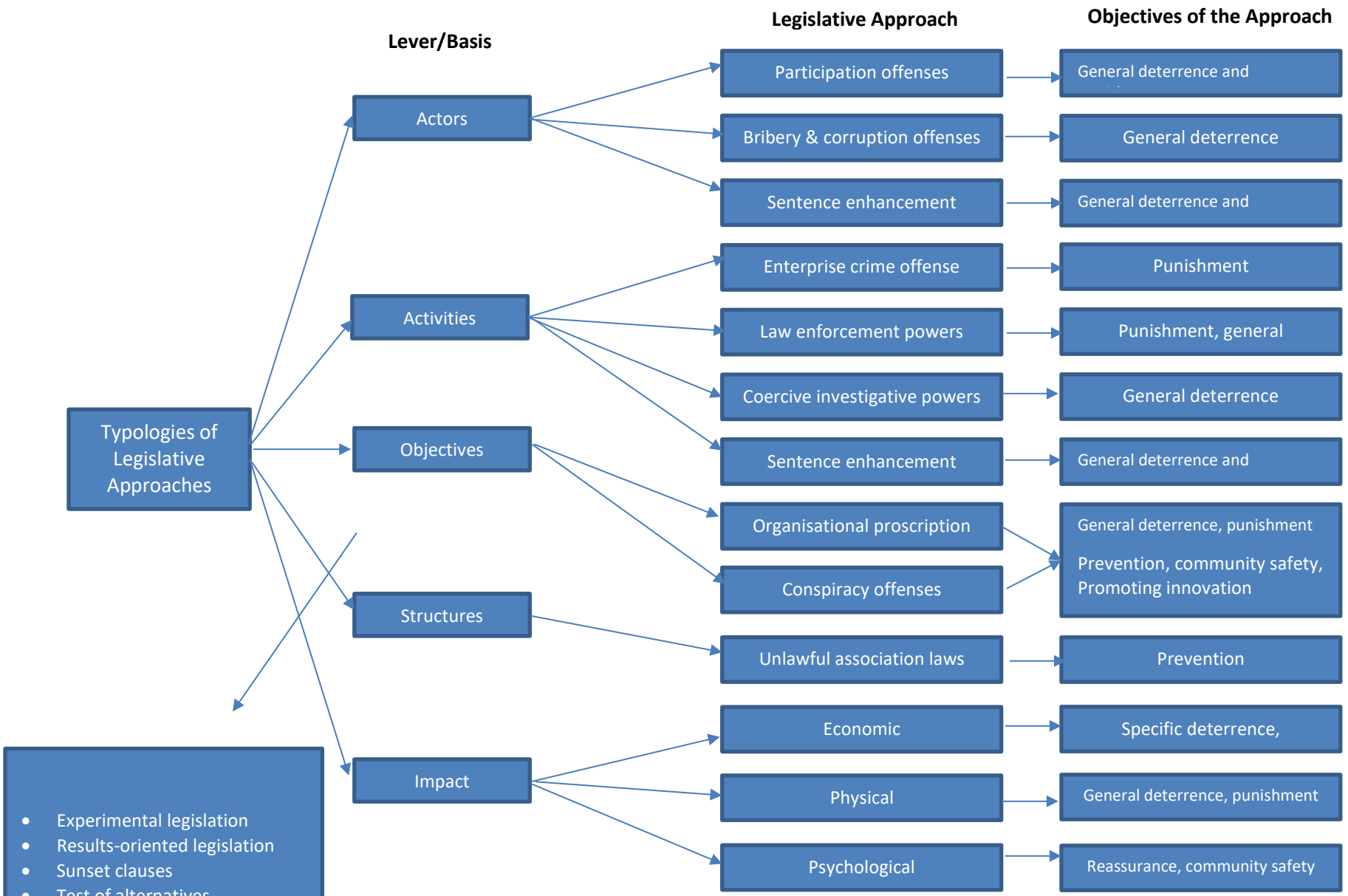
targeted.[15] Due to the transnational nature of the TF risks arising from digital assets, the multiplicity of traditional security approaches is insufficient to cover all potential concerns.

The legislative approaches discussed herein are identified on account of their *prima facie* ability to promote the rule of law and their legality within and outside the country, as well as the cross-border nature of the risks of TF in the era of digital currencies. The discussion hereunder also recognizes the fact that digital currencies provide criminals and terrorist financiers with a multiplicity of highly flexible approaches to achieving their objectives.

The figure presented below offers a structured overview of various legislative approaches on the basis or lever, including actors, activities, objectives, structures, and impact. Each category is linked to specific legislative measures, which in turn are connected to their intended objectives. Similarly, different activities, such as enterprise crime offences and law enforcement powers, are linked to either punishment or deterrence. This classification helps to visualize how different legislative strategies aim to address criminal behaviour and enforce legal accountability. The diagram also highlights the broader structural and impact-based aspects of legislative approaches. Organizational prescription and conspiracy offences are categorized under "Structures," with objectives ranging from deterrence to promoting innovation. Additionally, unlawful association laws are linked to prevention, signifying the role of legislation in mitigating risks before they escalate. The categorization presented in the figure further distinguishes economic, physical, and psychological effects, illustrating how laws influence not only criminal activity but also societal perceptions of safety and justice.

An important aspect of this figure is the inclusion of different legislative methodologies at the bottom left, such as experimental legislation, results-oriented legislation, and innovation-friendly legislation. These approaches suggest that legislative strategies are not static but can evolve through testing, adaptation, and refinement.

[15] S Ross, and M Hannan, 'Money laundering regulation and risk-based decision-making,' (2007) 10 J of Money Laundering Control, 1, 106.


Lever/Basis
Legislative Approach
Objectives of the Approach
Typologies of Legislative Approaches
Actors
Activities
Objectives
Structures
Impact
Participation offenses
Bribery & corruption offenses
Sentence enhancement
Enterprise crime offense
Law enforcement powers
Coercive investigative powers
Sentence enhancement
Organisational proscription
Conspiracy offenses
Unlawful association laws
Economic
Physical
Psychological
General deterrence and
General deterrence
General deterrence and
Punishment
Punishment, general
General deterrence
General deterrence and
General deterrence, punishment
Prevention, community safety, Promoting innovation
Prevention
Specific deterrence,
General deterrence, punishment
Reassurance, community safety
Experimental legislation
Results-oriented legislation
Sunset clauses
Test of alternatives
Top-runner approach
Pilot projects
Innovation-friendly legislation

5.3 Bahrain legal framework

The legal framework for Bahrain is designed to align the strategies, objectives, approaches and priorities of the AML/CTF practices with the international standards for verifying, reporting and investigating suspicious transactions. The most recent changes, such as those contained in Central Bank of Bahrain Vol 7,[1] are also motivated by the changing investment management industry, which calls for improvement in the regulatory regimes and processes. The introduction of collective investment undertakings[2] brought about the need for enhanced risk assessment, identification and mitigation.[3] The risks arise from the evolution of investment management tools, processes, products, and services, as well as the stakeholders involved since the country has become an investment hub for the region.

Empirical studies[4] point towards the fact that despite the multiplicity of threats facing the country, Bahrain has achieved significant success in preventing and responding to ML/TF threats. In one study,[5] the country was found to have achieved a significant qualitative and quantitative reduction in risks associated with ML between 2014 and 2015, including the number of suspicious transactions and the number of suspicious financial reports from different corporations. Under Article 37 of the constitution, Bahrain utilises the principle of direct implementation of international conventions. Under the Monist system, the direct effect is a principle that implies that countries have accepted that signatories to an international legal framework or treaty be bound to recognise and enforce any provisions within the legal framework without conditions or discretion.[6] Essentially, this system drives most countries to remain convergent towards international law by incorporating international law into national law without translation. The prioritisation of the desirability of the established formal

[1] CBB Vol 7 involves collective investment, as included in Appendix 3.
[2] Referred to as CIUs under the CBB Rulebook.
[3] C Muller J Suglia and B Liu, 'Evolving Investment Management Regulation: Light at the end of the Tunnel', (2013). https://assets.kpmg/content/dam/kpmg/pdf/2013/06/EIMR-Light-at-the-end-of-the-tunnel-2013-KPMG.pdf > accessed 23 February 2023 indicates that the 2012 changes were the third in 20 years (since 1992), following enhanced measures in 2007.
[4] M E Lokanan, and N Nasimi, 'The effectiveness of Anti-Money Laundering policies and procedures within the Banking Sector in Bahrain', (2019) 23 Journal of Money Laundering Control', 4, 769.
[5] *Ibid*., at 774.
[6] The direct effect is a principle which implies that countries have accepted that signatories to an international legal framework or treaty to be bound to recognize and enforce all provisions within the legal framework, without conditions or discretion.

international legal order influences the propensity of such countries to develop national laws.[7] Bahrain has recognised the role of corruption and governance-related problems in the ML/CT activities in the country.[8] A look at the governance system's periphery reveals that there are several domestic institutions, legal frameworks, corporate institutions and non-government institutions involved in the process. These entities play several key roles, including the following.

5.3.1 Customs Agency

The agency ensures that all transactions relating to trade, physical inflow or outflow of cash, and the transportation of valuables are transparent. The agency also monitors the movement of persons into and out of Bahrain, with a specific focus on high-risk individuals.[9] By operating at key entry points for goods and services into and outside of the country, the agency is responsible for the recognition and seizure of any products that are suspected or known to have been used for the generation of illegal finances and/or terrorism. The regulations[10] by the agency specifically relate to trade-based ML (TBML) while taking into account the TF exposures due to the risks and opportunities presented by digital currencies.[11] The customs agency operates under the integrated GCC custom laws, which were modelled around the objectives of the Customs Union of the GCC.[12] The agency deals with risk exposures for ML/TF[13] in the digital era, including the risks of payment for goods and services

[7] D A Telman, and A Jeremy, 'Monist Supremacy Clause and a Dualistic Supreme Court: The Status of Treaty Law as U.S. Law. Basic Concepts of Public International Law: Monism and Dualism' (Valparaiso University Legal Studies Research Paper No. 13-6 2013)

[8] Implementation Review Group, 'Review of Implementation of the United Nations Convention Against Corruption,' (2019) https://www.unodc.org/documents/treaties/UNCAC/WorkingGroups/ImplementationReviewGroup/17-18December2019/V1910900e.pdf. accessed 19 March 2022

[9] United States Department of State, "Investment climate statement –Bahrain", Bureau of Economic and Business Affairs, (2015) indicates that in 2019 placed sanctions upon specific individuals from the GCC regoion who were suspected of facilitating TF within and outside Bahrain. Although the individuals were not directly involved in TF using digital assets, they engaged in import and export activities that created value through goods and services, and their access to Bahrain presented a risk for engaging in predicate offenses that facilitate TF through digital currencies.

[10] Bahrain Customs Agency, 'Customs Affairs Strategy 2021-2024'. (2020). https://www.bahraincustoms.gov.bh/sites/default/files/202102/Customs_Affairs_Strategy_Handbook_2021_2024.pdf.> accessed 19 March 2022

[11] P Verdier, and M Versteeg, 'International Law in National Legal Systems: An Empirical Investigation', (2015) 109 The American Journal of International *Law*, 3 514.

[12] S B Alshammari, 'Impact of Customs Union Agreement on GCC Bilateral Trade, using Aggregated and Disaggregated Data' (2019) SAMA Working Paper, 19/11.

[13] Section 30 and 31 of the GCC Customs Law identifies illegalities, such as fraudulent custom declarations, failure to submit manifests, improper reporting and declaration of the weight, size, quantity and origin of freight.

in furtherance of terrorism financing goals between domestic and foreign persons or foreigners utilising the Bahraini trade environment for TF activities through digital assets.

5.3.2 Central Bank of Bahrain (CBB)

The activities of the CBB are outlined under the CBB Rulebook (see Appendix 3). The Rulebook outlines the supervisory, regulatory and oversight mandates of the CBB relating to institutions that are directly and indirectly involved in the financial sector. A diversity of legislative approaches is employed in the development of the rulebook, which relates to both conventional and Islamic financial products and services and, more recently, digital assets. The CBB operates with a Compliance Directorate,[14] which is mandated to ensure that all licensed entities adhere to the mandates for maintaining a license while complying with emergent directives. Through these mechanisms and the provisions under the CBB and Financial Institutions Law of 2006, the CBB acts as a 'gatekeeper' for screening and filtering transactions and operations to detect any risk due to failure to comply with the prevailing regulatory mandates. Similarly, the CBB has taken measures to integrate ML/TF risks as the primary financial crime under FC-A 1.3.[15] The legislative approaches adopted by the CBB reveal that the country is cognisant of the fact that there is a need for training of investigators who operate within the licensed financial services providers, as well as products and services designed with recognition of the need to detect the risks and exposures associated with TF when using digital assets. These include segmentation of the normal low-risk customers from those with high-risk exposure to TF, then applying commensurate risk-based approaches. In setting a regulatory perimeter for digital currencies, the CBB has focused on the following mechanisms.

5.3.2.1 Customer Due Diligence

The CBB rulebook[16] outlines the new procedures for CDD in response to the risks associated with the use of digital currencies, even though the objective remains the same: the identification of customers and the verification of that customer's identity.[17] The relevant

[14] Vol 1 of the CBB defines the Compliance Directorate as the "unit within the Agency responsible for verifying licensees' compliance with the requirements of the BMA Law, the AML Law, this Module and other BMA/CBB Regulations relating to terrorist financing and money laundering, and for collating and monitoring suspicious transaction reports from licensees".

[15] CBB Rule Book, *Financial Crime Module, Vol 2: Islamic Banks*, (CBB 2021), which provides updates to the section, which reorients the financial institutions offering Islamic banking products to consider financial crimes under the two key umbrellas of money laundering and terrorism financing. A similar change is included in CBB *Rule Book, Financial Crime Module, Vol 1: Conventional Banks* (CBB 2021), which relates to conventional banks.

[16] CBB Rule Book, *Financial Crime Module, Vol 1: Conventional Banks* (CBB, 2021) under FC-1.4.

[17] *Ibid.*

persons[18] implement CDD through simplified[19] or enhanced[20] methodologies. Similar provisions are outlined under the obligations of registered persons under Articles 3 and 5 of Ministerial Order No. 173 of 2017, as amended under Ministerial Order of 2018. The determination of which approach to use is dependent on the characteristics of the customers, the products/service/business model, the transactions and the fulfilment approach for the business operations. The CBB has changed some provisions regarding simplified CDD, while enhanced CDD is mandated for several specific persons. Firstly, politically exposed personnel (PEPs) who are under AML 1.5 under the CBB rulebook are treated as persons possessing high-risk exposures for TF. Secondly, targeted financial sanctions (TFS) are transactions that do not involve face-to-face interactions, transactions involving new technologies, and those associated with charities, societies, and clubs.[21] Thirdly, CRA- 7.1.3 mandates that licensed Crypto-asset Platform Operators[22] must use enhanced customer due diligence when onboarding new customers, including those who have been referred to the entity. The concerns regarding PEPs[23] are raised under the Penal Code Articles 190, 202 and 203, whereby public officials are not authorised to receive undue advantage on account of their positions since this predisposes them to risks that can be translated to TF activities by corrupt officials. For institutions at risk of TFs, Bahrain provides measures for freezing the assets without delay, considering that the digital assets are easy to move and utilise, especially for persons intending to engage in TF.

[18] Under Regulation CBB Rulebook Vol 1.4, relevant persons under the regulatory framework include persons acting in the process of business conducted within the Bahrain, including credit rating institutions, financial institutions, external accountants, auditors, tax advisers, trust/trust-service providers, casinos, high-value dealers, estate agents, independent legal agencies and insolvency practitioners.

[19] FC 1.11 under the CCB (n16) Simplified CDD is utilised where prior risk assessment has shown a low or negligible level of risk of ML/TF. CDD is thus carried out for the purpose of identifying the customer, without the need to verify their identity.

[20] *Ibid*, FC-1.1-1.10A defines enhanced CDD is carried out when there is a high risk for ML, such as when relating to a politically exposed individual, with the measures for CDD including subsequent information for identifying the customers, determining the source of wealth or funds, determination of the characteristics of the business relationship, determining the purpose of the transaction, and subjecting the customer to additional and sustained monitoring procedures.

[21] See FATF-MENAFATF, 'Anti-Money Laundering and Counter-terrorist Financing Measures for Kingdom of Bahrain: Mutual Evaluation Report' (FATF 2018), under Recommendation 6 and 7.

[22] Hereinafter 'CPOs'

[23] FATF, n(21)

5.3.2.2 Know Your Customer (KYC)

KYC guidelines in Bahrain are contained under the AML Law 2001.[24] The verification of identities is performed using the official documents provided by the government, depending on the status of the individual in the country.[25] In 2019, the Bahrain Information and eGovernment Authority (IGA) introduced electronic KYC (e-KYC) for financial institutions following the launch of the national digital identity platform. The cloud-based program, which is built around blockchain technology, facilitates the screening of customers without physical presence, authentication or documentation, whether domestically or internationally.[26] By basing it on blockchain technology, any entity that is required to perform KYC for a TF risk assessment before transacting with the client can be liable if such transactions end up aiding or abetting TF activities. The measure also acts as a deterrent as the cloak of anonymity that was previously assured for clients transacting through digital currencies has been lifted.[27] The novel Customer Identification Protocols implemented through e-KYC facilitate international cooperation for ongoing customer identification through the availability of digitised information about customers who deal with digital assets, as well as other pertinent information that can be utilised in risk assessment.

5.3.2.3 Suspicious Transaction Reporting (STR)

Volume 6 of the CBB Rulebook provides for STR under AML 4[28] and AML 6.[29] Similar provisions are included in FATF Recommendations 20 to enable licensees and other individuals to report any transactions that they deem suspicious.[30] Licensees under the CBB are mandated to provide Suspicious Transaction Reports (STRs)[31] to financial intelligence

---

[24] International Monetary Fund, 'Detailed Assessment of the Anti-Money Laundering and Combating the Financing of Terrorism' (2005) < https://www.imf.org/external/pubs/ft/scr/2007/cr07134.pdf> accessed 19 March 2022

[25] These include a valid passport, Iqama, a valid driver's license and a national identity card.

[26] N Youssef, 'Digital Customer On-Boarding, e-KYC and Digital Signatures in The Arab Region' (2020). https://www.amf.org.ae/sites/default/files/Files/Digital%20Identy%20Booklet.pdf Accessed 25August, 2021 indicated that Bahrain, through the Bahrain Electronic Network for Financial Transactions (BENEFIT), has designed and implemented a national electronic KYC utility that is based on blockchain technology.

[27] The assurance of anonymity for transactions using digital currencies is viewed as a motivator for engagement in TF activities, especially among individuals who wish to support the activities of terrorists without participating in attacks.

[28] FATF, n(21)

[29] CBB Rulebook, *Crypto-Asset Module: Central Bank of Bahrain Rule Book, Vol 6: Capital Markets*. (CBB 2019), CRA-7.1.5, which mandates that licensees MUST comply with the requirements for CDD, which lay the foundation for record keeping.

[30] Ibid.48. There was an increase in the STRs received by Bahrain FIU from 369 in 2012 to 4186 in 2017.

[31] SARs are designed for LEAs by providers of financial services for the purpose of alerting the LEAs about activities that constitute illegalities, or those with potential for culminating to ML/TF.

units (FIUs) to facilitate additional investigations. Under the elevated risks presented by digital assets, Bahrain mandates that those licensed as CPOs must maintain records of all transactions. Despite the anonymity provided by the digital assets, blockchain technologies are designed to provide transaction reports that are readily available to the users. The permanently fixed user offers a snapshot of all transactions, thereby providing licensees with the ability to determine which of the transactions is an outlier and then utilise enhanced CDD to determine the necessary response.

These legislative approaches associated with STRs serve several goals which are integrally linked to the risks associated with TF through digital assets. First, it limits the possibility of terror groups utilising traditional fiat-based transactions as a starting point for the acquisition of digital currencies that can then be utilised to finance terrorism.[32] Second, it establishes the basis for primary and secondary liability for institutions in the financial sector by mandating those entities to take the necessary risk mitigation and management measures for the prevention of TF, as well as acquisition and retention of records to determine criminal and civil liabilities for those who facilitate, aid or abet TF. Finally, it lays down the foundation for oversight over individuals and institutions that deal in cryptoassets to reduce the possibility of acquisition, transfer or withdrawal of those assets for TF activities without the knowledge of authorised institutions. The oversight simplifies the process of tracing and seizing digital assets acquired illegally or those deemed to be destined for TF activities, even when terrorists use advanced strategies such as tumbling.[33]

The guidelines are also derived from the provisions under the Central Bank of Bahrain and Financial Institutions Law (Decree No. 64) of 2006.[34] The guidelines on STRs for digital assets were introduced under Volume 6 of the CBB Rulebook[35] to bring these elements of the

[32] FATF, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF', (FATF 2019), who states that this is achieved by eliminating the gateways through which one category of digital assets can be converted into other types or fiat currencies and vice versa.

[33] P Sprenger, and F Balsiger, 'Anti-Money laundering in Times of Cryptocurrencies: Cryptocurrencies-Game Changes in Many Ways' (Master Thesis, Queen Marry University, 2018) who defines tumbling as the act of mixing clean digital assets with those tainted in order to obscure the trail back to the original sources.

[34] Decree No. 64 of 2006. Article 38 of the law empowers the CBB governor to make the necessary changes to the law, through directives and regulations, in order ensure that the provisions therein fulfill the objectives of the Central Bank.

[35] In summary, Vol 6 of the Rulebook outlines five key regulatory mechanisms, including High-level Controls (corporate governance); market Intermediaries and Representatives; Anti-Money Laundering and Combating Financial Crime; Dispute Resolution, Arbitration and Disciplinary Proceedings; and International Cooperation and Exchange of Information. The earliest guidelines on digital assets were introduced in 2019, which were comprised of removal of existing provisions, introduction of new regulations, changes to the rules, as well as improvement of the regulatory regime.

financial sector into the regulatory perimeter of the AML/CTF regime, as well as subject the assets to the necessary supervisory and regulatory measures as part of the portfolio of financial products in the country. The Rulebook provides directives by the CBB relating to traders, dealers, advisors and portfolio managers involved with authorised cryptoassets, either as principals, agents, custodians or crypto-asset exchanges. The regulations apply to crytoassets held within the country, or cryptoassets registered in the country.

In developing STRs, financial services institutions are guided by the fact that digital assets have become integral components of the financial sector products, services and business models. It is thus prudent to establish guidelines for the minimisation of risks, considering that natural and legal persons from and associated with the country use these assets.[36] The guidelines are also designed to enable the country to limit the misuse of digital assets for illegal purposes, thereby increasing the country's risks for ML/TF activities.

5.3.3 Strategies for CTF in the Era of Digital Currencies

The motivation behind the emergent regulations is intelligence gathering through the collection, storage and sharing of information to create a zero-tolerance regime. The current portfolio of requirements imposes a significant burden on private sector firms, who have to comply with superfluous obligations, mandates for the production of numerous risk assessment reports, gather and store large volumes of data and information while being subjected to extensive discretion by the CBB in interpreting and making decisions on the guidelines. There are claims that the exponential growth of the quantity of regulation is counterproductive.[37]

For Bahrain, the criminalisation of predicate offences is achieved through the provisions under Decree-Law No. 4 of 2001. The criminalisation of these predicate offences is a recent strategy following the recognition of the crime-terror nexus. Bahrain recognises a multiplicity of predicate offences for money laundering and terrorist financing and has introduced legislation to outline the punitive and preventive measures in line with the legislative approaches.

As the earliest legal framework dealing with AML/CTF in the country, the original DL No. 4 of 2001 was a direct adaptation of the UNSC Resolution 1373. The framework laid the

[36] CRA 1.1.5 of the CBB Rulebook (n16) defines such a person as one who is incorporated within the Kingdom of Bahrain (legal person), has an address in the Kingdom and solicits clients from the Kingdom.
[37] L Gelemerova, 'On the frontline against money-laundering: the regulatory minefield', (2009) 52 Crime Law Soc Change 33–55, who references the multiplicity of regulations under MLR 2007, although the current regulations under MLR 2017 have increased.

foundation for the criminalisation of ML for all types of properties, including self-laundering.[38] The law lays down the foundation for the confiscation of ML proceeds, including those assets that are directly/indirectly associated with criminal activities.

The amendments to the DL No. 4 of 2001 under Law No. 54 of 2006 related specifically to the introduction of measures for CTF in line with the requirements under the UN Sanctions regime.[39] Under the amendments, Bahrain authorities criminalised TF, whether or not the event that was being financed occurred or not.[40] The amendments under Law No. 54 created the basis for criminal and civil liability for terrorism-related activities. The amendment integrates a multiplicity of legislative approaches. This is achieved through the definition of the actions that constitute terrorism and the identification of the legal aspects of those crimes. Article 3.1 of the Decree further provides for punitive measures for the financing of terrorism activities for events that occur outside Bahrain.

The criminalisation of TF[41] under this law introduces preventive abilities to the existing legal frameworks. Under Article 3 (1) of the decree,[42] the punishment for TF activities includes imprisonment for life or a sentence of at least 10 years, accompanied by a fine of between BD 100,000 and BD 500,000 for any individuals directly or indirectly involved in such activities. These legislative approaches instituted under this law are key to ensuring CTF proactivity. Article 3 of the decree imposes similar penalties for persons who attempt to commit TF. The provisions are specifically designed for CTF in the era of digital currencies since it criminalises the receipt of funds or properties of any kind from terrorist groups to preserve or utilise them to further the goals of terrorism.[43]

---

[38] Self-laundering refers to the process by which an individual or organization uses its own controlled channels to conceal the origins of illicit funds. Instead of relying on external shell companies or third-party facilitators, the perpetrator directs money through a network of entities or accounts they have established themselves, effectively layering transactions within their own financial ecosystem. This method allows the launderer to obscure the trail of money by intermingling legitimate and illicit funds, thereby complicating detection efforts by law enforcement. Self-laundering exploits vulnerabilities in regulatory oversight and internal controls, creating a sophisticated form of money laundering that is particularly challenging to trace and dismantle.

[39] See UN Security Council Subsidiary Organs, 'Subsidiary Organs Of The United Nations Security Council' (2022). <https://www.un.org/securitycouncil/sites/www.un.org.securitycouncil/files/subsidiary_organs_factsheets.pdf> accessed 19 March 2022

[40] This was a key element in the amendment, since, whereas TF was viewed as a criminal act under the previous law, the provision of finds for terrorist activities were only punished if the terror event materialized.

[41] International law has introduced mandatory criminalization of TF as a way of establishing baseline standards for international cooperation. CTF is also mandated under Chapter VII of UN Charter of the Security Council.

[42] As amended by Law No. 54 of 2006, Law No. 25 of 2013 and Law No. 36 of 2017.

[43] These provisions are necessitated by the parity with Penal Code 1976, Article 36 -42, which establishes offenses for an attempt to commit criminal offenses. Article 43 of the Penal Code further establishes criminal liability for

These amendments and provisions utilise the sentence enhancement approach, whereby the sanctions imposed on entities are dependent on their level of involvement in TF activities. This is integral in accommodating the principle of materiality,[44] especially since there are different ways in which the various actors contribute to TF.

The criminalisation of terrorism plays an integral role in the determination of what TF entails by providing a clear and articulate list of actions that are considered part of the terrorist acts in the country.[45] The acts included in the law are prohibited, and punitive measures for financing or participating are identified concerning natural[46] and legal[47] persons. Decree No. 25 (2013) creates a link between ML and TF, with paragraph 2.1 identifying the proceeds of criminal activities, including money laundering, as an explicit contravention of the crimes under TF activities. Several ministerial orders have been utilised to enhance risk aversion. A comparison between Ministerial Order 173 of 2017 and Ministerial Order 108 of 2018 reveals the utilisation of a multiplicity of legislative approaches in integrating several risk-mitigation measures. For instance, under Ministerial Order 173 of 2017, the Ministry of Industry, Commerce and Tourism[48] identified three of the five industries[49] earlier classified as designated non-financial businesses and professions[50] as being high-risk entities for ML/TF. The provisions are included in Article 3[51] , and they mandate several additional measures that are integral to CTF in the era of digital currencies.

The most recent improvements are contained in Decree-Law No. (29) of 2020. Decree-Law No. (29) of 2020 provides updated definitions of what 'money' and 'terrorism' entails. Under Article 1, money is defined as "…all assets, property, economic resources and things of value, whatever their type, description, nature, or method of obtaining them, and whether they

participating in, associating with, or conspiracy to commit a crime, while Article 44 outlines the criminal liability for persons who aid, abet or facilitate the commission of a crime.

[44] Decisions based on the existence of a logical relationship between the action and its consequences to the effects of a case.

[45] I Salami, 'Terrorism Financing with Virtual Currencies: Can Regulatory Technology Solutions Combat This?', (2018) 41 Studies in Conflict & Terrorism, 1–22.

[46] Natural persons face civil and or criminal sanctions.

[47] Legal persons, including corporations and other entities created by law are normally punished by being held criminally liable, fines, prohibition from continuing operations/ being shut down.

[48] Hereinafter 'MOICT'

[49] KPMG, Anti-Money Laundering (AML) Advisory Services (KPMG 2019). <https://assets.kpmg/content/dam/kpmg/bh/pdf/2019/7/kpmg-bahrain-aml-flyer-2019.pdf> accessed 15 March 2022 who states that these entities include jewelers and other retailers of high-value items, accountants and auditors, and car sales and leasing companies.

[50] Hereinafter 'DNFBPs'.

[51] Ministerial Order (108) of 2018, Article 3 (f) to (k).

are material or moral, movable or immovable, tangible or intangible, and include…".[52] Bahrain adopts a multiplicity of legislative approaches in achieving the goals of criminalising TF, with a focus directed on the actors, activities, objectives and the impact of the terrorist attack being financed. This explains the disparity in the various amendments, as well as the applicability of the propositions under the criminal code.

5.3.4 Cooperation with The International Community

The existence of model legislative provisions for AML/CTF strategies has been reviewed in the past to ensure that Bahrain collaborates with the international community in the AML/CTF. The need to cooperate with the international community arises from the fact that the generation, transfer and use of crytoassets occur domestically as well across international borders.[53] These model legislative frameworks guide jurisdictions through the legislative processes to ensure conformation with international standards, as well as provisions for cooperation with other nation-states.[54] Under the Minister of Justice Decision No. 66 (2017), Bahrain has created a directorate for the management of preserved assets.[55] The Directorate is currently working on procedures for executing requests for international cooperation.

These measures are fully supported under Article 122 of the CBB and Financial Institutions Law. The legislative approaches outline that the procedures and mandates vary from one situation to another. Article 122 (b) (1) provides for reciprocity when determining the response by Bahrain to a request for assisting an overseas authority concerning matters relating to investigations of financial crimes and transactions. Through cooperation with the US, Bahrain has implemented an intricate AML/CTF framework. The involvement of the US in Bahraini affairs arises from the extensive threat posed by countries such as Iran. A case in point is the designation of the Future Bank, which was established in Bahrain by Iranian

[52] Decree-Law No. (29) of 2020.
[53] FATF above, n(32)
[54] Over and above the adherence to the 49 recommendations by FATF, which are transmitted through MENA FATF, Bahrain legal framework are aligned with the UN Legislative provisions under Part XI relating to financial sanctions, the provisions by the UNSCRs on preventing, suppressing and disrupting the proliferation of weapons of mass destructions, and the financing of terrorist activities under FATF Recommendations 7.
[55] Commonly referred to as the Reserve Management Directorate (RMD).

investors.[56] Bahrain also works with the Egmont Group,[57] with the Anti Money Laundering Unit having been admitted to the group in July 2003.[58] Part of the rationale for joining the Egmont Group was to enhance the ability of Bahraini institutions to solve the challenges presented by investigations into suspicious transactions that involved foreign entities.[59]

The legislative approaches employed in the creation of these global institutions and assignment of responsibilities for oversight, regulation, supervision, monitoring and imposition of sanctions for legal and natural persons involved in TF include all the typologies identified in Figure 1. The outcome of the establishment of the legal frameworks and institutions is thus broad-based, including general and specific deterrence, prevention, punishment of perpetrators, reassurance and achieving community safety. Since the measures are drawn from the CTF measures before the era of digital currencies, the legislative approaches lack the elements of promoting innovation, which lies under the category of objectives.

5.4 Financial Technology (FinTech)

The integration of technology into the financial sector has led to increased transparency, diversification, innovation and efficiency. FinTech relates to the multiplicity of financial services, including mobile devices, mobile banking, and cloud/digital services.[60] Traditional banking institutions are faced with increased competition from the highly innovative and dynamic start-ups that create value for customers in the financial sector. Unlike traditional banking institutions, which are faced with a broad range of regulatory bottlenecks, FinTech start-ups can identify ways to innovate around the limitations of regulatory regimes.

---

[56] KPMG, "Anti-money Laundering Sanctions Update' (KPMG, 2020).< https://assets.kpmg/content/dam/kpmg/my/pdf/kpmg-newsletter-anti-money-laundering-6.pdf >accessed 19 March 2022 which states that following investigations instituted after the CBB raised concerns about the operations in the bank, it was determined that the Future Bank was involved in wholesale and systematic violations of the laws and regulations under the Bahrain banking sector. The operations of the bank were also against the established AML regulations.

[57] The Egmont Group was created in 1995 to provide FIUs with a platform for the secure exchange of expert and financial intelligence in the process of combatting money laundering, terrorism financing and other related predicate offenses. At the national level, the FIUs collect information relating to unusual of suspicious financial transactions, process and analyse that information, then refer the findings to a law enforcement agency for further action as and where necessary.

[58] J A Adetunji, 'Rethinking the internal mechanism of the EGMONT group in financial crime control' (2019) 22, Journal of Money Laundering Control, 2, 334

[59] *Ibid*, at 336.

[60] J Mueller, and M Piwowar, 'The Rise of FinTech in The Middle East - An Analysis of the Emergence of Bahrain and The United Arab Emirates' (2019).

Financing inclusion, which has been a primary goal in the alleviation of poverty, focuses on the facilitation of payment.[61] Innovations in technology facilitate financial inclusion by introducing novel payment options. FinTech has led to the introduction of novel products, applications, business models and processes, which in turn present challenges and opportunities.[62] In the process of enhancing access, usage and safety of transaction accounts, FinTech innovations in Bahrain have leveraged the designs of these innovations, thus leading to ubiquitous access, enhanced user experiences, awareness of options, improved efficiency, and elimination of traditional barriers to market entry.[63] These design options present advantages that are laced with risks from cybercrime and operational resilience, market concentration, privacy and confidentiality, protection of client funds, and exclusivity for digital users.

These features highlight the need for increased supervision, regulation, oversight and control[64] over the FinTech sector to avert the possibility of contributing to reduced financial inclusion, as well as the possibility of misuse of the technologies for ML/CT activities. The FinTech sector leads to the emergence of non-bank payment services providers (NBPSPs), who offer new services such as mobile payment services, alternative credit scoring systems, novel savings products, peer-to-peer lending and insurance services, among others.[65] Since these institutions operate in a sector different from that of traditional banking services providers, it is necessary for the development of a regulatory regime designed purposefully for the type of risks expected. These risks include the loss of privacy, compromises to the security of personal data, higher risk of scams, unintended discrimination arising from data-driven decision-making

[61] Payments are a gateway to other financial services, including insurance, savings and credit, with the outcome being an increase in the number of transactions.
[62] C Haddadm and L Hornuf, 'The Emergence of Global FinTech Market: Economic and Technological Determinants', (2019) 58 Small Bus Eco, 81 indicates that growth in the FinTech sector is driven by the norms in the technology sector, including the number of users of internet services, mobile phone subscribers, changes in the labour force, as well as the financial sector, including ease of access to financial products and the number of start-ups in the country.
[63] Mueller and Piwowar n(60), 3
[64] The measures include involvement of stakeholders, an effective and comprehensive legal and regulatory framework, information availability and effectiveness communication. See Muller, and others n(3) who uses the example of the growth in mutual funds in the country, which have in turn led to the need for better corporate governance frameworks, and better definition of the roles and responsibilities of all parties to the fund.
[65] UNSGSA FinTech Working Group and CCAF, *Early Lessons on Regulatory Innovations to Enable Inclusive FinTech: Innovation Offices, Regulatory Sandboxes, and RegTech (*Office of the UNSGSA and CCA , 2019) 7.

and data analytics, manipulation of the markers of consumer behaviour, and lack of adequate knowledge and skills by the market participants.[66]

The regulatory and oversight mechanisms necessitated by FinTech consider whether the NBPSPs are designed to provide front-end,[67] back-end[68] services or both. In designing regulatory frameworks for these NBPSPs, it is necessary to take into account the potential risks, including challenges with the protection of consumers, resilience to operational and cyber requirements, protection of funds during storage and transfer, protection of consumer data, ensuring digital inclusion for parity in capabilities, and resilience for the market concentration. These risks are the basic determinants of whether the prevailing regulatory framework is sufficient or whether there is a need for change. In addition to these risks, the issuance of e-money introduces novel considerations for regulation, especially concerning virtual assets. The establishment of a FinTech regulatory framework enables Bahrain to align its goals and process with those other jurisdictions involved in AML/CTF activities. Through the framework, Bahrain can adjust the scale and scope of interventions based on the perceived risks and circumstances while adopting and adapting standards and practices that have been proven to be effective in other locations. Furthermore, a few of the basic FinTech regulatory mechanisms are necessary for the functioning of the financial sector. As a result, the multiplicity of measures under FinTech serves different goals, hence their utility to Bahrain's legal system.

5.4.1 FinTech in Bahrain

The Bahraini financial system is highly diversified, comprised of 400 licenced financial institutions.[69] Starting with the stock market, the Bahrain Bourse lists 13 licenced brokerage firms and 40 corporations, which is indicative of an active and diversified market.[70] The growth of the industry[71] is driven by an open market economy, prudent fiscal and monetary policies, credibility of the regulatory framework, a highly qualified workforce and

[66] M Vucinic,'FinTech and Financial Stability Potential Influence of FinTech on Financial Stability, Risks and Benefits' (2020) 71, Journal of Central Banking Theory and Practice, 49, who identifies these risks in relation to financial technology firms.
[67] J Ehrentraud, and others. 'FinTech and Payments: Regulating Digital Payments Services and e-Money' (2021) < https://www.bis.org/fsi/publ/insights33.pdf> Accessed August 30, 2021.
[68] *Ibid*
[69] A A Aljawder, 'Uniform Anti Money Laundering Policy and Laundering Process Eradication', (PhD Thesis, Brunel University 2018), with the 400 institutions comprised of wholesale banking institutions, finds/asset management firms and insurance companies.
[70] MA Naheem, 'Analysis of Bahrain's anti-money laundering (AML) and combating of terrorist financing (CTF) practices' (2020) 24 Journal of Money Laundering Control p 3 indicates that the bourse lists over 35 fixed income products and 20 mutual funds.
[71] Aljawder n(69).

stable macro-economic systems. The Bahraini FinTech sector has sought a two-pronged approach to growth, featuring an increase in the number of capital inflows, as well as the efficiency and productivity of those capital resources. This is achieved through the introduction of new products and services, including Bahrain Real Estate Investment Trusts (B-REITs) for the domestic and regional markets and the Private Investment Undertakings (PIUs), which are highly flexible mutual funds for the facilitation of private investments for high net-worth individuals[72], as well as diversification of the types of investments based on the investor categories.[73]

The FinTech sector is mandated to engage in the prevention of TF activities through tracking, detection, searching, seizure, apprehension and conviction of perpetrators.[74] This is achieved through performing due diligence on all customers, determining the legality of the source of income, identifying active and potential political exposure for public officers, including PEPs, and enhancing CDD for high-risk entities, such as charities, civil societies and other clubs,[75] and conducting a yearly risk assessment for all digital currency products and services as well as clients to determine exposure to TF risks.[76]

The FinTech sector in Bahrain must be satisfied with the concerns on compatibility between the technological innovations for financial inclusion and the principles of Islamic finance. On the one hand, there is the widely shared[77] notion that FinTech has a positive influence on Shariah principles, including the reduction of costs as a way of enhancing profit-sharing outcomes.[78] Similarly, applications built on blockchain technology facilitate charitable activities and the elimination of illegal activities,[79] considering that charitable institutions associated with Islamic finance are a key target in the 'follow the money'

[72] Muller and others n(3)
[73] Ibid, who identify four types of investors, including private, expert, retail and exempt.
[74] These measures also deter criminals from engaging in ML activities, including smurfing, placement, layering, integration and legitimization of funds.
[75] Financial institutions must seek authorization from the respective ministry before transacting with non-profit organisations (NPOs) or charities. The Ministry of Social Affairs regulates all the NPOs through a multiplicity of laws that create a sound environment for corporate governance aimed at reducing the vulnerability to ML/TF activities.
[76] A report on the assessment is sent to the Money Laundering Reporting Officer (MLRO), who works under the FID.
[77] R Hasan, M K Hassan, and S Aliyu, 'Fintech, Blockchain and Islamic Finance: Literature Review and Research Agenda' (2020) 3 IJIEF: International Journal of Islamic Economics and Finance, 1, 75.
[78] *Ibid*.
[79] I Saba, R Kouser, and I S Chaudhry, 'FinTech and Islamic Finance-Challenges and Opportunities' (2019) 5 Rev of Econ and Dev Studies, 4, 581.

strategies adopted following the 9/11 attacks.[80] These compatibility concerns are further magnified by the fact that the financial sector in the country is comprised of both conventional and Islamic finance products and services.

More recent developments aimed at accelerating compliance with regulatory mandates include the elevation of the Bahrain Bourse (BHB) to a self-regulatory organisation (SRO).[81] As an SRO, the BHB shall create and enforce regulations at the industry level. The change is aimed at bestowing the responsibility for oversight and regulation to individuals and institutions that have the professional training, knowledge and competence to achieve those mandates.[82] By integrating the interests of private actors in government oversight, the BHB targets to achieve efficiency and effectiveness in regulating the complex and dynamic operating environment.

5.4.2 Innovative Regulatory Initiatives under FinTech

FinTech has forced financial regulators to identify novel ways to balance the contemporary objectives of monitoring and oversight for the protection of consumers and financial stability with the emergent goals of promoting growth and innovation.[83] The creation of the FinTech sector, as well as the legislative approaches utilised, is determined by the existing legislative frameworks that seek to ensure that procedural mechanisms are in place to enable the regulators and licensees to be aware of the substantive offences. The sector also avails several tools necessary for mitigating and eliminating risks, including smart regulation. There are three ways in which regulatory institutions in Bahrain utilise it: regulatory technology, regulatory sandboxes, and innovation offices.

5.4.2.1 RegTech

The Financial Services Authority (FSA) introduced the principles of regulatory technology (RegTech) in 2015.[84] RegTech is a subset of FinTech, which utilises digital technologies[85] to promote compliance with regulatory and oversight frameworks. RegTech

[80] J Gurule, *Unfunding Terror: The Legal Response to the Financing of Global Terrorism*, (Edward Elgar Publishing, 2019).
[81] Resolution No. 11 of 2018.
[82] A Hassan, and R Sabirzyanov, 'Optimal Shariah Governance Model in Islamic Finance Regulation' (2015) 3 Int J of Ed and Res, 4, 1.
[83] D A Zetzsche and others, 'Regulating A Revolution: From Regulatory Sandboxes to Smart Regulation' (2017) 23 Fordham Journal of Corporate and Financial Law, 1, 31.
[84] M Turki and others, 'The Regulatory Technology "RegTech", and Money Laundering Preventing in Islamic and Conventional Banking Industry' (2020) 6 Heliyon, 5.
[85] D W Arner, J Barberis, and R P Buckley, 'The Emergence of RegTech 2.0: From Know Your Customer to Know Your Data', (2016) 44, Journal of Financial Transformation, 79.

involves the management of regulatory and oversight procedures for the financial industry using the available technological innovations.[86] RegTech, which is necessitated by the expansion of the FinTech sector, can be attributed to the overhaul of the regulation of the financial sector, as well as the multiplicity of financial technology innovations. Currently, in Bahrain, RegTech involves automation of regulatory compliance, which increases efficiency and reduces the costs of oversight, thereby creating value for both the regulatory institutions and the financial institutions being regulated.[87] It also entails monitoring the regulation, reports on performance and operations, and compliance. RegTech involves the use of machine learning, big data analytics and cloud computing to automate compliance.[88] The processes utilise risk management, reporting and strategic planning applications to enable organisations to remain well-informed about regulatory changes.

Bahraini RegTech is both a strategic and integral tool among modern financial institutions for several reasons. First, it involves the transfer of part of all of the regulatory responsibility to the financial institutions.[89] In addition to facilitating time and cost-efficiency across different regulatory typologies, it enables financial institutions to increase effectiveness during the regulation of emergent FinTech tools and applications whose design accounts for the challenges in monitoring under the legacy and traditional regimes.[90] In Bahrain, RegTech is designed to facilitate verification of identifies, anti-fraud measures, reduction of AML/CTF risks, and KYC measures as part of the broader CDD measures. RegTech offers the possibility for real-time and proportionate regulatory regimes for the various cryptoassets, thereby recognising that although there are different cryptoassets, the TF risks have numerous similarities.

Bahrain utilises RegTech to create an environment where the TF risks from technological innovations are mitigated on a case-by-case basis. This elevates the utility of RegTech for legislative approaches in the era of digital currencies. The risks associated with unregulated operations can be monitored and are limited to a small scope of the institutions.

[86] Turki and others n(84)
[87] M Becker, K Merz, and R Buchkremer 'RegTech—the application of modern information technology in regulatory affairs: areas of interest in research and practice', (2020) 27 Intell Sys Acc Fin Mgmt, 1, who estimated that the top US banking institutions used over US$70.2B in compliance costs in 2013, which was twice the cost of compliance in 2007 (US$34.7B).
[88] Bahrain, using artificial intelligence is expected to reduce human error, and simplify the standardized regulatory procedures, thereby cutting the costs and time required for oversight.
[89] Ross and Hannan, n(15) at 113.
[90] For instance, automation of KYC processes to ensure real-time information across different regulatory regimes.

RegTech enables Bahrain to utilise non-conviction-based approaches, such as civil forfeiture, which is one of the mechanisms for depriving criminals and terrorist groups of the instrumentalities of crime and terror attacks, respectively.[91] The introduction of RegTech has provided Bahrain with an additional tool in combatting ML/TF risks while also enabling it to adopt foreign and international practices in response to the changes in the adoption and use of cryptoassets within its borders. Through RegTech, Bahrain has established the framework for growing its regulatory mandates in line with changes in the highly dynamic technology industry. Since the country is an adopter of technology, this approach is integral in orienting the trajectory of change towards countries that innovate, thereby ensuring that Bahrain does not lag in awareness and management of risks associated with ML/TF, specifically concerning digital assets.

5.4.2.2 Regulatory Sandboxes

The first regulatory sandbox framework in Bahrain was developed by The Trucial Investment Partners from Dubai, the Singaporean FinTech Consortium and the Bahrain Economic Development Board in 21017.[92] The facility offers space for private offices, co-working, events and acceleration programmes concerning digital assets, which are responsive to Islamic finance products.[93] These are formal programs designed to facilitate the virtual testing of digital products, services and business models within a FinTech sector to determine their suitability for customers before launching them into the market.[94] The testing process focuses on safeguarding and designing features for market development while keeping abreast of global standards. Regulatory sandboxes utilise structured experimentalism to enable regulators to remain involved in the innovations associated with FinTech to promote inclusion while reducing emergent and extant risks, with a specific focus on ML/TF risks.[95] Regulatory sandboxes provide the basis for evidence-based policymaking while enabling regulators to

---

[91] See UNCAC, 'Report on the Meeting of the Ended Intergovernmental Working Group on Asset Recovery Held in Vienna on 29th and 30th May, 2019 (UNODC, 2019)< https://www.unodc.org/documents/treaties/UNCAC/WorkingGroups/workinggroup2/2019-May-29-30/V1905966e.pdf. >accessed 19 March 2023

[92] M Wechsler, L Perlman, and N Gurung, 'The State of Regulatory Sandboxes in Developing Countries' (2018) SSRN electronic journal < https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=3285938> accessed 19 March 2023

[93] N Alam, and S N Ali, *Fintech, Digital Currency and the Future of Islamic Finance: Strategic, Regulatory and Adoption Issues in the Gulf Cooperation Council,* (Springer, 2020), 231

[94] I Jenik, and S Duff, 'How to Build a Regulatory Sandbox: A Practical Guide for Policy Makers (2020) <https://www.cgap.org/sites/default/files/publications/2020_09_Technical_Guide_How_To_Build_Regulatory_Sandbox.pdf > accessed 19 March 2023

[95] Zetzsche and others n(83)

develop additional tools and avenues for financial inclusion. The regulatory framework for Bahraini sandboxes is developed through a multiplicity of legislative approaches, most of which are informed by the need to prevent and intervene in cases of TF through virtual assets. First, there are generic aspects that are common across all regulatory sandboxes, including the framing of the legislative frameworks to accommodate the novel TF risks presented by the operating environment. These include proposals for regulators to monitor the operations within the sandbox, specify the uniform duration for existence within the sandbox, clarify the mandates for reporting and responsibilities of the managers, and outline the mechanisms for exiting the sandbox. In achieving this goal, Bahrain utilises several experimental legislations,[96] with decisions based on outcomes. For instance, the duration for participation in the regulatory sandbox is set at 9 months.[97] During the nine months, the applicants have to prove that their products and services (which are mostly based on virtual assets) adhere to the relevant regulations by the CBB regarding KYC, AML/CFT, customer due diligence and fulfilment of the financial inclusion goals and protection by the customers. The CBB reserves the right to vary the 9 months to a year[98] through legislation that best fits the test of alternatives, as it seeks to identify the best approach to incubating the technologies for cryptoassets to insulate itself against any potential TF risks once the entities are deployed in the market.

In Bahrain,[99] the CBB has adopted innovation-friendly legislation to regulate sandboxes. Due to the novel nature of the regulatory sandboxes in Bahrain, the legislative approaches also feature elements of organisational proscription[100] since any organisation that has not participated in the regulatory sandbox is not allowed to deal in cryptoassets in the country. Through these legislative approaches, Bahrain has achieved several goals relating to CTF, including general deterrence, prevention, community safety, and promoting innovation. Regulatory sandboxes are a unique strategy that is integral in promoting the adoption and use

[96] The legislative frameworks are termed as experimental since they are implemented for the short-term, after which decisions are made based on how successful or useful they are for the purpose.
[97] S Ahmed, and K Chavaly, 'Blue Print of FinTech Regulatory Sandbox Law: Preparing for the Future of FinTech Innovation (2020) <https://vidhilegalpolicy.in/wp-content/uploads/2020/03/20200313_Blueprint-of-a-Fintech-Regulatory-Sandbox-Law.pdf>a ccessed 19 March 2023 who reveals that other countries have adopted much lesser durations, even though they provide for extension of the period. For Bahrain, leaving the duration open to interpretation is necessary for the objectives of promoting the FinTech sector, and creating a favourable operating environment.
[98] *Ibid*.
[99] Regulatory sandboxes fall under the Central Bank of Bahrain and Financial Institutions Law (Decree No. 64) of 2006.
[100] The CBB and Financial Institutions Law (Decree law No. 64 of 2006) points out that the provision of false or misleading information under the application (for participation in the regulatory sandbox) may result in refusal for the application, and subsequent cancellation of the license if discovered later.

of cryptoassets as part of a technological transformation of the country. In recognition of the complexities associated with the novelty of digital assets, the regulatory sandboxes are part of the measures by the government to extend a helping hand to the institutions and individuals who use cryptoassets in the country. The measures are aimed at guiding the users to ensure that they are not exploited by deploying the resources and knowledge of the state as a cushion against potential exploitation by foreign entities that have extensive technological capabilities. The temporary nature of regulatory sandboxes reveals the extent to which the government recognises the value of cryptoassets from the perspective of the financial benefits while also recognising the potential pitfalls linked to risks for ML/TF.

5.4.2.3 Innovation Offices

Innovation offices[101] play a primary role in regulatory initiatives for crytoassets since they facilitate the engagement of regulators and innovators in a process best described as crowdfunding regulation.[102] By improving the understanding of financial innovations while supporting the financial innovations mediated by technology, innovation offices reduce the risks and uncertainties associated with regulatory mechanisms, especially for novel FinTech products. This signals to the entities involved in the industry that the regulator is pro-innovation, hence laying down the foundation for inclusive FinTech. Innovation offices highlight the importance of timely interventions through engagement with innovators, with the primary goal being the coordination of the innovation to ensure that the trajectory of development is suited to the market needs and requirements. Innovation offices also provide the necessary resources for FinTech companies. This discussion reveals that to achieve the goals of regulation in a highly fragmented marketplace, where technological innovations are introduced in a highly unpredictable manner, it is necessary to adopt a sequential reform process, starting with the adoption of digital solutions introducing smart regulations.

The three classes of institutional frameworks are established as a way of promoting the adoption of cryptoassets in the country. Bahrain has invested in these types of institutions as a way of creating a favourable environment for the adoption and utilisation of cryptoassets. Rather than focus on the regulatory and enforcement mandates, these institutions are part of Bahrain's unique approach to ensuring that the ML/TF risks associated with cryptoassets are

[101] Zetzsche and others n(83)

[102] BEDB, *Bahrain FinTech Ecosystem Report 2018* (BEDB 2019) which was introduced under the CBB Rulebook Vol. 5-Financing Based Crowdfunding Platform Operate, and amended under Vol 6 of the CBB Rulebook.

reduced. The functions of the three categories of institutions culminate in a more informed population in the country, thereby reducing the potential for exploitation of unwitting persons who are drawn into the use of cryptoassets by unscrupulous individuals. The three institutional frameworks are designed to enhance awareness among those using or dealing in cryptoassets on account of the recognition that the technology is still novel in the country. Additional rationales include the fact that Bahrain seeks to promote the use of cryptoassets by its citizens, and the quantitative increase in these activities implies an increase in the risks associated with ML/TF through digital assets.

5.5 RAIN-The First Crypto Asset Exchange.

Existing literature recognises the fact that whereas crytoassets present novel risks for ML/TF, their utility for TF is limited by several bottlenecks.[103] By establishing a domestic crypto-asset exchange that is regulated domestically, Bahrain bases the regulations on the crypto asset on the actors and the objectives, which explains why the provisions under the rule book focus on participation offences, general deterrence, punishment, prevention of criminal acts, promotion of innovation, community safety and sentence enhancement. Part of the measures is covered under the innovative regulation under the FinTech segment.

The regulation module for crypto-asset platform operators (CPOs), which is part of Vol 6 of the CBB Rulebook, is developed through a multiplicity of legislative approaches. The regulation recognises the four categories of tokens that the CPOs are authorised to deal with within the country, including payment, utility, asset, and hybrid tokens. The framework is modelled around the measures by the Monetary Authority of Singapore (MAS), which is a technology-enabled supervisory framework.[104]

The establishment of RAIN, as well as other frameworks for regulating digital assets, arises from the fact that digital currencies, such as cryptoassets, present novel risks when utilised in an environment where Islamic finance is the primary financial system. The legislative approaches adopted recognise the extant[105] and emergent[106] theories of liability. In

[103] Ahmed and Chavaly n(97)
[104] R Coelho, J Fishman, and D G Ocampo, 'Supervising Cryptoassets for Anti-Money Laundering, FSI Insights on Policy Implementation' (2021) https://www.bis.org/fsi/publ/insights31.pdf> accessed 19 March 2023 reveals that relies on network analysis, data analytics and close surveillance on the digital token payment sector in order to accommodate the elevated ML/TF risks.
[105] A Bitterly, Can Banks Be Liable for Aiding and Abetting Terrorism? A Closer Look into the Split on Secondary Liability Under the Antiterrorism Act, (2015) 83 Fordham L. Rev, 3399.
[106] *Ibid*, 3402.

recognising these forms of liability, Bahrain has adopted a highly conservative approach to the licensing of crypto exchanges due to the multiplicity of TF risks associated with transactions involving digital assets. Whereas the four categories for licensure are clearly outlined with commensurate mandates for service provision, the CBB has only offered a license to Rain due to the need to insulate itself against risks from crypto cleansing using various digital assets. The risks arise when advanced digital exchanges provide the services of exchanging primary coins, such as Bitcoin, for other forms of coins, including altcoins.[107] By placing Rain under close state supervision, Bahrain has established a robust and highly regulated environment for the handling of digital assets. The legislative approaches utilised in the licensure of Rain entail several methodologies identified in the typology in Figure 1.

5.5.1 Licencing and Procedure

The licensing of institutions involved in the financial industry in Bahrain is derived from the CBB and Financial Institutions Law of 2006 (CBB Law) and CRA-1. Article 125 (a)-(c) of the CBB Law prescribes the actions that the regulatory institutions can take against institutions that fail to adhere to the legal requirements, including penalties, seizure of assets as well as sanctions for individuals involved in the management of the crypto exchange. CRA 1.1 outlines the requirements and exclusions of services for crypto-asset services providers in Bahrain. In line with the propositions by FATF, all individuals and corporations interested in providing crypto-asset services in Bahrain have to be licensed for such activities.[108] CRA 4.3.3 provides for the reservation of the right to determine the suitability of the various crypto-asset services, which are taken into account.[109] These measures, which focus on the actors, play an integral role in ensuring an even playing field, as well as laying down the foundation for supervisory cooperation with regulatory institutions in other locations outside the country.

CPO licensees are tasked with responsibilities that facilitate the reduction and elimination of ML/TF risks, including adhering to mandates on record keeping, minimum capital requirements and reporting requirements. Failure to adhere to these statutory requirements automatically leads to loss of license or punitive measures by the CBB. The

[107] Sprenger, and Balsiger n(33)

[108] The mandates for licenses as a Bahraini CPO are deemed necessary to eliminate the possibility of arbitrage and the challenges associated with uneven implementation and adoption of international standards on regulating cryptoassets.

[109] In licensing individuals, the CBB, under CRA 4.3.3, bases its decision on 18 key factors, including (a) the technological experience, (b) cybersecurity systems and controls… (d), Protocols in place…(f) developments in the market…(o) connectivity, (p) market demand, (q) type of distributed ledger, (r), innovation/ efficiency, (s), functionality.

legislative approach adopted by Bahrain reveals that the CBB recognises the duality of cryptoassets as a new tool for providing the same financial services as the contemporary institutions as well as providing a novel financial service that is not fully covered by the existing regulatory framework.[110] Under CRSA-1.2.18, Bahrain utilises enterprise crime offence legislative approaches in outlawing the misrepresentation of an applicant as a licensee before official authorisation by the CBB.[111] The provision is founded on the premise that such entities are predisposed to engage in illegal activities and may lack the necessary tools and abilities to fulfil their AML/CTF responsibilities as part of the financial services industry.

Bahraini institutions have elected to establish different guidelines for VASPs, even if they hold licensing for the provision of traditional financial services. In line with FATF recommendations, these institutions are already faced with a portfolio of regulations that fit the AML/CFT risks associated with financial instruments and services. These licencing measures have proven to be effective as deterrents for ML/TF in other locations, hence justifying Bahrain to adopt this strategy. Licencing also serves a multiplicity of purposes in the regulation of financial industries, thereby introducing strategies that are considered traditional in the digital era. The combination of processes that culminate in the acquisition and retention of a licence enables the Bahraini regulatory institution to achieve AML/CTF goals while also enabling the regulators to adhere to international standards.

5.5.2 Minimum Capital Requirements

The module relating to minimum capital requirements under the CBB Rulebook also outlines the capital requirements for the different categories of licensees, including the paid-up share capital. Under CRA 3.1.2, the CBB rule book provides for four classifications of CPOs based on their capital requirements for operations.[112] The provisions relating to minimum capital requirements also adopt the top-runner approach under CRA 3.1.5, which is designed to enable the CPO licensees to proceed with operations despite short-term shortfalls in the capital. Furthermore, this categorisation also plays a role in the prescription of fines for contravention of the licensing guidelines,[113] with higher fines and punitive measures set for

[110] H Y Jabotinsky, 'The Regulation of Cryptocurrencies: Between a Currency and a Financial Product' (2020) 31 Fordham Intell. Prop. Media & Ent. L.J. 1, 121.
[111] Such an act is in contravention of Article 40 and 41 of the CBB law, with an assigned penalty of up to BD1M.
[112] The CRA 3.1.4 further provides nine considerations to be considered by the CBB will utilize in determining whether a licensee under CBO requires additional capital, since not all institutions have similar risk profiles.
[113] See CRA-14.6.13, which sets the penalty for late filing for Category 1 licensee at BD 40 per day, BD 60 per day for category 2 and 3 licensees, and BD 100 for category 4 licensees.

entities with higher minimum capital. However, to limit risk exposures, such licensees must provide written notifications to the CBB and a plan on how to requalify for the current license. The agile nature of these provisions is cognisant of the fact that the value of the assets held by crypto-asset dealers fluctuates due to factors outside the control of most market players,[114] and in the absence of recognition of such risks, most operators under RAIN would be in contravention of the existing laws.

In regulating crypto exchanges, Bahrain has established four categories of licenses, with specific guidelines on their obligations in the industry, as shown in Appendix 4.[115] The legislative approaches utilised in determining the limitations obligations resemble what traditional banking institutions face since the TF risks are often assumed to be directly related to the available assets.

5.5.3 Measures to safeguard interests

The CBB has established guidelines under the Market Intermediaries Representative Module, which outlines rules on the separation and management of the assets and money belonging to each client.[116] There are also requirements for disclosure for all licensees, including the general and specific terms and conditions set for clients under each product and service category. This also includes requirements for confirmation and consent before every transaction. Similarly, provisions under the CBB Rulebook under CRA -14.9.1.c[117] adopt the conspiracy legislative approach by mandating that CPO licensees start operations within six months of acquiring approval from the CBB. Measures are put in place to accommodate the highly dynamic cryptoassets industry. Furthermore, the mandate for commencing operations within that period arises from the fact that all licensees must provide assessment reports based on operations in the market.

In achieving the CTF objectives, Bahrain uses legislative approaches designed to avoid unlawful associations through the provisions under CRA 7.1.4.[118] The section prohibits the registration of certain institutions which are considered high-risk as clients, including charitable institutions, religious groups, sporting clubs, social and cooperative clubs and other

[114] See BEDB n(102)
[115] *Ibid.*
[116] This is necessitated by the similarity in digital assets, which accounts for similarities in risks for ML/TF.
[117] CBB Rulebook, *Crypto-Asset Module: Central Bank of Bahrain Rule Book, Vol 6: Capital Markets* (CBB 2019).
[118] *Ibid*, 105

societies.[119] The risks attached to these institutions, considering that some of these institutions operate globally, call for an aggregative appreciation of ML/TF, both at a global level and in the digital era. Clear appreciation is also integral in the identification of the emergent risks associated with the transition from what is considered traditional to new-age terrorism. As a result, the measures to safeguard interests are framed in an aggregative manner to avoid overlooking any dimension.

5.5.4 Technology Requirements

The licenced entities must meet basic network security standards under the best practices proposals.[120] The procedures and measures in place must be accorded robust priority to the management of technological innovations, specifically those associated with cyber-security risks. In response to the risk arising from the possibility of anonymisation of transactions involving cryptoassets, Bahrain has adopted additional measures over and above what is required for other capital markets services providers.[121] The requirement is mandated due to the presence of crypto-asset wallets and encrypted safe customer accounts, which have to be retrievable and secure at all times. The protections included in these network security measures include protection against theft or hacking. These technology requirements prevent the prevalence of cybercrime, where individuals acquire digital currencies that could end up facilitating TF.

5.5.5 Outsourcing

The module outlines procedures for contracts relating to the use of vendor and outsourced services concerning digital assets.[122] The regulations are designed to ensure that all licensed entities have plans for business continuity in case the offshore or onshore vendors are unable to provide the outsourced services. The provisions of CRA 8.2 mandate that all licensees must perform a risk assessment of third parties that act as custodians of digital assets to determine whether the third party can provide similar protections as those mandated under the CBB Rulebook. The legislative approaches, which focus on the type of associations, allowed

[119] As discussed earlier, these institutions are highly amorphous and are known to be used for a multiplicity of undeclared activities that can end up leading to facilitation of TF.
[120] Professional or commercial procedures that are prescribed or accepted as being the most effective for achieving the goals within the industry. Eventually, best practices influence policy, regulations and laws.
[121] AML 6.1.1 mandates that "Capital Market Services Providers must comply with the record-keeping requirements contained in the AML Law and in the CBB Law…must therefore retain adequate records (including accounting and identification records)" ...for a minimum of 5 years after the end of the customer relationship (AML 6.1.1 (a) and (b)).
[122] CBB n(117) CRA 8.2, relating to custodial arrangements.

the recognition of the fact that the value of digital assets for TF activities differs from what fiat currencies possess.[123] Similarly, the licenced entities are only authorised to outsource non-core functions. Among the core functions that cannot be outsourced include the regulatory obligations, which determine the legality of the operations within the country.

In summary, due to the novel nature of the industry, the legislative processes in the development of these regulatory mandates can also be analysed from the overriding objective. As part of the innovation-friendly legislation, it is apparent that most of the provisions are justified by the need to promote flexibility in taking advantage of the inclusion of cryptoassets in the Bahraini financial sector. These provisions bear elements of experimental legislation, while where it serves best, the top-runner approach is adopted. The effect of these legislative approaches is the imposition of five key responsibilities and obligations on entities that use cryptoassets in the country, including enrolment,[124] establishment and maintenance of AML/CFT programmes,[125] CDD,[126] reporting[127] and record-keeping.[128] Furthermore, the legislative approaches associated with the FinTech sector, including those that facilitate RegTech, are essentially motivated by the need to elevate Bahrain's ability to promote innovation. This is why the discourse reflects heavily on elements of the original DL NO. 4 of 2001 and its amendments, as well as the CBB Law.

5.6 Financial Intelligence Units (FIU) of Bahrain.

The FIUs are established according to the provisions of Article 4(4) of DL No. 4 of 2001. As part of the transactional networks emerging from the globalisation of CTF, FIUs are often viewed as expanding the regulatory capacity of states outside the national borders to respond to the increasingly complex environment before the establishment of these units. The Anti-Money Laundering Unit (AMLU) received and processed disclosures and reports on ML

[123] For instance, risks emerge from the significant fluctuations in the value of cryptoassets held in custody, which makes it possible for facilitation of TF.
[124] All entities involved in the cryptoassets markets in the country must be enrolled, through registration or licensing, within Bahrain as a CPO before it commences operations.
[125] Each institution has an internal ALM/CTF program, designed for identification, mitigation and management of ML/TF risks, which is aligned with the prevailing legal framework, but customized to the environment in which the company operates.
[126] Identification and verification of the identity of customers, as well as ongoing monitoring of their transactions in order to identify any suspicious transactions.
[127] Notification to the authorities on every suspicious activity, especially those which contravene the threshold for transactions, as well as transfer of funds across borders.
[128] Entities are required to retain all records of transaction, electronic funds transfer, customer details and other information for up to 5 years after the customer departs in order to facilitate any potential investigations.

and other predicate crimes. However, as a police-type FIU,[129] the AMLU lacked a close working relationship with the primary sector regulators due to the absence of high-profile links to other reporting entities, such as Designated Non-Financial Businesses and Professions.[130]

FIUs, which operate under the Financial Intelligence Directorate (FID), [131] are specialised agencies that play an integral role in AML/CTF in several ways. First, by cooperating with financial institutions and banks in AML/CTF measures within and outside the country. As a law enforcement agency,[132] the FID has access to the data collected by police departments and other investigative entities in the country. The FID has access to the Najem unified criminal database system, which is a unified application for the criminal investigative department designed to overcome the barriers to the daily handling of information and metadata. Its objective is to increase the productivity and efficiency of law enforcement agencies, including reports from traffic police, immigration agencies, and agencies involved in resident affairs. The FID can also request institutions to provide information regarding transactions. Bahraini regulatory entities work hand in hand with regulatory institutions from Europe (UK), the Americas (US), Africa (Tunisia and Egypt), and the Middle East (Saudi Arabia) to intensify the training in different modules. In 2016, the country became a signatory to the Mutual Administrative Assistance on Tax under the OECD to improve its ability to oppose financial crimes, including ML.[133]

Second, by monitoring transactions across financial networks, FIUs identify and investigate suspicious activities.[134] In addition to the FID, these STRs are sent to the MOICT and CBB, both of which focus on different dimensions of the reports, to ensure a comprehensive review of all the risk exposures facing the registered institutions. The efficiency and effectiveness of suspicious transaction reporting are best understood from the perspective

[129] See the definition of police-type AMLUs, which lack provisions for proactive ML/TF measures.
[130] Hereinafter 'DNFBPs'.
[131] Subsequent amendments to the law include Ministerial order 102 of 2001, Ministerial Order 9 of 2007, Ministerial order 17 of 2017 and Ministerial order 17 of 2017.
[132] Hereinafter 'LEA'.
[133] OECD, 'Jurisdictions participating in the Convention on Mutual Administrative Assistance in Tac Matters' (2021) < https://www.oecd.org/tax/exchange-of-tax-information/Status_of_convention.pdf> accessed 19 March 2023 which reveals that Bahrain became a fully signed member in 2018.
[134] Under Article 1 of Decision No. 18 of 2002, the FID is the institution authorized to receive all suspicious transaction reports relating to ML and TF in Bahrain, from all registered institutions.

of the qualitative[135] and quantitative[136] characteristics of the contents. An increase in STRs is not indicative of increased ML/TF exposure, and a decrease thereof does not imply an improvement in the efficiency of AML/CTF practices. Third, the FID conducts operational[137] and strategic[138] analysis and then disseminates the results of the initial analysis to the Public Prosecution Office (PPO). With the contours of this available information, the qualitative and quantitative changes in the STR and related cases reveal the growing propensity of Bahraini FID to break down the networks established by crime and terror groups within and outside the country for ML/TF activities.

In some cases, the STRs relate to scams designed to enrich key individuals. Fourth, FIUs provide law enforcement agencies and judicial entities with the evidence and tools for arresting and prosecuting suspects of financial crimes. These provisions are contained in DL NO 4 of 2001 and represent the key legislative approach relating to the powers of law enforcement. Fifth, the transnational nature of ML/TF activities, whether through traditional currencies or digital assets, implies that FIUs are constantly dealing with cross-border transactions involving one or multiple parties. The participation of the Egmont group enables FIUs to cooperate in investigating such transactions, with the primary goal being to share information. Through the principles of the Egmont Group and Article 9(1) of the Anti-Money Laundering Act[139] , Bahrain exchanges information on TF with foreign counterparts, be it upon request or under its initiative. The FID operates on a multiplicity of reports from stakeholders in different sectors, including exchange companies, the securities sector, the gold sector, precious metals and gemstones, real estate, accountants, lawyers, and the banking sector. The reports are based on three categories of indicators, including client-related indicators, transaction-related indicators, and geographic-related indicators.

In summary, a number of these measures are derived from other jurisdictions that face similar ML/TF risks. The customisation of the measures, including the recalibration of existing legal frameworks, reveals Bahrain's willingness and ability to orient itself towards measures that have been proven effective. However, it remains to be seen whether the country has fully

[135] The qualitative characteristics are defined as a measure of the potential validity and impact of the transaction, which is identified, as well as the weight of the adverse event that is averted due to the suspicious report and subsequent actions by the FIU.
[136] Quantitative characteristics are defined as the number of STRs identified and reported within a specific period, which can either be an absolute figure, or a proportion of the total 'actual' suspicious transactions that occurred.
[137] Ministerial Order 17 of 2017 Article 2.
[138] Strategic analysis involves assessment of trends in TF to implement the relevant countermeasures.
[139] Herein after 'AMLA'

adopted the measures in their entirety, considering the uniqueness of the Bahraini environment compared to other foreign locations.

5.7 Bahrain as a Member of FATF and MENAFATF.

The FATF makes policies for the generation of the essential political motivation for the introduction of regulatory and legislative reforms in AML/CTF areas. As the ML/TF watchdog, the FATF has established international standards designed to reduce and prevent illegal activities, as well as diminish their harmful effects on society.[140] The international nature of the standards leads to a coordinated response from predicate offences for ML/TF, including criminal activities, terrorism and corruption. The FATF has a clear trajectory for continuous strengthening of its standards in response to emergent risks, with the most recent proposals revolving around the regulation of virtual assets. The FATF reviews the existing processes, frameworks and methodologies within a specific jurisdiction and then provides high-level propositions that target the various strategic AML/CTF deficiencies. In addition, the FATF utilises lessons learnt from one jurisdiction across the globe in response to the globalised and highly integrated financial system in the 21st century.

In adapting the legislative provisions, Bahrain has taken care to appreciate the specific language and the underlying concepts under FATF to ensure compatibility with the legal and constitutional principles in its dual legal system, where Sharia and common law principles are utilised. Through its membership,[141] Bahrain contributes to international obligations associated with risk management, monitoring of transactions and other programs designed to screen sanctions placed upon individuals by institutions and nation-states from across the globe.[142] Essentially, this enables the institutions within Bahrain to prevent the evasion of state-level sanctions associated with the use of digital currencies, as well as other risky activities such as ML and TF. In cases where a disparity exists, Bahrain has supplemented or complemented the provisions to achieve the goals within the national context.

---

[140] R F Pol, 'Anti-money laundering effectiveness: assessing outcomes or ticking boxes?' (2018) 21 Journal of Money Laundering Control, 2, 215 defines FATF recommendations as a comprehensive and consistent framework of measures which countries must implement in the process of combatting ML/TF activities.

[141] MENAFATF, *Mutual Evaluation Report of the Kingdom of Bahrain on Anti-Money Laundering and Combating Financing of Terrorism*(FATF, 2006), Bahrain played a key role in the establishment of MENAFATF in 2004, by providing the headquarters for operations, as well as financing its operating budget for the first five years. Bahrain has also contributed to the development and strengthening of regional and international cooperation for CTF within and outside the GCC.

[142] *Ibid*

The FATF offers different types of reports, including risk-based approach reports,[143] mutual evaluation reports,[144] typology reports[145] guidance and best practices reports,[146] in addition to the annual report. These reports provide Bahrain with propositions on how to change their legislative processes, with those changes dependent on the objectives and purpose for which the report was made, the prevailing risks covered under the recommendations, the scope of the report, the prevailing legal framework in place, and the substance of the recommendations.

5.7.1 Mutual Evaluation Reports (MERs)

Currently, MENAFATF has provided two MERs to Bahrain in 2007 and 2018, with a follow-up report for the 2007 MER provided in 2012. The methodology for those MERs by FATF involves technical compliance and effectiveness of the regulatory and monitoring measures in place.[147] The methodology utilised by the FATF was introduced in 2012, featuring two dimensions: technical compliance and effectiveness. Technical compliance involves implementing the requirements for each recommendation by FATF. The recommendations are comprised of legal frameworks and means for enforcing such laws, as well as the procedures and powers to be applied by the assigned authorities. The extent to which a country complies (or fails to comply)[148] with standards is used to determine the type of interventions.

Effectiveness[149] is assessed to determine the extent to which the country has utilised the procedures proposed under the recommendations to improve outcomes under the FATF

[143] FATF relies on the risk-based approach for effectiveness in the implementation of recommendations. The risk-based approach enables the member countries to focus on

[144] Through peer reviews of member states, FATF performs assessments on the level of implementation of the recommendations, with an in-depth analysis and account of the systems for prevention of criminal and terrorist abuse of the financial system within the country.

[145] FATF provides an outline of the methods and trends through which criminals and terror groups engage in money laundering and terrorism financing, respectively. With the constant evolution in these approaches, as well as the evolution in the financial sector and other variables that determine ML/TF activities, the typologies report help countries to identify, assess and understand the various risks, and implement the necessary counter measures.

[146] These reports provide guidance on the best practices for assisting jurisdictions in implementing the changes recommended by the FATF. Accessed 19 March 2023

[147] FATF, *Methodology, For Assessing Technical Compliance with The FATF Recommendations And The Effectiveness Of AML/CFT Systems,* (FATF, 2020) < https://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf> Accessed 19 March 2023

[148] The four ratings include compliant (the country has fulfilled its regulatory mandates with no shortcomings at all), largely compliant (the country has fulfilled most of its regulatory mandates with minor shortcomings), partially compliant (the country has only fulfilled some of its regulatory mandates with moderate shortcomings at all), non-compliant (the country has fulfilled none of its regulatory mandates with numerous and major shortcomings), or non-applicable (the regulatory mandates included in the recommendation are not applicable within that country).

[149] Pol n(140), 218.

focus, the ability to identify the degree to which the AML/CFT program achieves the expected standards, the ability to identify any weaknesses in the system, and the ability to prioritise the risk exposures to ML/CT activities. The effectiveness of the methodology is dependent on the degree to which the expected results are achieved.[150] The methodology's effectiveness makes it possible to determine the entire AML/CFT system and how well it works for the intended purposes. A framework for assessing effectiveness exists with 11 elements.

These objectives serve two overarching questions: determining the extent to which outcomes are being achieved and identifying interventions for enhancing effectiveness. However, there are concerns that the 'effectiveness' component of the methodology lacks a specific results-based framework, as discussed in the various MERs. The problem lies in the labelling of outcomes as activities and outputs, thereby leading to the evaluation of outcomes as effects and impacts of AML policies.[151] Furthermore, the determination of effectiveness is based on outcomes, which are influenced by the dynamic combination of inputs, processes, and external variables, creating a circular reasoning problem.[152] The challenge arises from the fact that the multiplicity of regulatory measures proposed is dependent on the prevailing risks which arise from the effectiveness of the existing regulatory measures.

The legislative approaches in response to the recommendations under FATF are derived from the 2018 MER, as shown in the table hereunder. The legislative approaches can be deduced based on the level of assessed compliance, as well as the intrinsic characteristics of the relevant legislation in place. However, the MERs are based on subjective assessment, which introduces the risk of skewed reviews. Furthermore, the use of a qualitative scale limits the ability of non-technical users of the report to appreciate the meaning of the assigned level of technical compliance. Finally, the diversity of standards with interrelated outcomes presents the danger of jurisdictions engaging in tick-box culture without rigorous review of the actual level of compliance.

Figure 1: MER Report for Levels of Compliance in 2018 for Bahrain

[150] S D Jayasekara, 'How effective are the current global standards in combating money laundering and terrorist financing?' (2021) 24 J of Money Laundering Control, 2, 257
[151] Pol n(140), 215.
[152] L S Terry, and J C Robles, 'The Relevance of FATF's Recommendations and Fourth Round of Mutual Evaluation to the Legal Profession, (2018) 42 Fordham Int. Law J 2, 627.

Standard	Level of Technical Compliance 2018
1) Assessing risk and applying a risk-based approach	Partially compliant
2) National cooperation and coordination	Largely compliant
3) Money Laundering Offence	Largely compliant
4) Confiscation and provisional measures	Compliant
5) Terrorist financing offence	Partially compliant
6) Targeted financial sanctions, terrorism and terrorist financing	Partially compliant
7) Targeted financial sanctions-Proliferation	Partially compliant
8) Non-profit organisations	Largely compliant
9) Financial institution secrecy law	Compliant
10) Customer due diligence	Largely compliant
11) Record keeping	Compliant
12) Politically exposed persons	Largely compliant
13) Correspondent banking	Largely compliant
14) Money or value transfer services	Largely compliant
15) New technologies	Compliant
16) Wire transfers	Largely compliant
17) Reliance on third parties	Compliant
18) Internal controls and foreign branches and subsidiaries	Largely compliant
19) Higher risk countries	Largely compliant
20) Reporting of suspicious transactions	Largely compliant
21) Tipping-off and confidentiality	Largely compliant
22) DNFBPs[153]: Customer due diligence	Partially compliant
23) DNFBPs: Other measures	Partially compliant
24) Transparency & BO of legal persons	Largely compliant

[153] Designated Non-Financial Business and Professions.

25) Transparency & BO of legal arrangements	Largely compliant
26) Regulation and supervision of financial institutions	Largely compliant
27) Powers of Supervision	Largely compliant
28) Regulation and supervision of DNFBPs	Largely compliant
29) Financial intelligence units	Compliant
30) Responsibilities of law enforcement and investigative authorities	Compliant
31) Powers of law enforcement and investigative authorities	Compliant
32) Cash couriers	Largely compliant
33) Statistics	Largely compliant
34) Guidance and feedback	Largely compliant
35) Sanctions	Largely compliant
36) International instruments	Largely compliant
37) Mutual legal assistance	Largely compliant
38) Mutual legal assistance, freezing and confiscation	Largely compliant
39) Extradition	Largely compliant
40) Other forms of international cooperation	Largely compliant

5.7.2 Typologies Reports

The structure and content of SARs must meet the evidentiary goals for investigative leads, which is essential for the integrity and truth-seeking objectives of the criminal justice system. These criminal law procedures are integral in protecting the information relating to clients and customers for confidentiality and secrecy goals. Such protections and assurances increase the reliability of intelligence sources, as well as their willingness to provide autonomous evidence without compromising the source of the intelligence, as well as the methods through which the evidence is gathered.[154]

Rules on the collection of evidence must correspond to the type of offence concerning the use of digital assets for TF activities. Bahrain has taken measures to ensure that convictions

[154] FATF n(141)

can be achieved based on testimonies of co-conspirators, accomplices, co-principals, accessories and/ or other criminal associates. The country has also taken measures to ensure that corroboration of the evidence can be acquired, when necessary, with provisions on how presumptions and statutory inferences are made.[155]

5.7.3 Guidance and Best Practices Reports

A review of the interpretation of FATF Recommendation 15 lays the foundation for several novel legislative approaches that specifically target CTF in the digital era. FATF also offers propositions to guide the legislative process to help regulate and supervise VASPs and organisations involved in virtual asset (VA)-)-related activities. The report recognises the fact that each jurisdiction must create or adopt legal frameworks that facilitate the collection, processing or analysis of data to help industry players identify and manage ML/TF risks more effectively.[156]

FATF also offers propositions to guide the legislative process to help regulate and supervise VASPs and organisations involved in VA-related activities. The report recognises the fact that each jurisdiction must create or adopt legal frameworks that facilitate the collection, processing or analysis of data to help industry players identify and manage ML/TF risks more effectively.[157]

The most recent MER for Bahrain is based on CTF activities that were carried out before the release of the guidance for a risk-based approach to VAs for VASP. As shown in Table 1, Bahrain was found to be 'compliant. However, the draft guidance outlines several novel measures for dealing with the emergent and extant TF risks and exposures in the era of digital currencies. The novel supervisory, monitoring and regulatory responses imply the utilisation of new or additional legislative approaches in Bahrain. The measures relate to the identification of customers, the definition of what constitutes 'funds' concerning the use of

[155] MENAFATF, *MENAFATF Biennial Typologies Report, 4th Edition 2020* (FATF 2021). https://www.menafatf.org/sites/default/files/Newsletter/MF.21.TATWG31.02.E.%28V1.0%29.pdf Accessed 19 March 2023

[156] FATF n(141)

[157] *Ibid*, The FATF recognises that new technologies, specifically those which are closely linked to digital financial inclusion, present novel risks for TF, since they provide new mechanisms for delivery of financial service and or introduce new ways for use or development of products and services, some of which are derivatives of existing products. The FATF proposes the assessment of risks before such products are launched, in order to determine the necessary oversight mechanisms for management and mitigation of those risks.

digital currencies for TF activities, licensing of VASPs, identification of suspicious transactions, and the novel ways through which digital assets are used for TF activities.[158]

In responding to these risks, Bahrain utilises several legislative approaches to achieve RegTech goals in the financial sector, as well as among DNFPBs.[159] The measures are designed to limit TF through the use of traditional regulated financial systems, whereby terrorists convert fiat currencies to digital assets or one digital asset to another to obfuscate the source and destination of funds. The measures achieve a dual purpose of making it challenging for terror groups to remain assured of the anonymity of their activities and to monitor and flag such transactions as 'STRs' for further investigations by FIUs.

Bahrain also insulates itself against TF risks arising due to the novel value systems present in digital currencies. In the new recommendations, the definition of TF recognises the opportunity for utilisation of the fluctuations in the value of digital assets to achieve the goals of financing terror. By including 'corresponding value' in the definition of what 'funds' are in the definition of TF, Bahrain ensures that VASPs do not engage in actions such as market manipulation and destabilisation of the financial systems in ways that culminate in the facilitation of terrorism through digital currencies.[160]

Finally, following the adoption of FATF recommendations, Bahrain is no longer limited by the requirements for double criminality in incidences relating to the use of digital currencies for TF, which is integral for international cooperation. This indicates that double criminality guidelines require that an act must be criminalised in two jurisdictions (where the event occurred and where the claims are made) for it to be prosecuted, especially under international cooperation. [161] Bahrain perceives these measures as integral to proactivity in CTF,[162] with emphasis on discretion (risk-based approach), as opposed to rigidity (the rule-based approach). The use of legislative approaches that impose criminal and civil liabilities upon individuals and organisations that are found liable, whether directly or indirectly, through aiding and abetting the offence. The FATF recognises that new technologies, specifically those which are linked to digital financial inclusion, present novel risks for TF since they provide

[158] *Ibid*
[159] *Ibid*
[160] BEDB n(102)
[161] UN Office on Drugs and Crime, *Preventing Terrorist Acts: A Criminal Justice Strategy Integrating Rule of Law Standards in Implementation of United Nations Anti-Terrorism Instruments (* UNODC, 2006). https://www.unodc.org/pdf/terrorism/TATs/en/3IRoLen.pdf> Accessed 19 March 2023
[162] Dual criminality is provided for under Article 8-10 of the Penal Code.

new mechanisms for the delivery of financial services and or introduce new ways for use or development of products and services, some of which are derivatives of existing products. The FATF proposes the assessment of risks before such products are launched to determine the necessary oversight mechanisms for the management and mitigation of those risks.

With the adoption of FATF recommendations, Bahrain perceives these measures as integral to proactivity in CTF,[163] with emphasis on discretion (risk-based approach), as opposed to rigidity (the rule-based approach).

5.7.4 Risk-Based Approaches

The first risk-based approach to AML/CTF relating to virtual assets, covering the roles and responsibilities of crypto-asset service providers, was released in 2019.[164] The introduction of the risk-based approach implies that risk became a metric through which Bahrain would determine how financial agencies structured their monitoring and reporting activities, as well as how regulatory and law enforcement agencies allocated their CTF resources. In 2019, clarifications were made on the risk-based approaches regarding monitoring and supervision of VASPs, registration or licensing, measures to prevent ML/TF risks,[165] and enforcement measures, including sanctions and propositions for international cooperation and coordination. The guidance offers indicators of risks, as well as the most effective mechanisms to mitigate those risks. It also provides the basis for determining whether an entity falls within the scope of regulation by the FATF on account of providing VA-related activities. The guidance mandates that VASPs, as well as other institutions involved in VA-related activities, must adhere to the preventions outlined in Recommendations 10 to 21. By adopting these guidelines, some of which applied to traditional financial institutions, CPOs licensed and registered in Bahrain.

The propositions in the guidance also lay the foundation for organisational prescription in the legislative process for jurisdictions such as Bahrain. The provisions under Recommendation 15 mandate the licencing and registration of VASPs (and those dealing in VA-related activities), according to a particular risk-based approach, while the unlicensed or unregistered entities are viewed as operating illegally and destined to engage in ML/TF or other unauthorised activities that warrant sanctions.

[163] Dual criminality is provided for under Article 8-10 of the Penal Code.
[164] FATF, n(21)
[165] Ibid, including record keeping, suspicious transaction reporting and customer due diligence among others.

There have been extensive changes in institutional frameworks in the country on account of propositions under the FATF/MENAFATF reports. Following the criminalisation of TF, the Public Prosecutor's Office (PPO) was moved from the Ministry of Justice to the Ministry of Interior. The change is designed to enhance the investigatory, judicial and prosecutorial functions since the institution is faced with cases associated with ML and TF, as well as their predicate offences. A case in point is the fact that the PPO plays a key role in mutual legal assistance for cases involving foreigners and the extradition of such individuals to a different jurisdiction. Second, the role of regulating financial institutions in the country was bestowed upon the CBB by the Bahrain Monetary Agency.[166] As the overall supervisor of financial institutions in the country, the BMA's role revolved around regulation. However, with the multiplicity of emergent risks associated with ML/TF activities, the regulatory mechanisms must go beyond licensing-based oversight. Whereas licensing is necessary for operations, its effectiveness in limiting the risks of TF is weakened by the fact that terror groups have increasingly focused on implementing attacks with limited resources.

5.7.5 Response to Changes in the Environment

In May 2020, CBB adopted and implemented some of the measures outlined in the report entitled '*COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses'* in line with the provisions of the FATF.[167] In the report, the COVID-19 pandemic is defined as a momentous event whose effect changes the criminal economy and precursor variables that influence criminal conduct.[168] The contextualisation of these measures is in response to emergent vulnerabilities and threats due to the changes in financial transactions during the COVID-19 pandemic, including tax relief, social assistance and

[166] Hereinafter 'BMA.
[167] FATF, *COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses*, (FATF, 2020), The measures are developed by a consortium of professionals from the World Bank, FATF and the Committee on Payment and Market Infrastructures,
[168] S Scott and L J Gross 'COVID-19 and crime: Analysis of crime dynamics amidst social distancing protocols', (2021) 16 PLoS ONE, 4, 1.

restrictions on travel.[169] Empirical research has also shown that there are increased risks for criminal and terrorism-related activities,[170] including the following.

First, the pandemic has led to increased crime in the form of fraud, misdirection of public funds, and exploitation of cross-border financial assistance. The increase in crime can be attributed to social assistance programs, as governments seek to stimulate economic recovery, with an estimated monthly increase of US$199B across 132 developing nations.[171] The increased availability of financial assets creates opportunities for misuse of the relief aid during and after distribution, with the possibility of transfer to ineligible individuals.

Second, the measures for preventing the spread of COVID-19 have changed the conduct of criminals, thereby necessitating increased use of online transactions.[172] Work-from-home arrangements, as well as social distance guidelines, imply that most organisations have had to adopt digital options to operations that were previously conducted in person. In addition to the lack of skills for such tasks among the various employees, the increased use of digital platforms has led to an overload of oversight and supervisory functions, thereby increasing the potential for insufficient monitoring and control.

Finally, the COVID-19 pandemic has weakened the ability of public and private entities to implement and oversee AML/CTF obligations due to weaknesses in regulation, supervision and reformation of policies for STR. The use of online and digital fulfilment mechanisms affects the identification of customers, thereby limiting the effectiveness of traditional KYC

[169] MENAFATF, *Coronavirus Pandemic (COVID-19) and its impact on AML/CFT systems in the Middle East and North Africa Region* (FATF, 2020) identified potential risk exposures for increased ML/TF activities from the pandemic, including the possibility for prolonged global recession, increase in bankruptcies and increased corporate consolidations, inability of sectors and industries to recover after the pandemic, increased structural unemployment among the youth, increased restrictions for movement of goods across borders, weakened fiscal positions in key countries, lengthened disruption of global supply chains, economic collapse in developing countries, increased cyber-attacks and online fraud cases due to changes in working processes, and the potential for subsequent pandemics due to compromised public healthcare systems.

[170] S Wang, and X Zhu, 'Evaluation of Potential Cryptocurrency Development Ability in Terrorist Financing,' (2021), 15, Policing: A Journal of Policy and Practice, 4, 2329, who found that terrorist groups have increasingly sought ways to utilise the global crisis to make illegal profits, specifically through provision of essential services following the breakdown of global systems. See also J C Crisanto, and J Prenio,' Financial Crime in Times of Covid19-AML and Cyber Resilience Measures (FSI Briefs No.7 2020) <https://www.bis.org/fsi/fsibriefs7.pdf> Accessed 19 March 2023 who found that criminals have continued to exploit the vulnerabilities that emerged during the Covid19 lockdowns, thereby increasing the risk of cyber-crime, ML and TF.

[171] M Akram, A Nasar, and A Rehman, 'Misuse of charitable giving to finance violent extremism; A futuristic actions study amidst COVID-19 pandemic' (2021), Social Sciences & Humanities Open, 4, 1 reports that the figure rises to trillions, when developed countries such as the US and countries in the European region are included in the analysis.

[172] Restrictions on travel has led to increased e-commerce.

practices.[173] In response, Bahrain must adapt to the emergent challenges, with strategies including looking for solutions in other locations where solutions for such problems have been implemented successfully. The universality of the emergent challenges, as well as the potential for adopting measures and then customising them to fit the domestic situation, is evident from past AML/CTF strategies.

5.8 Conclusion

Bahrain has adopted a combination of novel CTF measures which complement and supplement the traditional CTF measures that were originally designed for TF risks associated with fiat currencies. These traditional measures are relevant in CTF measures in the era of digital currencies since some of the funds that end up being used to finance terrorist activities are converted from fiat to digital currencies. As a result, TF risk management approaches targeting traditional financial service providers, including Islamic and conventional banks, are a key component in Bahrain's CTF measures in the era of digital currencies.

The emergent risks associated with digital currencies have necessitated the implementation of novel strategies, including training and the facilitation of knowledge acquisition for TF risks from digital currencies. Licensed institutions offering financial services rely on this knowledge to identify, reduce or prevent risk exposures for TF through digital currencies. The training is also necessary for elevating the awareness of international norms and standards, as well as the state-level risk mitigation protocols. For these purposes, specific legislative approaches are adopted to ensure parity in knowledge among licensees, promote innovative capabilities, and protect clients.

The legislative approaches identified from the various laws, decrees, ministerial orders, FATF recommendations and provisions under the Rulebook reveal that Bahrain is committed to moving from punishing offences that have been ‘ordered’, ‘committed’, and ‘contributed to’, aided or abated’, to conspiracies, preparations, planning and other related provisions that facilitate ML/TF through digital assets. The legislative approaches are motivated by the objectives under those typologies, including prevention, general deterrence, deterrence of specific activities, punishment, community safety, reassurance and community safety.

The ease with which Bahrain has implemented these legislative approaches can be attributed to the duality of its legal system, as well as the absence of constitutional bottlenecks.

[173] See FATF n(167)

The liberalisation of most governance systems in the country has played a key role in the adoption of international standards, as evidenced in the amendments to the definition of TF under DL No. 4 of 2001, which, through a multiplicity of amendments, facilitates the law enforcement-oriented responses to TF activities. Although several weaknesses exist in the legal and judicial framework, the multiplicity of legislative approaches identified herein provides robust and multifaceted methodologies for the introduction of amendments to achieve any goal under CTF in the era of digital currencies.

The legislative approaches can be summarised as leading to the following outcomes. First is the establishment of a CTF authority, which guides all institutions involved in the handling of digital currencies. Second, a legal framework that contains directly applicable guidelines in a multiplicity of areas of concern relating to risks presented by digital assets, including beneficial ownership, corruption, and customer due diligence. Third, an institutional framework comprised of financial intelligence units, RegTech for FinTech, and improvements in the law enforcement agencies to oversee the use of digital assets must be established. The increase in institutions, including regulatory sandboxes and innovation offices, leads to increased structuring of the financial sector for the riskiest financial tools. Fourth, periodic updates to the existing legal and institutional frameworks to accommodate the dynamics within the domestic and international environment. The combination of legislative approaches has led to the harmonisation of the CTF rules, thereby laying down the foundation for synergistic and symbiotic outcomes. The importance of symbiotic and synergistic outcomes is evident when tackling emergent risk exposures that are not directly covered in the existing legislature or when easing the process of accommodating emergent risks into the existing legislative framework. Fifth, full traceability of transactions involving digital currencies, thereby making it possible to determine their sources and destination, as well as the purpose for which they were acquired and used. Finally, due to the novel nature of some of the risks associated with ML/TF concerning crytoassets, the legislative framework promotes a coordinated and cooperative approach at different levels and sectors, as well as linking the AML/CTF strategies to other counter-terrorism strategies.

Different legislative approaches are applied to achieve a singular purpose, while in some cases, different outcomes are achieved through a singular methodology to ensure convergence in processes. Evidence herein reveals that legislative approaches that are defined based on their objectives (such as the approaches to deter TF under FinTech) fulfil the same goals as those under sentence enhancement, albeit through different procedures. These

outcomes and strategies are attributed to the fact that the risks presented by digital assets vary, thereby necessitating differentiation in the mechanisms for deterrence. On the same note, there is evidence of changes in the legislative approaches. First, there is evidence that Bahraini institutions have acquired novel responsibilities, with the changes designed to enhance the capacity of the institutions to accommodate the rules and risks associated with TF due to cryptoassets. Second, some decrees that predate the use of digital assets in Bahrain have been amended to accommodate the emergent and extant risks presented by these assets in the domain of TF.

Finally, Bahrain has utilised several legislative approaches to shore up the abilities of the domestic institutions to identify, reduce and prevent TF risks from digital assets. The utilisation of legislative approaches has a particular trajectory, which involves movement towards the promotion of innovation while achieving the fundamental objectives of general and specific deterrence, prevention, punishment of perpetrators, reassurance, and community safety. The increased utilisation of digital assets within the financial services sector implies that legal and natural persons face novel risk TF exposures. It also implies that several advantages enjoyed by citizens and foreigners, including the liberal economic system, tax advantages and the promotion of products for financial inclusion, are, in turn, potential tools for TF activities.

Based on the discussion herein, the legislative approaches are designed to achieve a multiplicity of goals, including prevention, general and specific deterrence, punishment, community safety, promoting innovation and reassuring the stakeholders. These objectives play different roles in the portfolio of concerns surrounding the known and unknown ways through which digital assets can be used in TF activities. The next chapter will conduct a similar analysis of the ML and terrorism financing framework in the United Kingdom.

Chapter VI: United Kingdom

6.1 Introduction

The history of counter-terrorism financing (CTF) in the United Kingdom is long and widely established, with some of the current policies rooted in legislative measures implemented in the 18th Century. Early legislative frameworks focused on tackling the entirety of the threat from terrorism.[1] However, over time, the UK anti-money laundering and counter-terrorism financing (AML/CTF) approaches have shifted from the enforcement-oriented[2] and prevention-oriented,[3] oriented methodologies under the primary legislation, such as the Proceeds of Crime Act 2002,[4] to feature a more diversified approach.[5] The UK's CTF regime historically comprises structural features that were transformed into regulatory lacunas by the emergence of digital currencies. First, the regime was created along sectoral lines, with the primary basis being the critical product packages and models.[6] Second, the extensive involvement of the regulated subjects in the CTF regime led to the emergence of close ties that were compromised by the new actors in the cryptoassets industry.[7]

A review of the opinions that underlie the AML/CTF decisions, policies and strategies by the key institutions in the UK reveals a disparity in perceptions.[8] According to the National Crime Agency,[9] terrorism financing (TF) through virtual currencies represents a novel yet large-scale area of risk for ML/TF. On the contrary, the Financial Conduct Authority (FCA) referred to the

[1] See for example, the Explosive Substances Act of 1883, the Criminal Law and Procedure (Ireland) Act of 1887 and the Civil Authorities (Special Powers) Act (North Ireland) of 1922.
[2] Whereby certain acts or omissions related to ML are criminalized as well as investigation of ongoing cases.
[3] Ensuring that illicit money is kept out of the UK financial system.
[4] SN Ryder, 'Is It Time to Reform the Counter-Terrorism Financing Reporting Obligations? On the EU and the UK System', (2018) 19 German Law J, 5, 1173.
[5] The current AML/CTF approach features supervision, regulation, governance, reporting and facilitation, due to the involvement of a broader range of stakeholders.
[6] R Coelho, J Fishman, and D G Ocampo, 'Supervising Cryptoassets for Anti-Money Laundering, FSI Insights on Policy Implementation' (2021), <https://www.bis.org/fsi/publ/insights31.pdf> Accessed March 25, 2022.
[7] The mainstream financial institutions have played an integral role in the development of the regulatory regime prior to the introduction of cryptoassets. These new market players may not be automatically considered as functionally equivalent to other traditional 'regulatees'.
[8] I H Chiu, 'Regulating Crypto-Finance: A Policy Blueprint', ECGI Working Paper Series in Law, (2021), <https://ecgi.global/sites/default/files/working_papers/documents/chiufinal.pdf> Accessed March 25, 2022who attributes these differences to the financialisation of the UK economic system, through the increased role of the financial motives for participating in the economy, (including the criminal and terrorist's goals), the changes in the financial institutions and actors, changes in products and services, as well as the fulfilment channels, and the internationalisation of the entire sector.
[9] Hereinafter 'NCA'.

potential TF risk arising from cryptoassets as higher than previously estimated. A different perspective is held by HM Treasury, which perceives the utility for cryptoassets in TF as being currently low. The variations in perceptions are attributed to the fact that each of those institutions is involved in a different level and phase of the AML/CTF regime. Furthermore, the shared responsibilities, as outlined in Appendix 1, reveal that the institutions play complementary and supplementary roles, either under a primary or support role.

UK regulatory institutions utilise a diversity of penalties or sanctions depending on the circumstances.[10] The current UK's AML/CTF regime is established under several mandates, with the responsibilities included under the Money Laundering Regulations 2017, as amended in MLR 2019. These include supervision, including enforcement and staff training,[11] information and intelligence gathering and sharing,[12] cooperation and coordination with other supervisors,[13] applying the risk-based approach,[14] governance,[15] and recording keeping and quality assurance.[16] Unlike the previous investigator-oriented approach, the UK relies on input from multiple stakeholders, including the customer, on account of the importance of data, information and intelligence in the AML/CTF regime. The regulations hereunder focus on four dimensions, including representation,[17] rights,[18] issuance[19] and transferability.[20]

---

[10] HM Treasury, '*Anti-Money Laundering and Counter-Terrorism Financing: Supervision Report 2019-20*', (HM Treasury, 2021) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1034539/HMT_Supervision_Report_19-20.pdf> Accessed 19 March 2023

[11] Regulation 46 deals with the mandate of supervising through monitoring of the activities of the institutions under their charge, to ensure that they adhere to the requirements under the AML/CTF regime

[12] Regulation 17 directs the responsible institutions to collect data about customers and transactions, so they can use that data as information and intelligence when conducting investigations.

[13] Regulation 50 of MLRs requires supervisors to take the necessary measures to cooperate and coordinate with other institutions when developing and implementing AML/CTF policies.

[14] Under Regulation 17 of MLRs, all institutions involved in AML/CTF have to apply the risk-based approach, starting with assessment of risks for ML/TF, based on probability of occurrence and the impact of the event.

[15] Regulation 102 of MLRs requires all supervisors to establish best practices for AML/CTF, including rules, actions and norms that are formal, sustainable, structured, regulated and with specific accountability procedures.

[16] Regulation 56 discusses the role of supervisory institutions in record keeping and ensuring that quality standards in all AML/CTF activities are achieved. The inclusion of quality standards reveals the recognition of the imperativeness of continual improvement due to the dynamic nature of the ML/TF risks.

[17] J G Allen, and others 'Legal and Regulatory Considerations for Digital Assets' <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/10/2020-ccaf-legal-regulatory-considerations-report.pdf> Accessed 19 March 2023

[18] A determination of the rights associated with the asset,

[19] How the asset is created (focusing on mechanisms and frequency of creation) and distributed (depending on how it is accessed and channels of distribution).

[20] Identification of ways through which is asset is transferred, including physical delivery, updates to the master ledger, measures to prevent replication and controls regarding authority to transfer or update the ledger.

Since 2015, the ML/TF risks associated with the specific use cases of cryptoassets have arisen from the fact that their intrinsic characteristics are not coherent with the established categories of financial products for which the past laws were made.[21] The changes in the legislative approaches adopted in the UK are attributed to the improvements in the appreciation of the ML/TF risks, as well as mechanisms for mitigating such risks. In the cryptoassets era, the changes involve improvement in the conceptualisation of the technical aspects of cryptoassets, including the vulnerabilities that criminals and terror groups exploit to finance their illicit activities.

The legislative approaches discussed hereunder reveal that the UK is cognisant of the risks of an overregulated cryptoassets industry, including the fragmentation of the industry into compliant and non-compliant venues.[22] Most of the AML/CTF activities in the era of the cryptoassets take into account the following considerations: protection of consumers, creating legal and regulatory certainty,[23] promotion of competition and choices,[24] and the regulation and use of emergent and existing technologies,[25] and alignment with provisions in other jurisdictions.[26]

Therefore, the chapter will seek to provide an answer to the following subsidiary research questions: 1) To what extent is the UK compliant with the FATF recommendations? 2) What is the model of regulation in the UK towards cryptocurrencies?

6.1 Primary Authorities

Primary authorities are established to ensure transparency and integrity in the UK financial markets.[27] The contribution of primary authorities goes beyond the AML/CTF regime since they

[21] I H Chiu, 'Decrypting the Signs of Regulatory Competition in Regulating Cryptoassets, (2020) 7 European Journal of Comparative Law and Governance, 3, 299.
[22] See L Sauce, 'The unintended consequences of the regulation of cryptocurrencies', (2022) 46 Cambridge Journal of Economics, 1, 60.
[23] The clarity on regulations, as well as the rationale for use of the assets and related services is integral in ensuring that customers and service providers are aware of their options and choices when entering the market. This has the ability to utilize the input from the regulated population in achieving the AML/CTF goals.
[24] Some cryptoassets are integral in improving the customer experience for core financial services, including financial inclusion.
[25] The increased application of DLT and cryptography in other industries implies that these technologies have specific value within the jurisdiction, for economic purposes among others. The UK has taken measures to steer clear of regulating the technology on which cryptoassets are based, since this has the power to curtail innovation.
[26] The UK has taken measures to ensure that its regulatory environment supports domestic and cross-border innovation, including in the European region and other countries. These concerns are integral in ensuring that the cryptoassets industry contributes positively to the dominance of UK's financial sector. The cross-border alignment is thus integral in the prevention of regulatory arbitrage.
[27] K Harrison and N Ryder, *The Law Relating to Financial Crime in the United Kingdom'*(2nd Edn, Routledge, 2016) 21.

safeguard the financial system in a multiplicity of ways. As the competent authorities in that jurisdiction, the UK's primary authorities enhance the effectiveness of the AML/CTF policies in line with the emergent and extant risks, as well as international standards. The next three sections examine the primary, secondary and tertiary authorities responsible for combating and preventing money laundering and terrorist financing in the UK. Such discussion is necessary not only to provide a background on how the UK's regulatory framework operates but also to clarify the roles, responsibilities, and interagency cooperation essential to effective enforcement. This material will also set the scene for a comparative analysis in the next chapters of the work, as a similar analysis of the responsible agencies in ML prevention was also presented in chapter four.

6.1.1 His Majesty's Revenues and Customs (HMRC)

HMRC is a supervisor under the UK's AML/CTF regime, whose mandate extends to firms that the FCA, OPBAS and the Gambling Commission do not cover.[28] HMRC operates a highly effective registration process, which features monitoring and supervision, to ensure that each person with a tax obligation fulfils their mandate.[29] In the process of monitoring the economic activities of companies and individuals in the UK, the HMRC has access to a wealth of data and information that can provide intelligence for use in assessing the ML/TF risks.[30] The role includes oversight over the Trust or Company service providers,[31] which are perceived as a source of risk due to misuse by criminals for establishing institutional frameworks for ML activities. HMRC also oversees the activities of high-value dealers.[32] HMRC has achieved a broad range of best practices, as proposed by MLR 2019 and OPBAS.[33] Existing data from the National Economic Crime

[28] House of Commons Treasury Committee, 'Economic Crime-Eleventh Report of Session 2021-22', (House of Commons 2022). https://committees.parliament.uk/publications/8691/documents/88242/default/ Accessed 19 March 2023

[29] All businesses operating in the UK have to be registered with the HMRC within 45 days of incorporation. These businesses, as well as individuals involved in employment in the UK jurisdiction are mandated to provide tax returns, which are a legally binding document.

[30] T Bowler, 'Countering Tax Avoidance in the UK: Which Way Forward?' (Feb 2009) <https://ifs.org.uk/comms/dp7.pdf> Accessed 19 March 2023

[31] TCSPs hereafter, See HM Treasury, '*National Risk Assessment of Money Laundering and Terrorist Financing 2020*, (HM Treasury, 2020), <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/945411/NRA_2020_v1.2_FOR_PUBLICATION.pdf> Accessed 19 March 2023

[32] High value dealers are businesses that make or accept cash payments exceeding €10,000 in exchange for goods. Such businesses have to register with the HMRC.

[33] HMRC, 'Corporate Report: HMRC Anti-Money Laundering Supervision Annual Assessment', (HMRC, 2021) <https://www.gov.uk/government/publications/hmrc-anti-money-laundering-supervision-performance-assessment/hmrc-anti-money-laundering-supervision-annual-assessment. HM Treasury, n(10)

Centre[34] reveals that the number of suspicious activity reports[35] from TCSPs was lesser than expected, hence the need for additional oversight, especially due to the increased risk from cryptoassets services providers. The data and information it collects play a key role as an input in the intelligence-gathering functions under AML/CTF.

HMRC treats cryptoassets as property rather than currency, hence the application of capital gains tax on the person who trades in these assets.[36] However, the process of determining the tax base is still a challenge since owners of the cryptoassets do not use the pound sterling when trading and may prefer to exchange one cryptoassets for another.[37] Similarly, due to the volatile nature of cryptoassets, the process of valuation during disposal is not straightforward. In cases where cryptoassets are earned through other ways, such rewards must be taxed as income, depending on whether the process is considered an investment or a trade.[38]

The involvement of the HMRC in the UK's AML/CTF regime is a complement to other regulatory, supervisory and monitoring activities. The imposition of tax obligations reinforces the recognition of the existence of cryptoassets as a component of the economic and financial systems in the country. It thus acts as a gateway by only allowing companies that have fulfilled certain requirements to get licences to operate in the country.[39]

HMRC is also involved in the UK's AML/CTF regime on a case-by-case basis in roles such as those outlined in the Economic Crime Plan 2019-22.[40] The involvement extended to the delivery of an enhanced risk-based approach and guidance to all entities under its enforcement perimeter, as well as providing feedback reports on the self-assessed ML supervision. It also

[34] Hereinafter 'NECC'.
[35] Hereinafter 'SARs.
[36] HMRC, 'Tacking Tac Evasion: Government Guidance for the Corporate Offenses of Failure to Prevention the Criminal Facilitation of Tax Evasion', (HMRC, 2017) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/672231/Tackling-tax-evasion-corporate-offences.pdf> accessed 19 March 2023
[37] The HMRC proposes that in case a holder of cryptoassets decides to swap one currency for another, the transaction triggers the need for accounting for capital gains tax based on the profit, even when no currency exchanges hands. Similarly, if the transaction leads to a loss, the seller has to make additional disposals through actual currency to cover the related tax obligations.
[38] Includes other ways through which cryptoassets can be earned, including staking, yield farming, mining or from validation of transactions.
[39] NCA, 'UK Financial Intelligence Unit-Suspicious Activity Reports Annual Report 2020, (2020). <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/480-sars-annual-report-2020/file> accessed 19 March 2023
[40] HM Treasury, n(10)

participates in the Joint Fraud Taskforce and the Joint Money Laundering Intelligence Taskforce.[41] By monitoring economic activities and managing data on transactions and ownership, HMRC contributes crucial insights that are especially relevant as cryptoassets become more prevalent in financial crime. Under its AML/CTF role, HMRC supervises high-risk entities such as Trust or Company Service Providers (TCSPs) and high-value dealers, identifying risks from businesses susceptible to misuse by criminals. However, low levels of suspicious activity reporting from TCSPs signal a need for HMRC to tighten oversight of cryptoasset service providers, which pose increased ML risks. HMRC's approach to cryptoassets treats them as taxable property, addressing capital gains from trade and income from earnings. As part of the Economic Crime Plan 2019-22, HMRC's tax imposition helps legitimise cryptoasset use, ensuring compliance for businesses seeking licenses.[42] Through participation in the Joint Money Laundering Intelligence Taskforce, HMRC supports a collaborative, risk-based response to ML/TF challenges in the cryptoassets sphere.

6.1.2 The Home Office

The Home Office, through the NCA, acts as an important institution that monitors and enforces compliance with AML/CTF regulations. The NCA plays a key role in filtering intelligence from reports by the companies in the financial sector and then delivering the relevant information to judicial processes. The filtration process is integral in maintaining the necessary levels of privacy by individuals and companies, thus limiting exposure to unauthorised persons. The UK Financial Intelligence Unit[43] is a centralised, autonomous and independent agency that is involved in AML within and outside the jurisdiction. The UK utilises the administrative model for its FIU, which serves as a buffer between the LEAs and the obliged entities.[44] The role of UKFIUs is to request and or acquire SARs from obliged entities that provide reports on ML/TF, analyse the data to create information and intelligence, and distribute it to LEAs and other competent authorities for investigations and prosecutions under the various laws. The role of UKFIUs

[41]JMLIT hereafter. As indicated in Appendix 1, the HMRC performs financial intelligence purposes for collecting data to identify persons who are involved in tax avoidance and other crimes related to taxation in the UK.
[42] HM Treasury, n(10)
[43] UKFIU hereafter. The UKFIU is established in line with provisions under Article 7(1)(b) of Palermo Convention 2000 as applied by the Egmont Group.
[44] G C Velkes, 'International Anti-Money Laundering Regulation of Virtual Currencies and Assets', (2020) 52 Int. L and Politics, 10, 879, who defines an administrative model FIU as a centralized and independent administrative entity that is situated within a government agency. The government agency provides access to financial information and SARs from the financial institutions.

includes assisting in making decisions that enable other regulators to perform their duties quickly and efficiently.

UKFIU announced the creation of new codes for reporting SARs relating to 'cryptoassets'. These codes represent part of the good practice guidance since they facilitate the prompt and efficient analysis of data, information, and intelligence that is collected and shared by the UKFIU and other LEAs under the multi-agency institutional frameworks. Through the unified code system, all transactions involving cryptoassets are similar and have a high level of continuity, thereby making it possible to identify incidences of misuse of the system for ML/TF. The most common indicators of misuse include transactions, clients who use multiple exchanges for transactions with a similar purpose, which leads to the similarity in the reporting mechanisms for transactions involving cryptoassets.

The NCA has taken measures to enhance the utility of the SAR regime through the introduction of a committee to oversee the development of annual reports on all SARs, as well as the harmonisation of the reporting processes to ensure uniformity across all institutions in the country.[45]

6.2 Secondary Authorities

These authorities are designed to supplement and complement the AML/CTF activities of the primary authorities, including tracing, seizing and confiscating the proceeds of crime, as well as persons involved in terrorist financing. The cooperation and coordination with primary authorities extend outside the jurisdiction. The role of secondary regulatory authorities in AML/CTF prevention has become even more important in the past 10 years as the secondary authorities have a much more prominent role in detecting the potential use of crytoassets for illicit activities, including terrorist financing.

[45] NCA, 'UK Financial Intelligence Unit-Suspicious Activity Reports Annual Report 2020, (2020). <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/480-sars-annual-report-2020/file> accessed 19 March 2020

6.2.1 HM Treasury

The involvement of HM Treasury in the UK's AML/CTF regime in the era of cryptoassets arises from its contemporary role as a policy setter.[46] The HM Treasury-approved guidance for all sectors is accompanied by an annual report, as mandated under Regulation 51 of the MLRs.[47] It is the responsibility of HM Treasury to provide a National Risk Assessment,[48] which outlines the main ML/TF risks, with the first report acting as a benchmark for improvements.[49] The report serves the binary function of informing and advising institutions on the procedures for effectively and efficiently detecting, deterring and disrupting ML/TF activities within their businesses. It also highlights the ML threat and vulnerability variables that are considered most valid in the UK at any point.[50] Based on the most recent report, the risk score for ML/TF in the UK increased from 'low' to 'medium' between 2017 and 2020.[51] The change is attributed to the willingness and ability of criminals and terrorist groups to use and incorporate cryptoassets into the ML/TF methodologies. Cryptoassets are also increasingly available to customers and businesses in the UK, with criminals preferring to launder money illicitly from offline crimes through online platforms.

HM Treasury appoints supervisors to monitor and control ML/TF risks in line with the MLRs 2017, including the FCA and HMRC.[52] In 2018, the HM Treasury launched an Inter-Institutional Taskforce designed to explore the effects of the rapid development of the cryptoassets industry.[53] Over the past two years, changes in the UK environment have nullified the validity of

[46] T Helm, A Low, and J Townson, 'UK FinTech-State of the Nation' (2019) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/801277/UK-fintech-state-of-the-nation.pdf>. accessed 19 March 2020

[47] The report provides data on the supervisory and enforcement involving the statutory requirements issued to the entire sector. The report also outlines measures that supervisory institutions have to take to ensure consistency in supervision and enforcement across a broad range of guidelines relating the prevention of illicit financial activities.

[48] Hereinafter 'NRA' See HM Treasury, n(31) which indicates that Regulation 16 of MLRs mandates the HM Treasury to provide such an assessment in order to guide the actions of all institutions involved in the AML/CTF regime in the UK.

[49] HM Treasury, n(2)

[50] See M Hopkins, and N Shelton, 'Identifying Money Laundering Risk in the United Kingdom: Observations from National Risk Assessments and a Proposed Alternative Methodology', (2019), 25, *Eur J Crim Policy Res*, 70.

[51] See HM Treasury, n (2)

[52] HM Government and UK Finance 'Economic Crime Plan 2019-22 (HM Government 2022) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/816215/2019-22_Economic_Crime_Plan.pdf> accessed 23 February 2021

[53] HM Treasury, n(2)

the findings of the Taskforce.[54] In response, HM Treasury sought input from industry participants through consultation, which provides multiple stakeholders to provide evidence, comments and views on key legislative and regulatory changes.[55] The consultative approach towards the regulation, supervision and monitoring of the cryptoassets industry is deemed necessary in achieving agility within the risk-based strategies preferred by UK regulators in service of the maxim of 'same activity, same risk, same regulation'.[56]

HM Treasury is responsible for ensuring accountability and transparency by encouraging good practices and providing reports on how well those practices have been achieved.[57] HM Treasury has taken steps to outline the actions that the licensed businesses involved in the cryptoassets industry have to take to reduce and eliminate the ML/TF risks. These include the identification and verification of the identities of the legal and natural persons with whom they conduct business. The requirement also extends to those people who use licensed businesses as agents within the jurisdiction of the UK. HM Treasury also requires all regulated businesses to conduct due diligence, depending on the characteristics of the customers.[58] These regulated businesses include cryptoassets exchange services providers for clients exchanging cryptoassets for similar or other cryptoassets,[59] service providers for peer-to-peer exchange services, services providers for cryptoasset automatic teller machines,[60] persons that issue new cryptoassets,[61] and persons who publish open-source software for crypto-related services. HM Treasury has opted for an approach that features elements of facilitation, supervision, regulation and monitoring to ensure that the response to ML/TF risks is proportionate, dissuasive and effective.[62] The supervisory and monitoring responsibilities under HM Treasury include overseeing advertising for products and services in the cryptoassets industry, which can be used to draw consumers into the industry to lay

[54] The Taskforce concluded that although DLT has the potential for significant impact across multiple industries with the ability to deliver tangible benefits in the financial services sector, the scale and scope of adoption was too low to warrant any concerns.
[55] M Hopkins and N Shelton, n(50)
[56] UK Finance, 'Same Activity, Same Risk, Same Regulation' (UK Finance2021), <https://www.ukfinance.org.uk/system/files/Same%20activity%2C%20same%20risk%2C%20same%20regulation%20-%20FINAL.pdf> accessed 23 February 2021
[57]HMTreasury, n(10)
[58] Ibid
[59] This includes service providers for exchanges between one type of cryptoassets for another, or exchange services involving exchange for value of a similar cryptoassets.
[60] Physical locations where holders of cryptoassets can exchange those assets for fiat currency or acquire cryptoassets using fiat currencies.
[61] Any entity that is involved in initial coin offerings (ICOs).
[62] HM Treasury, n(10)

the groundwork for ML/TF activities.[63] The oversight targeting cryptoassets advertising seeks to promote fairness, clarity and accuracy in the information provided in the advertisements. The regulation is perceived as necessary to ensure that all people who are involved in the industry have a reasonable degree of understanding of the risks that they are exposed to.

HM Treasury is also involved in the implementation of sanctions through the Office of Financial Sanctions Implementation.[64] As part of the AML/CTF regime, the OFSI is responsible for ensuring that companies in the UK understand financial sanctions.[65] Similarly, the OFSI enforces and implements a sanctions regime aimed at playing a critical role in the AML/CTF.[66] Furthermore, the HM Treasury collaborates with other regulators and stakeholders, including the Financial Conduct Authority (FCA) and HM Revenue and Customs (HMRC), ensuring that the oversight of cryptoassets transactions aligns with the "same activity, same risk, same regulation" principle. The Treasury's 2018 establishment of an Inter-Institutional Taskforce emphasises this focus, although the rapidly evolving crypto market has necessitated further consultations and adaptability.

6.2.2 The Financial Conduct Authority (FCA)

The FCA[67] is the UK's financial watchdog, and its responsibilities include the prevention of fraud, ML, TF, corruption, and bribery. The FCA is established under the Financial Services Act 2012.[68] The involvement of the FCA starts with AML obligations in the pre-placement phase, which empowers the FCA to impose sanctions on any person or a member of the regulated sector who violates the UK's AML/CTF regime.[69] The regulated sector, as defined in Schedule 9 of the Proceeds of Crime Act 2002 (POCA), refers to businesses and professions that are at higher risk of being used for money laundering or terrorist financing. These include, but are not limited to,

[63] See HM Government and UK Finance, n(52)
[64] Hereinafter 'OFSI'
[65] BoE, 'Joint Statement from UK Financial Regulatory Authorities on Sanctions and the Cryptoasset Sector –11 (BOE 2022) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1060448/Statement_from_UK_authorities_on_Cryptoassets_-_March_2022.pdf> accessed 19 March 2023
[66] Ibid, p1.
[67] FCA hereafter. The FCA is a successor to the Financial Services Authority, which was disbanded due to failures in preventing the collapse of the economy in the late 2000s.
[68] A Adeyemi, 'Slipping Through the Net: The Financial Conduct Authority's Approach in Lessening the Incidence of Money Laundering in the UK', (2018) 21 J of ML Control, 2, 6.
[69] K Harrison and N Ryder n(27)

financial services: banks, investment firms, and insurance providers, accountancy services, legal professionals, estate agents, high-value dealers, trust and company service providers:

FCA's supervisory toolkit, which sets benchmarks for sustainable innovation and market integrity,[70] is built around reconciling the dual view that whereas cryptoassets present potential harm to the financial sector and customers, the underlying technology is potentially beneficial to the financial services.[71] The involvement of the FCA in the regulation of the cryptoassets market in the UK commenced with the amendments to the '*MLR 2017'*.[72] Under the framework, the supervisory, regulatory and monitoring roles of the FCA are outlined.

Second, the government has shown increased interest in cryptoassets, with key institutions such as BoE, the UK Cryptoassets Taskforce[73] and the Payment Systems Regulator. The regulatory, supervisory and monitoring activities of the FCA are derived from several pre-existing legislative frameworks due to the nature of cryptoassets. First, the Financial Services and Markets Act 2000[74] and the FSMA 2000 (Regulatory Activities) Order 2001.[75] However, the contents of the guidance are not legally binding, implying that firms can fail to adhere to the standards without attracting liability for breach of rules.

Most of the novel guidelines on cryptoassets by the FCA are the product of consultations featuring multiple sectors, with the government taking active and passive measures based on the

[70] FCA, 'Business Plan 2021/22', <https://www.fca.org.uk/publication/business-plans/business-plan-2021-22.pdf> accessed 19 March 2023

[71] HM Government and UK Finance, 'Economic Crime Plan 2019-22' n(52) which indicates that the FCA has offered a blanket warning to customers who invest in cryptoassets of the possibility of losing all their money, and that the FCA has limited power to protect them from loses, due to the unregulated nature of the products and services in the industry.

[72] Hereafter, MLRs 2017. See also HM Treasury, 'Consultation on the Fifth Money Laundering Directive: Response To The Consultation' (Jan 2020), <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/860491/5MLD_Consultation_Response.pdf>, accessed 23 February 2023 which states that the involvement of the FCA is ratified through responses by stakeholders in the UK, which led to subsequent assignment of the responsibility for FCA in the AML/CTF in the national Economic Crime Plan.

[73] K Braddick, A Bailer, and D Ramsden, 'Cryptoassets Taskforce: Final Report' (2018). <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf>, which outlines the framework for use in the regulation of cryptoassets. The Taskforce, which works hand in hand with the Treasury, the FCA and Bank of England, relies on a framework based on the risks, benefits and implications of regulation on cryptoassets. See also S Maxson, S Davis, and R Moulton, 'UK Cryptoassets Taskforce publishes its final report, (2019) 20 J of Investment Compliance, 2, 31.

[74] FSMA 2000

[75] SI 2001/544 RAO 2001

views of the industry representatives.[76] The supervisory mandates of the FCA recognise the fact that compliance with legal obligations does not necessarily imply that the institutions adhere to the practices outlined under the Financial Crime Guide.[77] Thus, the FCA utilises several backstops for each ML/TF risk exposure.

6.2.2.1 FCA response to the risks and vulnerabilities of cryptoassets

This section will discuss how it has attempted to address the risk factors that make some individuals and businesses vulnerable to terrorism financing and money laundering. The FCA is aware of the unique ML TF risks posed by the proliferation and complexity of the cryptoassets markets. To address these risks, the FCA uses customer due diligence and enhanced due diligence to ensure that cryptoasset firms verify the true beneficial owners of assets, especially in high-risk situations or complex transactions. Additionally, the FCA employs proactive communication to inform customers of potential risks while implementing a risk-based approach to identify suspicious behavior patterns and mitigate client-related ML/TF vulnerabilities.

The FCA is cognisant of the complex nature of ML/TF risks associated with the customers involved in the cryptoassets industry. The risks arise from the increase in the interest of the public[78] as represented by the growth in the cryptoassets market, media coverage, volatility in prices, increased involvement by institutions in the financial services sector and growth in institutional investments. Similarly, the complexity of cryptoassets also contributes to the limited appreciation of the ML/TF risks from cryptoassets among the average UK citizens.[79] In the recent past, the FCA

[76] See Statutory Instrument No. 1511, 'Financial Services: The Money Laundering and Terrorist Financing (Amendment) Regulations 2019' that uses the example of the changes that the government intended to introduce to MLR 2017, Regulation 28(3)(b) and 4(c), in the form of removal of the requirements for reasonability of measures for achieving risk-based outcomes under CDD. The input from stakeholders includes views that the removal of such provisions will result to disproportionate checks under CDD, with the possibility of excluding some customers from service. Furthermore, the withdrawal of the proposed changes has limited value in prevention of ML/TF risks. Similarly, amendments to MLR 2017 Regulation 28(8), regarding the additional requirements for the verification of the identity of senior management for the purpose of CDD was supported by the stakeholders under the consultations, thereby leading the government to adopt the change to the legislation under MLR 2019.

[77] FCG here after. The guidelines under FCG can be classified into three, based on their purposes. First, mandatory guidelines must be adhered to, since they are derived from existing legislation. Second, guidelines should be followed, since they are a description of what is expected of entities in the industry. Such guidelines reference actions and measures that can be met through several strategies. Finally, guidelines that may be applied, which comprise good practices that enable entities to go beyond the requirements for compliance.

[78] Based on the FCA Business Plan 2021/22, there is an increase in public awareness, based on the estimation of ownership from 1.9M in 2020 to 2.3M in 2021. Over 78% of adults have come across information about cryptoassets.

[79] E Esoimeme, 'Identifying and Reducing the Money Laundering Risks Posed by Individuals Who Have Been Unknowingly Recruited as Money Mules', (2020) 24 J of ML Control, 1, 206.

has relied on the four core elements of customer due diligence[80] in reducing client-related risk factors.[81] These measures enable customers to make informed decisions and to take responsibility for their decisions, choices and outcomes.

Client-related risks vary broadly and are influenced by their financial literacy, technological competence, vulnerability to influence, and how well they utilise the existing financial services. The breadth of vulnerabilities informed the FCA to develop an AML/CTF methodology that keeps customers informed about the risks. The FCA employs proactive communication methodologies, which involve ensuring that the published information is readily available to customers.[82]

The FCA also recognises the possibility that firms in the cryptoassets are targets of criminals and terrorist financiers.[83] It has introduced explicit CDD requirements aimed at establishing the beneficial owner. For business-to-consumer transactions, the beneficial owner is determined by identifying the actual or ultimate individual who derives value from the financial product. For business-to-business transactions, the beneficial owner is identified based on the control structures and ownership of the company.[84]

The MLR regulations targeting client-related offences revolve around participation offences, hence the orientation towards punishment of the participants, as well as general deterrence of the activities that elevate the ML/TF risks. The current risk-based approach enables UK AML/CTF institutions to utilise the available information on the customer's past activities in predicting their propensity to engage in unacceptable risks. The recognition of behavioural patterns

[80] CDD hereafter

[81] See FCA, 'Prohibiting the sale to retail clients of investment products that reference cryptoassets' (FCA, 2020). <https://www.fca.org.uk/publication/policy/ps20-10.pdf> accessed 16 March 2023 which identifies the core elements of CDD, including the identification and verification of the identities of customers, identification and verification of beneficial ownership, appreciating the nature and goals of the customers, and engaging in ongoing monitoring to detect any suspicious transactions, while also keeping and updating the information about customers, based on the nature of the risks they present.

[82] In Decision Reference DRN 2924802, a client (Mr M) blamed an institution that is regulated by the FCA (Vanquis Bank Ltd.) for losses incurred through a complex cryptocurrency fraud.
In the decision, the FOS considered it fair and reasonable for Vanquis Bank to have taken the following measures: monitor the clients' account for all receipts and payments; have a system to monitor unusual transactions; and take additional measures to shield the customer from financial harm.

[83] FCA, 'Guidance on Cryptoassets: Feedback and Final Guidance to CP 19/3' (2019). Policy Statement PS 19/22. <https://www.fca.org.uk/publication/policy/ps19-22.pdf> accessed 19 March 2023

[84] Ibid, who indicates for such entities, the FCA mandates that where the beneficial owner is not clearly specified, the identity of the senior managers has to be determined and verified.

is integral in customer risk assessment, as well as the determination of suspicious tendencies, such as the propensity to hide information or past criminal sanctions.

In response to the novel risks presented by cryptoassets, the FCA has mandated the customisation of CDD depending on the circumstances.[85] First, for clients who are perceived as presenting a higher than normal ML/TF risk, firms in the financial sector have to conduct enhanced due diligence.[86] EDD is recommended for, but not restricted to, clients with higher risk profiles for ML/TF if they operate in certain jurisdictions or sectors, their operations are unnecessarily or otherwise complex with obscure structures for beneficial ownership and control, and they are engaged in unusual transactions that lack apparent lawful or economic goals. The FCA's requirements for CDD and EDD are designed to ensure that organisations identify any activities or transactions that fit into the customer profile and then perform additional reviews to determine if they are indeed legitimate.

6.2.2.2 Geography-related risk factors

The FCA has taken measures to limit the effects of risk factors arising due to the location where transactions are carried out and where the parties to the transactions are located.[87] Evidence from the NRAs in 2015 and 2017 revealed that there are geographical disparities in the ML/TF activities from domestic and international perspectives. In the domestic scene, evidence revealed that the Metropolitan Police area and the City of London were perceived as the riskiest due to the diverse connections to risky jurisdictions, history of organised crime and cash-intense businesses.[88] In the era of cryptoassets, the determination of the jurisdiction of the UK institutions involved in regulation, oversight, law enforcement and judiciary response or intervention. In recognition of the obscure nature of the ownership of some of the cryptoassets in the UK market, and hence the challenges in applying the *lex situs* principles,[89] the UK has been keen on adopting international approaches in the AML/CTF concerning cryptoassets. While there have been attempts to target

[85] Ibid, which states that whereas face-to-face CDD is considered the most reliable in the verification that the person claiming the particular identity is in fact the person with that identity, the UK regulatory institutions understand that it is sometimes necessary for CDD to be conducted remotely.
[86] Hereafter, EDD.
[87] These measures are also targeted to locations where the transaction occurred.
[88] Hopkins, and Shelton, n(50), who indicates that the HM Treasury, which conducted the NRAs utilised a multifaceted ML Risk indicators developed for the Identifying and Assessing the Risk of Money Laundering in Europe (IARM) project to analyse the vulnerabilities and threats facing law enforcement agencies in 43 locations across the country.
[89] The doctrine relates to laws that govern the transfer of the title to property, dependent on, and based on the location of the property, in order to avoid conflicts in the jurisdiction of the courts.

money laundering and terrorism financing locally by concentrating the AML/CTF efforts in the areas that were deemed most risky, there is scarce evidence in the academic literature that the FCA has been able to do so in practice. In fact, commentators have noted that there is a sharp discrepancy between the positive Mutual Evaluation Report of FATF that the United Kingdom has received and the fact that London continues to be the centre of terrorist financing activities.[90]

6.2.2.3 Risk factors associated with products, services and transactions.

The FCA has created a preliminary asset taxonomy for classifying the cryptoassets, which include utility tokens,[91] security tokens,[92] exchange tokens[93] and e-money tokens.[94] Additional categorisation into regulated (e-money and security tokens) and unregulated tokens (utility and exchange tokens). Tokenisation is integral to the treatment of cryptoassets as property under English law.[95] The FCA-regulated cryptoassets have clear ownership or contractual rights, including e-money and security tokens. Due to the specificity of these rights, the holders of the tokens to these cryptoassets can engage in diverse activities using those assets. The classification as a regulated cryptoasset implies that customers can rely on the FCA for information and directions on the potential ML/TF risks attached to those cryptoassets.[96] On the contrary, the unregulated cryptoassets are characteristically anonymous and can be transferred through cryptoasset service providers.[97] Although they are outside the regulatory mandate of the FCA, the legislative frameworks mandate that they use have to comply with the provisions of the Fifth Anti-Money Laundering Directive (5MLD). However, the FCA has also signposted that it considered

[90] David Benton and Nicholas Ryder, 'Terrorism Financing, the United Kingdom, and the Financial Action Task Force: A Series of Omissions or Missed Opportunities?' in Nicholas Ryder (ed), *Sustainable Finance and Financial Crime* (Springer International Publishing 2023) 353

[91] Cryptoassets designed to enable holders to access current or future products or services under predetermined conditions. They can also be traded or exchanged as tokens in the secondary market or be used for speculative investment purposes.

[92] Cryptoassets that bear similar characteristics to traditional shares or debentures.

[93] Cryptoassets designed for use in remitting payments, such as Bitcoin.

[94] Cryptoassets designed for use as electronic money

[95] See T Cutts, 'Crypto-Property: Response to Public Consultation by the UK Jurisdiction Taskforce of the LawTech Delivery Panel' (LSE LAW 2019) <http://dx.doi.org/10.2139/ssrn.3406736> accessed 19 March 2023 The definition arises from the decision in *National Provincial Bank v Ainsworth* [1965] A.C. 1175, 1247-1248 which posited that "Before a right or an interest can be admitted into the category of property, or of a right affecting property, it must be definable, identifiable by third parties, capable in its nature of assumption by third parties, and have some degree of permanence or stability".

[96] FCA, n(83) indicates that regulated products are offered by companies willing to adhere to the stringent guidelines by the FCA, which reduces the exposure to the predictable ML/TF risks. However, such customers still must take measures to protect themselves from unforeseeable threats.

[97] FCA, n(81)

classifying some of the unregulated cryptoassets, such as derivatives, as financial instruments, thereby integrating them into the Markets in Financial Instruments Directive[98] regulatory perimeter.[99]

The legislative approaches that target entities that handle unregulated cryptoassets are classified under the objectives level. By focusing on the objective, the legislative approach provides information on the classification of the cryptoassets spanning from.

6.2.2.4 Risk Factors Linked to Product/Service Delivery Channel

In the UK, the FCA oversees the cryptoassets industry due to the heightened risks of ML and TF posed by rapid, complex transactions on DLT platforms. To address these risks, the FCA mandates regulated exchanges, insists on bank transfers for traceability, and enforces limits on cash transactions at crypto ATMs to mitigate potential ML activities. Furthermore, the FCA issues warnings about initial coin offerings (ICOs) due to fraud risks, even though the overall ML risk for ICOs is assessed as low, emphasising vigilance around potentially fraudulent exchanges and actors. Understanding how the FCA has addressed the ICO risks is important for this research as it can provide important information on how the UK AML/CTF framework has evolved to make the regulator better capable of addressing the risks that cryptoassets pose.

The channels through which products and services from the cryptoassets industry are delivered to customers present several ML/TF risks in the UK, hence the involvement of the FCA. The risks of harm arise from the speed with which transactions and interactions with customers occur, as well as the complexity and uniqueness of the DLT platforms on which the cryptoassets are developed.[100] In response, The FCA has simplified the procedures for determining the occurrence of ML/TF activities. The regulations are based on the degree to which business relationships occur through processes that can be relied upon. The involvement of intermediaries elevates the level of risk, while face-to-face contact is often considered a way of reducing uncertainties.

[98] MiFID II hereafter
[99] The MiFID II Directive (*2014/65/EU*), which in the post Brexit Era, is now to be implemented through different primary and secondary legislation under the FCA, with consultations going on between the FCA and Treasury.
[100] I H Chiu, n(8)

The FCA has recognised the ML/TF risks associated with several emergent product and service delivery channels for cryptoassets.[101] The FCA also regulates peer-to-peer cryptoassets exchanges[102] by only allowing regulated cryptoassets businesses to operate. Similarly, the FCA mandates both customers and companies to use official channels such as bank transfers for such transactions as a way of establishing an audit trail. It also enables institutions and people who lack robust AML/CTF systems and controls to benefit from the measures put in place by other institutions that have more robust controls in place. For cryptoassets ATMs,[103] there are limits to the amount of cash that can be transacted, thereby reducing the utility of this ML approach and increasing the chances that the use cases will trigger a suspicious activity red flag. However, these risks are mitigated through different supervisory and monitoring mechanisms aimed at ensuring that all transactions are recorded, reporting suspicious transactions, and overseeing cryptoasset companies, among others.

6.2.2.5 Risks Associated with Service Providers

The FCA has taken measures to extend its regulatory perimeter to target specific cryptoassets service providers.[104] The objective of the regulation is to ensure that businesses change their functions, roles, procedures and controls as a way of reducing ML/TF risks and exposures. The mandates for registration also serve a multiplicity of purposes, the primary one being to ensure that all firms face high standards of scrutiny as they enter the market and maintain those standards as they operate in the industry.[105] From the perspective of financial services regulation, all businesses interested in operating in the UK are mandated to be registered and to stay updated on

[101] FCA, 'Payment Services and Electronic Money–Our Approach, (2018). <https://www.fca.org.uk/publication/finalised-guidance/fca-approach-payment-services-electronic-money-july-2018-track-changes.pdf> accessed 13 February 2022 who identifies new payment cards that enable customers to trade cryptoassets for fiat currencies or use them for purchasing goods that can be traded for different forms of value.

[102] P2P here after. The ML/TF risks associated with peer-to-peer cryptoassets exchanges arise from the fact that some of the transactions and participants may not be covered under the MLRs.

[103] HM Treasury, n(31) reports that with number of cryptoassets ATMs increasing to 271 in 2020, up from 35 in 2016, there are increased opportunities for misuse of this fulfilment channel, as well as strong suspicions for collusion between ML perpetrators and the companies that manage the ATMs.

[104] R Coelho, J Fishman, and D G Ocampo, 'Supervising Cryptoassets for Anti-Money Laundering, FSI Insights on Policy Implementation' (2021) <https://www.bis.org/fsi/publ/insights31.pdf> accessed 19 May 2022 who indicates that in determining the regulatory remit, the FCA has taken into account the multiplicity of business models adopted by companies in the cryptoassets space within the country.

[105] FCA, n(72) which indicates that those standards create a more robust pathway to registration and renewal of licenses, establish a robust regulatory nursery for incoming firms, and ensure strong oversight over firms with rapid growth.

all the emergent requirements for authorisation and licensing within the UK.[106] Failure to adhere to the registration and licensing guidelines will attract sanctions and penalties depending on the circumstances, including termination of operations.[107] The decision to adopt this level of regulation arises from the fact that certain industry participants hold significant market power that influences the trajectory of innovations as well as consumer decisions. Whereas these risks are partly covered under the regulatory mandates targeting risks associated with the products/ services and the value delivery channels, the FCA found it necessary to target specific entities to regulate how they conduct business and minimise the risks to their clients and the overall ML/TF risk.[108]

The FCA regulates the type of information that cryptoassets companies provide to their customers and other third parties before, during or after the transactions. The guidelines relate to how advertisements are framed, the type of information that has to be disclosed, and the sanctions associated with failure to adhere to those standards.[109] Under the guidelines on promotions, all firms, whether regulated or unregulated, are mandated to ensure that all advertisements meet a certain standard that reduces the risk of fraud or exploitation of customers.[110] The actions by the FCA are also justified under the UK's financial promotions regime, based on FSMA 2000.[111] The regulatory perimeter introduced by the FCA seeks to eliminate deceptive advertisements which are characteristically designed by firms seeking short-term and unsustainable benefits, and that is indicative of ML/TF risks. Under the disclosure requirements, the FCA mandates firms to provide

[106] It outlines the regulation guidelines for investment business as relevant to securities tokens, regulations on payment services, insurers, consumer credit and e-money dealers, on account of their ML risks.
[107] HM Treasury n(31)
[108] The FCA offers a number of guidelines for activities that should raise red flags among CASPs, and which increase the risk of imposition of sanctions on the service provider, including transactions with customers from high-risk third countries, transactions with wallets associated with entities facing sanctions, transactions with services providers who have poor customer due diligence, transactions with customers whose main goal is to hide their location or source of wealth, and other ML red flags that are indicative of illegality.
[109] FCA, n(72) reveals that in the process of tackling misconduct to establish integrity and trust, the FCA is cognisant of the fact that there are firms that are unwilling or unable to adhere to the stipulated standards, and the cryptoassets industry provides a pathway for the achievement of such goals.
[110] See FCA n(83) who indicates that all advertisements have to be fair and clear without misleading the customers; include a prescribed warning about the potential for loss; be devoid of all forms of incentives for investment; and be approved by an entity authorised by the FCA for such purposes.
[111] D Johnson, 'What Are the Merits of Taking a Hybrid Regulatory Approach Toward the Enforcement of Corporate Financial Crime in the United Kingdom and United States of America?' (2022) 3 J. of White Collar and Corporate Crime, 1, 23, who indicates that Section 21 of the FSMA 2000 prohibits the issuance of financial promotion unless: a. issued by a FSMA authorised firm; b. approved by a FSMA authorised firm; or c. falls within an exemption under the Financial Services and Markets Act 2000 (Financial Promotion) Order 2005, (FPO), commonly referred to as Financial Promotion Restriction. The mandates are also outlined in Section 327 and 328 of the POCA 2002.

information that helps customers decide on whether to proceed with the transaction.[112] Disclosures by the cryptoassets companies to customers are necessary, especially concerning risky products and services that present the potential for loss to the client. Furthermore, the mandates regarding disclosures ensure that cryptoasset businesses do not exploit the information asymmetry that arises from the complexity of the cryptoassets industry.

The FCA has also taken measures to enhance its oversight while preventing regulatory arbitrage[113]through the introduction of the Temporary Registration Regime.[114] Under the TRR, the FCA acknowledges the concerns associated with the complexity and volume of requirements facing the companies in the cryptoassets industry in the process of complying with the new AML/CTF regime, including the costs of compliance.[115] The TRR is essentially a mechanism for relief, with the delay designed to offer the companies sufficient time so that they can develop solutions for compliance before the obligations can take effect.[116]

Regulated organisations are obligated to provide suspicious activity reports.[117] The provisions are derived from section 330 of POCA, which bestows criminal liability on organisations that fail to make such reports when there are reasonable grounds for such actions.[118]

---

[112] FCA, n(83) indicates that cryptoassets companies have to provide the required disclosures to the right individuals at the right time, in the right place, without prejudice, and in clear terms.

[113] See Braddick, and others n(73) who define the situation as a balancing act, where the FCA seeks to promote innovation in the cryptoassets space, while also ensuring that it prevents any adverse outcomes associated with the industry.

[114] TRR hereafter. FCA n(81) indicates that the registration, whose deadline was extended from July 2021 to March 2022, was designed to allow certain businesses to continue trading as the FCA reviews their application for registration.

[115] See Impact Assessment, '*Transportation of the Fifth Anti-Money Laundering Directive'*, (Oct 2019), <https://www.legislation.gov.uk/ukia/2019/172/pdfs/ukia_20190172_en.pdf>, which indicates that these costs arise from training of staff on the new standards, hiring of specialists in compliance, and the opportunity cost arising from regulatory arbitrage.

[116] See FCA, n(81) that identifies the compliance requirements targeting service providers, including the requirement to update their risk assessment for customers and businesses based on the new sanctions regime, performing customer due diligence for new and existing customers, screening customers and transactions to determine any breaches, identifying any activities that are not in line with the profile of customers and participate in public-private partnerships for gathering and disseminating intelligence among others.

[117] SARs hereafter. See A Adeyemi, 'Slipping Through the Net: The Financial Conduct Authority's Approach in Lessening the Incidence of Money Laundering in the UK', (2018), 21, J of ML Control, 2, 1, who indicates that regulated institutions are obligated to disclose such suspicious activities to the NCA, based on their suspicious or knowledge, with Part 7 of POCA 2002 dealing with SARs on ML, while Part 3 of Terrorism Act of 2000 deals with suspicious activities on TF.

[118] See C Hogg, K Jones, and N Swift, 'Failure to Prevent Market Abuse: A Potential New Corporate Criminal Offense?' (2020) 41 Bus Law Rev, 4, 124. See also Section 330 of POCA identifies the reasonable grounds to include where the designated person is aware of suspicious, or has reasonable grounds for awareness or suspicion that another person is engaged in ML; the information that gave rise to such suspicion or knowledge arose from business-related

Despite the perceived ML/TF risk, the available evidence reveals that the UK is not a key market for the cryptoassets sector.[119] In recognition of these risks, the FCA has taken measures to spearhead the supervision of AML/CTF activities in the UK, with the primary legislative approaches aimed at increasing the protections for consumers, promoting innovation in the industry, and bringing the cryptoassets industry into its regulatory perimeter.[120] These measures focus on preventing failures in the systems and controls through the credible deterrence strategy.[121] The strategy involves the imposition of financial sanctions on any legal or natural person who fails to comply with the existing regulations. The strategy is built on a policy that does not require the initiation of criminal proceedings, thus eliminating a multiplicity of the bottlenecks and red tape associated with such proceedings.[122]

In summary, the legislative approaches adopted by the FCA for AML/CTF purposes in the era of cryptoassets bear several similarities with traditional methodologies, which is evident from the FCA Banking Conduct of Business Sourcebook (BCOBS). These include the provision of context, an explication of the relevant rules, and an indication of the industry guidance to be complied with. There is evidence that the FCA relies on legislative approaches that focus on the psychological impact of adverse experiences with cryptoassets as a way of alleviating the ML/TF risks. To reassure the users of cryptoassets, as well as ensure the safety of communities, the legislative. The FCA also relies on legislative approaches under the lever of structures, whereby laws prohibit unlawful associations.

The legislative approaches utilised by the FCA focus on signaling the goals of the institution and playing a greater role in remaining initiative-taking at the boundaries of the regulatory perimeter. The FCA has adopted a legislative approach for sentence enhancement,

---

interactions, and, the designated persons can identify the other person, or has knowledge of the whereabouts of the property that is laundered, or has information that can easily be used to trace the perpetrator, or the laundered property.

[119] See Impact Assessment, n(115) which indicates that based on estimates by the FCA, the entire market is served by only 15 out of the 231 cryptoassets exchanges that operate in the world, and that 10% of consumers in the UK hold cryptoassets. Similarly, only 4 of the exchanges provide regular updates on daily trading, which are estimated at US$30M. An estimated provided by the UK Cryptoasset Taskforce reveals that there have been 56 ICOs in the UK, which represent less than 5% of the global volume.

[120] C Hogg, K Jones, and N Swift, 'Failure to Prevent Market Abuse: A Potential New Corporate Criminal Offense?' (2020) 41 Bus Law Rev, 4, 121.

[121] The authority and power for the credible deterrence strategy are built into the Financial Services Act 2021.

[122]Harrison and Ryder, n(27) 24, indicates that the FCA can initiate such proceedings with ease, by granting prohibitions upon individuals who breach the pre-placement rues from engaging in the criminal activities, thereby leading to increased effectiveness in its deterrence activities.

which targets tightening the regulation around the handling of cryptoassets, thereby reducing the ML/TF risks. The enhancement of sentences is carried out through policy statements, which provide the applicable regulatory, supervisory and monitoring regime. A case in point is PS19/22,[123] which offered guidelines on the regulatory regime for the various cryptoassets, followed by PS20/10,[124] which prohibited the trade of investment products that refer to cryptocurrencies. The multiplicity of legislative approaches identified under the AML/CTF responsibilities of the FSA arises from the fact that it is responsible for protecting consumers, mitigating ML/TF risks to the financial sector, as well as upholding the integrity of the financial market in the UK. The discussion provided in this section has highlighted how the model of cryptocurrencies regulation in the UK has evolved to respond to the numerous opportunities for TF that cryptoassets possess, and thus, it has directly addressed the sub-question nine this thesis has aimed to address.

6.2.3 Office of Professional Body Anti-Money Laundering Supervision (OPBAS)

The OPBAS framework is highly relevant to the regulation of cryptoassets, as professional bodies involved in accounting and financial services are integral to preventing the laundering of illicit funds through crypto transactions. Given the anonymity and complexity associated with cryptoassets, OPBAS's risk-based supervision ensures that these professional institutions remain vigilant in monitoring and reporting suspicious crypto-related activities.[125] By promoting information-sharing, governance, and intelligence within regulated bodies, OPBAS helps prevent professional enablers from unwittingly or negligently supporting ML/TF activities within the crypto sector, thereby strengthening the overall AML/CTF regime.[126]

The OPBAS establish a framework through which supervisors of professional bodies in the regulated sectors can participate in the AML/CTF activities.[127] Based on the 2020 NRA 2020,

[123] FCA, n(83)
[124] FCA, n(81)
[125] Duncan Smith, 'Supervision & Regulation; Investigation & Prosecution' in *Money Laundering, Terrorist Financing and Virtual Assets: Cases and Materials* (Springer Nature Switzerland 2024) 63
[126] Rukhsana Parveen, 'Impact of Anti-Money Laundering Legislation in the United Kingdom and European Union' (2020) 5 International Journal of Economics and Management Systems
[127] Hereafter OPBAS. See IMF, 'Review of the Fund's Strategy on Anti-Money Laundering and Combating the Financing of Terrorism', (IMF, 2019), 24, which indicates that these self-regulatory institutions oversee the activities of professional institutions in various sectors including finance, accountancy, legal and other professions covered under MLRs.
See also Regulation MLR 2017, which remained unchanged under MLR 2019, states that professional body supervisory institutions should plan for ways to exercise the supervisory functions in an independent manner

professional institutions in the UK are key targets of persons seeking to introduce or integrate illicit funds into the domestic and global financial system.[128] The suspected gaps in the prevention and management of ML/TF risks, which were attributed to unwitting, negligent or complicit involvement of the professional institutions, were confirmed in the first annual assessment report.[129] As enablers,[130] professional institutions play a role in the predicate offences for ML/TF, including the facilitation of fraud, exploitation of legal and accounting[131] professional services, and the development of organisational cultures and corporate structures that facilitate ML.[132] As a result, OPBAS acts as a supervisor of supervisors, and its involvement in the AML/CTF regime is a key addition to the professional supervisory bodies, as well as the institutions that are registered as members in those PBS.

The scale and scope of risks associated with these professional bodies have necessitated the enhancement of the sector-specific AML/CTF measures. First, OPBAS has enhanced the role of governance in AML/CTF within professional bodies.[133] Second, the OPBAS has led to the

(Regulation 49(1)(a)), and they should provide sufficient resources for those supervisory functions (Regulation 49(2)(a)).

[128] HM Treasury, n(31) which reports that based on the National Risk Assessment (NRA) report in 2020, the UK economy loses £37B annually due to the activities serious and organised criminal groups. Based on the same report, money launderers and financier of terrorism utilise the vulnerabilities in the legal and accounting professions for illicit activities.

[129] See J Barberis, D W Arner, and R P Buckley, *The RegTech Book: The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries in Regulation* (John Wiley & Sons, 2019), 173, who attribute the weaknesses to four circumstances. First, the professional bodies were primarily focused on representation of the interests of their members, rather than enforcing robust supervisory standards. Second, only a small proportion of the professional institutions were keen on enforcing the current ML/TF standards. Third, there were no frameworks and arrangements for sharing of intelligence on ML/TF risks with the necessary authorities such as UKFIUs and LEAs. Finally, 25% of the professional bodies did not undertake any form of supervision for ML/TF risks.

[130] HM Treasury, n(31) indicates that in the UK, businesses are perceived as the first line of defence in the AML/CTF strategies since they are integral in thwarting the exploitation of the financial system for criminal activities. These businesses are also critical in the detection of suspicious activities. See also H Koster, 'Towards better implementation of the European Union's anti-money laundering and countering the financing of terrorism framework' (2020) 23 J of ML Control, 2, 382, which cites the findings from the Panama Papers as an eye opener for regulators in the UK, by estimating that in spite of the massive ML activities discovered therein, none of the actions triggered any response from the existing AML/CTF regime.

[131] Ibid, 83, which assesses the risk of ML from accountancy and legal services providers as remaining 'high' between 2017 and 2020, while the risk score for facilitation of TF by the companies in the two sector as 'low' over the same period.

[132] OPBAS, 'Office for Professional Body Anti-Money Laundering Supervision (OPBAS): Sourcebook for Professional body anti-money laundering supervision' (OPBAS2018), <https://www.fca.org.uk/publication/opbas/opbas-sourcebook.pdf> accessed 19 March 2023

[133] HM Treasury, n(10) which indicates that The governance structures put in place outline the responsibilities for AML/CTF in their role as a gatekeeper, which also entails identification of mechanisms for best practices under each category of responsibility. See also OPBAS, n(132) which provides examples of best practices, which are directly contrasted with examples of poor practice.

implementation and utilisation of the risk-based approach in the AML/CTF regime in the supervision of professional institutions.[134] Through this approach, the OPBAS focused on two outcomes: ensuring that more focus is directed towards the riskiest institutions among the supervised population and supporting the awareness of the supervised population on how to deal with the most prominent ML/TF risks and vulnerabilities in the country.[135] Third, OPBAS engage in the supervision of the institutions that are member bodies of the professional bodies.[136] PBS is required to supervise the activities of the institutions that they certify since the membership of an institution with a professional body is associated with certain levels of confidence by potential clients and customers.[137] The OPBAS performs supervision for AML/CTF purposes through a multiplicity of ways, including questionnaires and desk-based reviews,[138] meeting senior managers,[139] requests for period and ad hoc information returns,[140] review of case files from members, and outreach and thematic works.[141]

[134] Regulation 46(2)(a) of the MLR 2017 require all professional body supervisors to adopt the risk-based approach for ML/TF risks, as well as other risks as outlined under Regulation 17.

[135] See C A Russo, R M Lastra, and W Blair, *Research Handbook on Law and Ethics in Banking and Finance*, (Northampton, Edward Elgar Publishing, 2019) 332, this support includes the allocation of supervisory resources, assisting in the development and implementation of policies as well as other forms of assistance to enable the supervised institutions to achieve the sector-specific AML/CTF goals.

[136] Regulation 46 of MLR 2017 outlines the guidelines for professional bodies to supervise the activities of the bodies under their oversight, to ensure that they comply with the requirements of regulations. See also HM Treasury, HM treasury n(10) which states the PBS conducted DBRs and site visits targeting 10% of the entities under its mandate. Among the accounting firms visited, 19% failed to meet the benchmarks for compliance, with similar results reported for 9% of those entities subjected to a DBS. Among legal firms, 10% of those assessed through DBRs were non-compliance, while the site visits revealed a 24% rate of non-compliance for the entire population of legal firms under the PBS. Based on the supervision report, the DBRs and site visits culminated in the conclusion that 6.5% of the professional bodies presented high risks for ML/TF, while 23% were graded at a medium risk.

[137] Regulation 46(2) (c) of MLRs 2019 mandates supervision through both on-site and offsite mechanisms. Additional measures include mandates for testing the risk-based procedures to determine their robustness and suitability of the intended purpose.

[138] See J Barberis, D W Arner, and R P Buckley, *The RegTech Book: The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries in Regulation* (John Wiley & Sons, 2019), 175, The PBS may undertake a review of information and data from the member company, without visiting the site, while questionnaires involve an inquisition about a specific aspect of the business, with objective targets about the business.

[139]Ibid, 175, PBSs have the responsibility to meet with senior staff members for supervisory reviews, a process that can also be performed through telephone or other forms of media. Such meetings entail information that is available among top management.

[140] N Lord, and others, *European White-Collar Crime: Exploring the Nature of European Realities* (Policy Press, 2021) 97, Periodic information returns are a requirement for member bodies, who have to provide returns about performance. These returns are legally binding documents about operations. Ad Hoc Information requests are made depending on the circumstances and may be required at any time during the year, regarding any aspect of the PBS or member company.

[141] *Ibid* 98, PBSs engage in outreach by summoning representatives from the member institutions to discuss any issues as a group, and address concerns and challenges that are particular to the sector.

Fourth, through the information and intelligence sharing framework, the OPBAS offers guidance and communication as part of the UK's AML/CTF practices.[142] The guidance provided by what is referred to as affinity groups relates to general support to all or individual member companies and industry training to contextualise and supplement the existing knowledge.[143] These arrangements, as well as the affinity groups, act as a single point of contact[144] , which enables the institutions under their supervision to facilitate the AML/CTF goals through prompt response to enquiries, sufficient security on key data and information, commitment to utilising intelligence in risk management, provision and utilisation of available resources for AML/CTF activities.[145]

6.3 Tertiary Authorities

Tertiary authorities, including professional bodies and trade associations, are involved in the AML/CTF regime on account of their direct/indirect exposure to ML/TF risks. The access to information about customers, market participants and transactions makes tertiary authorities an integral component of any AML/CTF regime in the era of cryptoassets. As the discussion illustrates below, the Joint Money Laundering Intelligence Task Force (JMLIT) supports the AML/CTF regime by fostering public-private partnerships that address crypto-related threats, offering intelligence that helps law enforcement distinguish between legitimate and illicit crypto activities.[146] The Joint Money Laundering Steering Group (JMLSG) complements this by providing financial institutions with guidance on crypto-specific AML/CTF practices, promoting best practices for detecting and mitigating crypto-based ML/TF risks.[147] Together, these authorities adapt traditional AML/CTF approaches to the challenges of cryptoassets, ensuring both proactive oversight and regulatory agility in response to evolving threats within digital finance.

---

[142] Under MLRs 2019 50(1), the professional bodies are mandated to cooperate with supervisory institutions from other sectors, coordinate the activities of their member institutions for AML/CTF objectives, and cooperate with overseas institutions for effective supervision and oversight.

[143] For instance, the Legal Sector Affinity Group (LSAG) and Accountancy Sector Affinity Group (AASG). See Lord and Others, n(140), 100, who state that communications entail passing on information through trade presses, consultations, and mailings for the purpose of ensuring parity in information about and intelligence within the sector. Currently, information- and intelligence-sharing arrangements include the Shared Intelligence Service (SIS) and the Financial Crime Information Network (FIN-NET).

[144] SPOC hereafter, which is a requirement under Regulation 49(2)(b) MLRs 2017.

[145] OPBAS, n(132)

[146] Nicholas Ryder, 'Cryptoassets, Social Media Platforms and Defence Against Terrorism Financing Suspicious Activity Reports: A Step into the Regulatory Unknown' (2020) Journal of Business Law 8, 668

[147] Joint Money Laundering Steering Group, 'JMLSG Publishes New Guidance' (JMLSG 2020) <https://www.jmlsg.org.uk/latest-news/jmlsg-publishes-new-guidance-3/>accessed 11 November 2024.

6.3.1 The Joint Money Laundering Intelligence Task Force (JMLIT)

The JMLIT[148] is a partnership between financial sector institutions and law enforcement agencies.[149] As part of the private-public partnerships and the unification of supervisory regimes, it creates a framework based on trust and mutual benefits, thereby facilitating the exchange and analysis of information about ML.[150] In addition, the task force targets economic threats from other activities to prevent predicate offences through information sharing, specifically those linked to SARs. This represents the intelligence-oriented strategies and tactics that were innovated in the UK to identify gaps in the risk-based AML/CTF regime. These intelligence-oriented strategies enable regulatory, supervisory and monitoring institutions to remain informed about the changes in the risk and threat profiles in the UK.

The intelligence-oriented approach[151] establishes the basis for planning and using the available data to generate information and ultimately create knowledge that can be applied for continual improvement in the AML/CTF tactics, operations and strategies.[152] The approach enables the institutions involved in the AML/CTF activities to understand the objectives of criminals and terrorist groups and why they need the services of the financial sector.[153] After all, data and information are no longer enough for decision-making and strategy implementation for AML/CTF in the era of cryptoassets. It is necessary to continuously assess, analyse, and enhance intelligence

---

[148] JMLIT hereafter. N J Maxwell, 'Expanding the Capability of Financial Information-Sharing Partnerships', (2019)<https://www.futureis.com/uploads/3/7/9/4/3794525/pr%C3%A9cis_of_ffis_paperexpanding_the_role_of_fisps_-_march_2019.pdf> accessed 11 November 2024 indicates that on account of the success of the JMLIT model, six other entities built around the same model were created in the UK, across Europe and other locations across the world, including Fintel Alliance in Australia, the Anti-Money Laundering and Counter-Terrorist Financing Industry Partnership (ACIP) from Singapore, the Fraud and Money Laundering Intelligence Taskforce (FMLIT) from Hong Kong, the Terrorist Financing Taskforce (TF Taskforce) from Netherlands, the Financial Crimes Enforcement Network (FinCEN Exchange) from the US, and the Europol Financial Intelligence Public Private Partnership (EFIPPP).

[149] The JMLIT is comprised of five LEAs and at least 40 FIs, in addition to working hand in hand with the NCA, Metropolitan Police Services, the HMRC, the City of London Police Department and the SFO.

[150] NCA, 'UK Financial Intelligence Unit-Suspicious Activity Reports Annual Report 2020, (2020). https://www.nationalcrimeagency.gov.uk/who-we-are/publications/480-sars-annual-report-2020/file accessed 11 November 2024 indicates that the model serves a multiplicity of roles, including reducing the possibility of defensive reporting, whereby firms provide an unnecessarily high number of SARs that are of low quality, thereby impacting the effectiveness of the reporting regime in the UK AML/CTF. For instance, the NCA received over 573,085 SARs in 2019-20, up from 478,437 in the previous period.

[151] The intelligence-oriented approach as a doctrine where the full spectrum of the operational environment is anticipated, visualized and understood with the objective of influencing the process and outcomes

[152] R J Lowe, 'Anti-money laundering – the need for intelligence', (2017) 24 J of Fin Crime, 3, 479, who indicates that the JMLIT facilitates the 'whole system' approach to AML/CTF regime.

[153] The institutions under the JMLIT use the information to determine the motivations and factors underlying the decision-making processes by persons engaging in ML/TF.

from multiple sources, including cross-border data from institutions with different SAR regimes.[154] With the increased use of financial services in the UK, stakeholders involved in AML/CTF activities are exposed to increasing quantities of data on transactions and how the financial system is utilised.

The UK financial and non-financial sectors rely on the input from the JMLIT to understand the tendencies of genuine customers and service providers from those who are interested in illegal activities.[155] The involvement of the JMLIT is integral, especially where the ML/TF activities are the product of insider activities or collusion. The utility of the JMLIT approach has led to the emergence of other sector-specific intelligence-sharing entities, including the Intelligence Sharing Expert Working Groups[156] and Financial Crime Information Network.[157] These changes call for the use of different types of intelligence, including predictive and actionable intelligence, to reduce the time and resources it takes for courses of action to be taken and interventions to be implemented.[158]

The application of an intelligence-oriented approach within a collaborative framework also reduces the chances of failing to detect ML/TF activity, especially in an environment where the perpetrators use novel and dynamic strategies to exploit the loopholes. It also increases the efficiency and effectiveness in the utilisation of the existing resources and capabilities while enabling the regulatory institutions to adjust their AML/CTF activities in response to changes in

[154] S Riondet, 'The Value of Public-Private Partnerships for Financial Intelligence' (2018) 2, J of Fin Compliance, 149, who uses the example of the public private partnership under Europol Financial Intelligence Public-Private Partnership (EFIPPP), launched in 2017. The partnership brings together experts from 15 major banking institutions from eight countries in Europe and seven from outside the EU. The cooperation involves LEAs, supervisors who share information and improve cooperation across national borders. The cooperation has evolved to exchange of strategic information on ongoing and past investigations, as well as sanitised case studies to ensure parity in AML/CTF abilities among the various countries.

[155] *Ibid*

[156] ISEWGs hereafter. HM Treasury n(10) who indicates that this body is forced by the NECC and OPBAS, for tactical and strategic intelligence to be shared between AML supervisors, PBSs and law enforcement agencies for the creation of reports, alerts and case studies that facilitate collaborative working environment to build trust among the institutions and ensure consistency in the AML/CTF approaches.

[157] Ibid, FIN-NET hereafter, which is an intelligence sharing network that works under the FCA and meets once every two months to facilitate knowledge sharing on the operations of government entities, supervisory institutions and law enforcement agencies.

[158] A Murphy, 'The Investigator-Centred Approach to Financial Crime: Doing What Matters, (*Mckinsey* 2020),<https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-investigator-centered-approach-to-financial-crime-doing-what-matters > accessed 14 March 2022 indicates that the JMLIT facilitate the matching of the who, where and what in relation to current and future ML/TF activities in the UK.

risk exposures. The combined efforts of the institution lead to proactive and reactive policing while utilising forward-looking and backwards-looking domains of law enforcement.

There is qualitative and quantitative evidence of the effectiveness of the JMLIT model due to the integration of mechanisms for developing and enhancing the systems and controls for the mitigation of threats from ML/TF crimes.[159] Under the JMLIT model, the UK has launched a multiplicity of programs[160] designed to target specific ML/TF methodologies for exploiting the weaknesses in the UK financial system. Finally, the utility of the JMLIT is evident from its recognition by the FATF, with additional jurisdictions adopting the model due to its status as a 'best practices model'[161] for AML/CTF. JMLIT is an active agent in the UK's Financial War on Terrorism by providing actionable intelligence and supporting the AML/CTF work of the other agencies. This material addresses the third research question - the evaluation of the implementation and the efficiency of the Financial War on Terrorism. The success of JMLIT is evidenced by its recognised effectiveness in mitigating ML/TF threats and by the recognition of the FATF. The adoption of similar models in other jurisdictions across the European Union Juunderscores JMLIT status as a best-practice model for global AML/CTF efforts.

6.3.2 The Joint Money Laundering Steering Group (JMLSG)

The JMLSG guides financial institutions, focusing on risk exposures through the provision of guidance to financial institutions and designated individuals in the financial services sector.[162] The steering group has four key functions, all of which are oriented toward providing customised guidance to the senior management personnel in financial institutions to enable them to acquire competence, capabilities and skills in performing case-by-case analyses of potential risk exposures. First, it assists the organisations in designing countermeasures and internal controls

[159] N J Maxwell, 'Expanding the Capability of Financial Information-Sharing Partnerships', (2019),<https://www.futureis.com/uploads/3/7/9/4/3794525/pr%C3%A9cis_of_ffis_paperexpanding_the_role_of_fisps_-_march_2019.pdf> accessed 14 March 2022 indicates the JMLIT played a key role in 443 judicial cases, leading to restraint of £12M in assets classified as suspicious. The cases led the arrest of 105 suspects, with 3369 accounts. Similar levels of success are reported in other JMLIT-type organisations from across the world.

[160] Ibid, who identifies an example such as the Future of Financial Information Sharing (FFIS), which has established a five-year plan from 2015-2020, targeting to trace how private-public partnerships evolve within the UK.

[161] Through the model, the UK has been able to focus on crimes and the techniques used by criminals, as well as the trajectory of evolution of those techniques to predict potential ways through which a person navigates or defat the existing AML/CTF defences and mechanisms.

[162] See Braddick, and others n(73), p.14

based on the prevailing AML/CTF regimes.[163] Second, the steering group has created an institutional framework to promote best practices among firms in the UK's financial sector.[164] The best practices include measures that are deemed necessary or integral but have not yet fully been integrated into the regulatory frameworks.[165] Third, the steering group assigns the responsibility for the design and implementation of procedures, policies and controls for ML/TF risk to the senior management. Because of their position of power within the institution, the JMLSG places this responsibility on the senior management and assigns criminal liability for any gaps in regulatory compliance that lead to incidences of ML/TF. Fourth, the guidance offered enables financial entities to voluntarily adopt and adapt a risk-based approach that is robust enough for the detection, investigation and prevention of ML/TF. Under the JMLSG, private-sector firms appreciate the objectives and concerns underlying the positions held by the public sector entities, while public-sector organisations benefit from the technological expertise that thrives within the private sector domain. Finally, the JMLSG has established risk-based guidance that enables organisations to determine their supervisory and monitoring perimeter based on fulfilment channels,[166] geographic characteristics[167] and customer characteristics.

The frameworks for guidance under these tertiary authorities have led to the amplification of the prominence of soft law in the UK AML/CTF regime in the era of cryptoassets. The directions on law, as provided by commissions/committees of experts and other representative bodies, offer

---

[163] Esoimeme, n(79), who indicates that the Steering Groups seeks to ensure regulatory compliance by assisting these institutions.

[164] See NCA, 'UK Financial Intelligence Unit-Suspicious Activity Reports Annual Report 2020, (NCA, 2020). <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/480-sars-annual-report-2020/file> accessed 14 March 2023 indicates that AML/CTF good practices are the professional procedures and measures that are widely accepted and prescribed as being correct and the most effective.

[165] T Douglas, 'Notes on new Joint Money Laundering Steering Group (JMLSG) guidance', (2006) 7 J of Investment Compliance, 1, 64, who indicates that the steering group lays is comprised of representatives from key trade associations with the objective of designing customised compliance strategies for the UK's AML/CTF regime in response to dynamic regulations and legislation under the FCA. Risk-based approaches focusing on internal decisions on monitoring customers, verification of identifies, use of pro-forma confirmation of transactions, monitoring of staff to ensure compliance, and measures to enhance their ability to reduce ML/TF risks through increased training and vigilance.

[166] See HMRC, '*Tacking Tac Evasion: Government Guidance for the Corporate Offenses of Failure to Prevent the Criminal Facilitation of Tax Evasion'*, (HMRC, 2017) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/672231/Tackling-tax-evasion-corporate-offences.pdf> accessed 15 March 2023 which identifies the risks associated with the product, services, transaction or delivery channel, including private banking, anonymised transactions, lack of face-to-face contact, and payment to unknown or associated 3rd parties.

[167] *Ibid*, 18, geographic characteristics, which are dependent on the characteristics of the country, include countries with weak AML/CTF regimes, countries facing international sanctions or embargoes, or countries that provide support to terrorists.

systematic and authoritative restatements, clarifications, revisions, and, where necessary, transpositions of the existing laws and regulations. The roles and responsibilities of the various institutions under the three tiers are both complementary and supplementary. Understanding the critical role of the JMLSG in the AML/CTF framework in the UK is critical to appraise how the UK government responded to the threat that the use of cryptoassets for terrorism financing poses to both individuals and financial markets.

6.4 The FATF Mutual Evaluation Report (MER)

One of the key subsidiary questions is to identify the role the FATF has played in supporting the development of the AML/CTF regime in both the UK and Bahrain and how each state has been compliant with the FATF Recommendation, some of which were presented in the FATF Mutual Evaluation Report. Therefore, the following section determines whether the UK government has considered the MER recommendation and whether the UK is becoming an international leader in fighting ML and TF in the digital realm.

The UK played a key role in the conceptualisation and creation of the FATF. Through its continued support, the FATF has enhanced its mandate through methodologies and recommendations under its AML/CTF activities. These recommendations revolve around the acquisition, retention and transmission of information on originators and beneficiaries.

6.4.1 Background

The UK has continually updated its AML/CTF policies in line with global standards.[168] This is evident from the changes in the specific standards under each recommendation and the level of compliance assessed under the FATF Recommendations between the 2007 and 2018 MER reports. First, in addition to the 40 Recommendations, which are classified into four categories, the 2007 MER also focused on nine special recommendations.[169] The 2018 MER deviates from

[168] See D Goldbarsht, and L Koker, *Financial Technology and the Law: Combatting Financing Crime*, (Springer Nature, 2022), 142 who indicated that the FATF standards had directly contributed to the promulgation of UK legislation in order to reflect the substance of what is recommended under the MERs and the accompanying notes. The 2021 FATF report led to the revision of European AML/CTF standards under Fourth Anti-Money Laundering Directive (4MLD), official referred to as the Directive (EU) 2015/ 849 of the European Parliament and of the Council. The changes adapted included strengthening of the AML/CTF obligations for traditional FIs through increased emphasis on the application of the risk-based approach to monitoring of transactions and customers as a way of determining the most suitable approach to due diligence.

[169] See FATF GAFI, 'Financial Action Task Force: The United Kingdom of Great Britain and North Ireland', (FATF, 2007) https://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20UK%20FULL.pdf> accessed 16 March 2023 whereby the categories for recommendations include Legal Systems, Preventive Measures, Institutional and

this approach by proposing and assessing each Recommendation separately while also assimilating the special recommendations into the 40 Recommendations.[170] These changes have simplified the process through which the FATF reviews the performance of jurisdictions while also introducing objectivity to the emergent categories of ML/TF risks in the era of cryptoassets. Unlike other supervisory and regulatory entities that inform the UK's AML/CTF regime, the FATF uses the term 'virtual assets' rather than cryptoassets.[171]

6.4.2 Technical Compliance Report-the UK

The 2018 MER report recognised the UK as having the strongest AML/CTF regime among countries the assessed countries.[172] The ratings reflect how well the supervisory institutions in the UK understand, coordinate and perform their duties under the AML/CTF regime.[173] The UK is assessed as being compliant with several CTF-related recommendations, including ML offences, TF offences, reporting of suspicious transactions, transparency and beneficial ownership of legal arrangements and regulation and supervision of financial institutions. The UK is gauged as largely compliant in recommendations such as 'targeted financial sanctions related to terrorism and TF, CDD, new technologies, higher-risk country, transparency and beneficial ownership of legal persons, and other forms of international cooperation. It is also evident that the UK has enhanced its performance under the three Recommendations in which it was found to be 'non-compliant' in 2007, including the management of risks associated with politically exposed persons, correspondent banking and foreign branches and subsidiaries. The performance under these dimensions is of concern since it relates directly to the supervisory and regulatory mandates that are discussed under the primary, secondary and tertiary institutions that oversee 90% of the

Other Measures, and International cooperation. The FATF.GAFI also who identifies the special recommendations as including implementation of UN Instruments (C), Criminalise TF (C), Freeze and confiscate terrorist assets (C), Suspicious Transaction Report (C), International Co-Operation (C), AML Requirements for Money/Value transfer services (LC), Wire transfer rules (PC), Non-profit Organisation (LC) and Cross-border Declaration and Disclosure (LC).

[170] FATF, 'Anti-money laundering and counter-terrorist financing measures–United Kingdom, Fourth Round Mutual Evaluation Report,, (FATF, 2018) http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-united-kingdom-2018.html accessed 16 March 2023

[171] Companies in the cryptoassets industry are referred to as Virtual Assets Services Providers (VASPs)

[172] HM Government and UK Finance, n(52) which indicates that the assessment is based on the ability to target its financial sanction regime as and when necessary, its appreciation of risks, including ML risks and for TF purposes.

[173] It also reflects how well those UK institutions works with foreign counterparts, aggressively investigate and prosecute ML/TF offenses, apply the right AML/CTF measures for all risks and threats, prevent the exploitation of the FIs by criminals and terror groups, and support the implementation of financial sanctions within and outside its jurisdiction for preventive and punitive purposes.

regulated sectors.[174] Each of the supervisory entities employs a unique approach in its risk-based supervision, which explains the existence of weaknesses in AML/CTF outcomes. However, the assessment does not imply that the existing regulatory or enforcement systems are strong enough for the emergent and extant risks in the country.

The report reveals systemic failures in the AML/CTF framework to prevent the engagement of multinational firms within the UK jurisdiction in such activities. The willingness and ability of these multinationals to pay the assigned fines imply that either the values of fines are not punitive enough or the ML/TF activities are too lucrative for the institutions to eliminate.[175] However, questions arise on the objectivity of the overall ratings vis-à-vis the performance under individual recommendations. The primary concern revolves around the assignment of the 'best practices' ratings for the UK under the 2018 MERs, while the UKFIUs are perceived as only being 'partially compliant in their AML/CTF.[176] Based on the explanation by the FATF, partial compliance is attributed to a lack of operational independence, inability to perform key functions due to lack of resources and the lack of capacity to strategically utilise its SAR regime. One of the key questions that the thesis aimed to address was to what extent the UK is compliant or not with the FATF recommendations, and the material presented above has demonstrated that the UK has one of the most robust regimes for AML/CTF and the attempts to come up with a valid framework for AML/CTF has been positively evaluated by the FATF.

6.4.3 Expansion of the Institutional Framework

The collaborative strategies adopted by the FCA and HM Treasury have proven effective in the design of AML/CTF policies. However, collaborations are limited on account of the scale, scope and tactics of cooperation, with most of the input from stakeholders involving the provision of information. In response, novel institutions have been introduced as an extension of the JMLIT model.[177] The National Economic Crime Centre[178], which is established under the NCA, functions

[174] HM Treasury, n(31)
[175] See Ibid, 32, the data reveals that although there was a drop in the number of fines issues from 376 to 320, there total value of fines imposed increased by 32%. There was an increase in the categories of offenses fined by the supervisors by 36%, revealing an increase in the regulatory appetite. Among the multinational faced with huge fines is Standard Chartered Bank, which was fined £102M for failing in AML/CTF in correspondent banking with UAE branches.
[176] FATF, n(170)
[177] See Section 1.4 under tertiary authorities.
[178] NECC hereafter

to ensure sustainability in the response to coordinate the UK's response to crimes of an economic nature. The collaborative centre is a multi-agency venture that coordinates the activities of different agencies that focus on the criminal domain of the AML/CTF regime in the UK.[179] The NECC brings governmental departments, private sector entities, law enforcement agencies, regulatory institutions and judicial institutions together with a mutual goal of tackling the risks from serious organised economic crimes, maintaining the reputation and prosperity of the UK's financial system, and protecting the public from exposure to complex criminal and ML/TF risks.

6.4.4 Digitisation of the Supervisory Regime

The prominence of the risk-based approach under FATF and other traditional AML/CTF policies in the UK has led to inefficiencies due to the high volume of cases referred by the MLROs.[180] The criminalisation of mistakes and errors in reporting suspicious activities has also led to the tendency of designated individuals to employ a conservative approach to risk analysis and management.[181] Section IV of the FATF offers several options for technological mediation in facilitating compliance with the AML/CTF regime.[182] The combined effect of this SAR regime is an increase in the volume of SARs that are escalated to the UKFIUs by the financial institutions. Digitisation facilitates the integration of analytical and visualisation methodologies in assessing the risks and threats, thereby leading to the development of cause-and-effect relationships that are easy to understand. Digitisation represents a new frontier in the application of advanced technologies in the financial and regulatory sectors to reinforce the AML/CTF system.[183] The

[179] HM Government and UK Finance, n(52) which indicates that the NECC is a multi-agency centre established in 2018 for collaborative purposes in confronting the complex challenge associated with serious and organised economic crimes in the UK. The centre draws from the FCA, the HMRC, the NCA, the Crown Prosecution Services (CPS), the City of London Police, and LEAs among others.

[180] NCA n(164)

[181] R J Lowe, n(152) who reported that in 2014, BNP Paribas was charged a $8.9M fine for failure to check businesses linked with Sudan. In response, other institutions like HSBC tripled their budgetary allocations for compliance costs by over US$200M in one year, with Macquarie Bank tripled its allocations over a period of three years.

[182] Some of the proposed technologies are still lagging in maturity and utility for the purpose they are intended, and their use will only be authorized once where are clear indications that they are suitable and effective. See also Government Office for Science, 'FinTech Futures: The UK as a World Leader in Financial Technologies', (Government Office for Science 2015), <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/413095/gs-15-3-fintech-futures.pdf> accessed 16 March 2023 who indicates that the UK has excelled in both Regulatory Technology and Financial Technology, which necessitates the introduction of novel approaches to accommodate the emergent risks.

[183] FATF, 'Annual Report 2020-2021', (FATF 2021). <https://www.fatf-gafi.org/media/fatf/documents/brochuresannualreports/Annual-Report-2020-2021.pdf> accessed 16 March 2023

decision to digitise through SupTech arises from the diversity of proven use cases,[184] coupled with applicability at the supervisory level.[185]

Therefore, the FATF recommendations play a key role in the transformation of the UK's AML/CTF regime. In addition to the multiplicity of changes in the Recommendations, which are considered key determinants of the regulatory, supervisory and monitoring activities, the FATF utilises unique legislative approaches that seek to elevate the global standards in the identification and mitigation of ML/TF risks. Additional goals notwithstanding, the multiplicity of legislative approaches is of significant value to the UK, which seeks to retain its position as the leading financial hub across the globe.

6.5 UN/ EU Fifth Money Laundering Directive

The legislative approaches under the anti-money laundering directives[186] start with the recognition that the ML/TF risks occur mostly at the various points of exchange. The implementation of the 5MLD[187] was motivated by several anonymity-oriented changes in the manner and extent to which criminal and terrorist groups exploited the existing financial systems for illicit activities.[188] First, the 5MLD was introduced to guide how to tackle the serious threats posed by virtual currencies, including the ML/TF risks and the potential exploitation of the financial system for illicit activities.[189] The directive serves to introduce definitions of virtual currencies within union law, which can then be transposed into national laws by countries across

[184] I A Boitan, and K Bartkowiak, *Fostering Innovation and Competitiveness with FinTech, RegTech and SupTech*, (Pennsylvania, IGI Global, 2020), 117 identifies four key use cases under the AML/CTF regime, including automation of the data, information and intelligence collection processes through data-pull and data-push mechanisms; advances in the validation, analysis and visualisation of data to help in decision making; integration of databases and platforms and improved data management and storage.

[185] See V Lemma, *FinTech Regulation: Exploring New Challenges of the Capital Markets Union* (Springer Nature, 2020), 454 who indicates that SupTech leads to supervisory level outcomes including improvements in the scope, accuracy and consistency of collected information; enhanced risk-based supervision; efficiency in the use of resources, and improved information and intelligence flow among the supervisory entities.

[186] Hereafter AMLDs.

[187]Also referred to as Directive (EU) 2018/843, with the propositions contained therein based on the EU's Supranational Risk Assessment and UK's National Risk Assessment of 2017.

[188] Koster, n(130) 379, who indicated that criminal and terrorist groups have proven capable of exploiting the existing systems for illicit purposes as evidenced under the revelations under the Panama Papers in 2016.

[189] L Haffke, M Fromberger, and P Zimmermann. 'Cryptocurrencies and anti-money laundering: the shortcomings of the fifth AML Directive (EU) and how to address them'. (2019), 21, *J of Banking Regulation,* 3 who indicates that the new directive was introduced following the realisation that new technology services were not fully regulated under the 4th AMLD, and over time, these were used as an alternative for ML/TF activities. Furthermore, the provisions under 4th AMLD lacked transparency in the financial transactions, with several emergent corporate and legal entities being exploited for ML/TF activities.

the EU. The Directive also covered new risks posed by the anonymity achieved through creative operations using traditional financial products and services, including those operations associated with trading in art, professional services for obscuring tax liabilities and the use of safe deposit boxes.[190]

Despite the departure from the EU, the UK is mandated to adopt and adapt the provisions under the 5MLD[191] into its domestic law. The transposition into the MLRs is based on proposals by HM Treasury to gold-plate the emergent guidelines and extend the AML/CTF mandates to the operations of four categories of entities in the UK cryptoassets market, including companies providing crypto-exchange services,[192] companies offering platforms for peer to peer cryptoassets exchanges,[193] Cryptoassets ATMs,[194] and non-custodian wallet providers.[195] The provisions, which were implemented in January 2020, are effected under MLRs 2019.

Despite the enhanced utility of mitigating emergent and extant ML/TF risks, the directive has drawbacks that necessitate several changes during transposition by Union member countries.[196] The weaknesses include a lack of specificity in the wording under some of the provisions[197] and limitations in the scope of the provisions.

The transposition of the 5MLD into MLRs is the first time that the UK has introduced formal regulation for the cryptoassets industry. The lack of sufficient data to inform the legislative approaches explains why most supervisory and regulatory institutions have relied on multi-sectoral

[190] Koster, n(130) 382, who indicated that a number of these strategies are designed to facilitate anonymous banking, hence making it possible for persons with intention of committing illegal activities to use the system to their advantage.
[191] Directive [EU] 2018/843, sometimes referred to as AMLD5, as well as 5MLD.
[192] S Maxson, S Davis, and R Moulton, 'UK Cryptoassets Taskforce publishes its final report, (2019) 20, J of Investment Compliance 2, 28, since such companies facilitate anonymity through layering of funds hereby masking the origin of the assets.
[193] Ibid, 29, such platforms facilitate the anonymous transfer of cryptoassets between two individuals or businesses
[194] Ibid, 29, since individuals and businesses can use them to purchase or sell cryptoassets for fiat cash.
[195] Ibid, 29, which offer services similar to custodian wallet providers, and can provide the anonymous transfer or storage of cryptoassets.
[196] L Haffke, M Fromberger, and P Zimmermann. 'Cryptocurrencies and anti-money laundering: the shortcomings of the fifth AML Directive (EU) and how to address them'. (2019) 21 J of Banking Regulation, 3. The weaknesses imply that a verbatim transposition is bound to create legal uncertainties and introduce loopholes for individuals keen on engaging in illegal finance.
[197] See for example, in the Article 1(1) (c), which states that "persons trading or acting as intermediaries in the trade of works of art, including when this is carried out by art galleries and auction houses, where the value of the transaction or a series of linked transactions amounts to EUR 10 000 or more", there is a lack of specificity of who should be considered an intermediary in the trade in art, as well as the comprehensive definitions of works of art.

consultations.[198] The MLRs 2019, which was scheduled to take effect in January 2020, sought to reinforce the UK's AML/CTF regime in line with the propositions under the FATF.[199] The adaptation by the UK goes further than what the EU recommends[200] to eliminate the loopholes through which illicit financial activities are perpetrated within the UK financial system while also reducing the burden on those involved in a legitimate business. One key loophole is the imposition of supervisory mandates on small and micro cryptoassets companies, which are exempt from the regulatory perimeter in line with the risk-based approach applied by the EU.[201] Through the provisions, UK regulatory institutions can easily detect and investigate any suspected criminal/terrorist misuse of the financial system. The provisions under the directive apply to the existing forms of cryptoassets, the associated services and intermediaries.

The provisions under MLR 2019 recognise the need for a customised approach in determining whether an institution engaged in the UK 'by way of business' should fall under the regulatory perimeter. The criteria, which are based on self-assessment, entail four domains, including the regularity and frequency of business,[202] the relevance to other businesses in the UK,[203] the commercial element,[204] the commercial benefit,[205] and whether it has operations in the UK.[206]

---

[198] The lack of sufficient data arises from the fact that most of the available information is sourced from consultations which are not reliable, and the cryptoasset industry is rapidly evolving, thus any data collected in 2018 is most likely outdated.

[199] HM Treasury, 'Consultation on the Fifth Money Laundering Directive: Response To The Consultation' (HM Treasury, Jan 2020), <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/860491/5MLD_Consultation_Response.pdf> accessed 23 February 2023 who indicates that the changes to the AML/CTF regime in line with 5MLD seeks to achieve three key goals, including responsiveness to changes in the ML/TF risks, comprehensiveness by accommodating all domains of the AML/CTF regime, and alignment with the dynamic international standards such as those proposed under FATF.

[200] HM Treasury, n(2), for instance the definition of the registrable crypto businesses under MLR 2019, which broader that what is proposed under the 5MLD. In addition to benchmarking with the provisions under FATF, the UK, through the MLR 2019 seeks to achieve higher regulatory rigor.

[201] The UK has elected to include all cryptoassets companies in the regulatory perimeter regardless of their scope and scale, based on the premise that their exemption from the AML/CTF regime prevents the effectiveness and the AML/CTF policies from achieving their aim. After all, such the combined actions of multiple micro players can facilitate significant illicit activity.

[202] Businesses that frequently conduct businesses using cryptoassets are perceived as presenting higher risk than others, which necessitates their regulation and oversight.

[203] Companies that engage in cryptoassets business as a core function of their success and survival, relative to other activities receive more regulatory focus by the FCA.

[204] Companies and persons who advertise, act or hold themselves out in a manner that suggests that they offer services related to cryptoassets are regulated more than the others.

[205] Organisations or individuals who stand to benefit directly or indirectly from businesses related to cryptoassets activities fall under the regulatory parameter.

[206] Regulation 9 of the MLR 2019 outlines that in addition to other criteria for determining whether the business falls within the UK jurisdiction.

The implementation of 5MLD is facilitated through SAMLA 2018. which is a legislative framework customised to ensure the seamless transition from the EU-based AML/CTF regime to domestic systems. The Act empowers UK institutions to impose a sanctions regime designed to achieve national AML/CTF goals. The MLR 2019 recognises two categories of businesses involved in the cryptoassets industry that must adhere to the new regulations under the oversight of the FCA. First are the cryptoassets exchange providers[207] and custodian wallet providers,[208] all of which are classified as cryptoassets businesses. This section provides an outline of the changes to the existing AML/CTF regime on account of the 5MLD guidelines by the EU.

6.5.1 Expansion of the Administrative and Supervisory Oversight

The MLRs have mandated the FCA to adopt a stringent approach to administrating all businesses under its regulatory perimeter. The guidelines introduce the requirements for the provision of additional information by the businesses at registration. [209] Regulation 54 (1) (A), which bestows the duty of maintaining registers for specific relevant persons onto the FCA, was adjusted to include two new categories of persons, including cryptoassets exchange providers and custodian wallet providers. The FCA is also mandated to maintain a register for these two categories of persons on account of their role in the AML/CTF regime in the UK.[210]

The 5MLD has led to a highly customised approach to the determination of the competence and proficiency of individuals who are involved in cryptoassets businesses within the UK. Under Regulations 58(A) 1[211] and 2, the FCA establishes the criteria under the 'Fit and Proper' test for

[207] See Statutory Instrument *No. 1511, 'Financial Services: The Money Laundering and Terrorist Financing (Amendment) Regulations 2019* that defines the businesses as persons (legal or natural), who by way of business, engage in the exchange, or decide for the exchange of: cryptoassets for money; money for cryptoassets, or one cryptoasset for another. It also includes a person who operates any automated machines for processing the exchange of cryptoassets for money.

[208] Ibid, who defines custodian wallet providers, which includes persons, who, by way of business, provides services on behalf of customers for safeguarding, or safeguarding and administering, either cryptoassets, or private cryptographic key that are integral for holding, storing or transferring cryptoassets.

[209] The information includes the company's business plan, its program of operations, the organisational structure, the controls and systems in place, internal control mechanisms and arrangements for governance, and key personnel.

[210] In recognition of the dynamic nature of the ML/TF risks associated with the cryptoassets, regulation 56(A) in the same part recognises the imperativeness of transitional provisions for the requirements for registration of these two categories of businesses. In exercising the provisions under the regulation, the FCA has utilised the objectives basis in the legislative approaches implemented the TRR.

[211] Statutory Instrument No. 1511, *'Financial Services: The Money Laundering and Terrorist Financing (Amendment) Regulations 2019'* outlines that "58A.— (1) The FCA must refuse to register an applicant ("A") for registration in a register maintained under regulation 54(1A) as a cryptoasset exchange provider or as a custodian wallet provider if A does not meet the requirement in paragraph (2). (2) A, and any officer, manager or beneficial

use in determining who can be licensed to operate cryptoassets businesses in the UK. The guidelines cover requirements for 'fitness and suitability' for key personnel in the cryptoassets businesses by applying the risk-based approach, thereby eliminating persons who have criminal records[212] or persons who are inclined to facilitate ML/TF even when they have no prior criminal sanctions.[213]

Regulation 58A establishes the requirements for the FCA to collect sufficient information from and about key personnel in the management and operations associated with cryptoassets to determine whether such individuals are 'fit and proper' to facilitate the achievement of the goals of the AML/CTF regime.[214] The new guidelines recognise the need for continuous monitoring and supervision of institutions operating in the cryptoassets industry, following licensing and registration. The new requirements relate to procedures, policies, and controls for the acquisition and handling of information on transactions and customers.

Under the new MLRs, the FCA has introduced a novel set of penalties and sanctions[215] in the form of directions. The FCA has also established the right to offer directions to cryptoassets businesses. Regulation 74C (3)[216] defines the type of directions that the FCA can impose on the cryptoassets businesses, as well as the intended purpose, including the achievement of AML/CTF objectives. The decision to impose such directions offers the FCA the opportunity to supervise the industry, especially in response to new ML/TF risks identified concerning the use of cryptoassets in the UK.[217] Similarly, Regulation 60 (2A)[218] provides for the process of suspending or cancelling the registration.

---

owner of A, must be a fit and proper person to carry on the business of a cryptoasset exchange provider or custodian wallet provider, as the case may be".

[212] Section 58(A) (3)

[213] Section 58(A)

[214] I H Chiu, n(8)

[215] HM Treasury, n(10).

[216] The directions can be imposed before or after registration, and they are designed to correct any failures regarding compliance with the existing regulatory framework, preventing failures to comply, remedy any sustained non-compliance and prevent the cryptoassets business from being used for ML/TF activities.

[217] See Regulation 74C (9), which indicates that the FCA must provide the targeted businesses with clear writing on the rationale for the direction. Part 10 (a) to (e) requires the FCA to advice the business on the timeframe for solving the issues in the direction, as well as options for seeking interventions from an Upper Tribunal.

[218] The FCA may suspend (for such a period as it considers appropriate) or cancel the registration of a cryptoasset exchange provider or custodian wallet provider if, at any time after registration, the FCA is satisfied that the cryptoasset exchange provider or custodian wallet provider (as the case may be) does not meet the requirement in regulation 58A (2).

6.5.2 Changes to Entities Subjected to Oversight for ML/TF Risk

The MLR 2019 has expanded the regulatory scope for obliged entities following the realisation that institution-level practices are integral in the fulfilment of the goals of the UK AML/CTF regime. The amendments to disclosures under the 5MLD are motivated by the realisation that, in some cases, companies in some sectors hold knowledge or engage in operations and products/services that are too complex for other persons to understand without express clarifications.[219] These include companies in the property sector,[220] tax advisors,[221] art market participants,[222] and companies in companies in the cryptoassets industry, including cryptoassets exchange services providers[223] and custodians of cryptoassets wallets.[224] Specific focus is directed towards AML/CTF guidelines for art market dealers since the provisions in past regulatory frameworks did not consider this industry a target for ML/TF activity.[225] Chapter 3, which deals with the obligations for disclosures, mandates cryptoassets companies to take reasonable measures to ensure that regulators understand the business model and activities.[226] The disparity in knowledge regarding the cryptoassets business has also motivated the introduction of training

[219] Koster n(130) 381,

[220] Under Regulation 13, letting agents are identified as part of the companies in the property sector that are involved with high value transactions that present increased ML/TF risks. Under the new guidelines, agents have reported any transaction valued at least €10,000 per month. The obliged entities include agencies performing introductory services, letting only, collection of rents, letting of commercial properties, and those engaged in full property management.

[221] The MLR 2019 provides for obligations for persons who help or advise on tax affairs of other persons, whether directly or indirectly through a 3rd party, as opposed to the more generalist statement under MLR 2017, which set obligations for people who offer advice about tac affairs of other persons.

[222] S Hufnagel, and C King, 'Anti-Money Laundering Regulation and the Art Market', (2020) 40 Legal Studies, 1, 1, which indicates that under the new provisions, entities that participate in the arts market are considered obliged entities if they are involved in transactions exceeding €10,000.

[223] HM Treasury, 'Consultation on the Fifth Money Laundering Directive: Response To The Consultation' (HM Treasury 2020), <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/860491/5MLD_Consultation_Response.pdf> accessed 15 March 2023 whereby the regulations define cryptoassets exchange providers as persons who, by way of business, exchange or make arrangements to exchange cryptoassets for money, money for cryptoassets, or one cryptoasset for another. The category also includes persons who operate machines that use automated processes to exchange cryptoassets for money, or vice versa. As outlined in the consultations with government entities, and as included in the recommendations by the FATF, the measures focus on companies that exchange fiat currency for virtual currencies.

[224] The regulation relates to persons, who by way of business, offer services on behalf of customers to safeguard, safeguard and administer, either private cryptographic keys (that are necessary for holding, storing or transferring cryptoassets), or cryptoassets.

[225] Hufnagel, and King, n(222) 3, indicates that as of 2015, there were over 167 laws and regulations applying to the UK art market, thereby bursting the myth that the sector is not fully regulated. However, those provisions were neither articulate nor specific to the emergent ML/TF risks.

[226] See Regulation 60A (1) (b).

requirements for the relevant persons.[227] In response to these challenges, the UK has expanded the mechanisms for oversight and administration through obliged entities.[228] Under Regulation 13, obliged entities are mandated to advise the Companies House on any discrepancies in the information on beneficial owners.[229] Understanding how the UK has expanded the mechanisms for oversight and administration is critical to understanding the underlying principles that have shaped the UK efforts to implement the Financial War on Terrorism to counter cryptoassets-related terrorism financing in the country. The discussion addresses the third research question.

6.5.3 Expansion of CDD

The changes to mechanisms for CDD are motivated by the realisation that there are ML/TF risks associated with the absence of a zero-value threshold,[230] thereby minimising the risk of smurfing.[231] In the new era, the provisions for CDD apply to companies that issue, exchange, or act as intermediaries for cryptoassets. The 5MLD gold-plates several provisions under the MLRs to enhance certainty on the processes and outcomes of the 'know your customer' guidelines.

Similarly, under MLR 2019, CDD can be carried out through electronic means as long as such means are proven to be secure and incapable of misuse.[232] Most of the firms under the regulatory and supervisory perimeter have digitised their operations, thus making it redundant to rely on manual processes.[233] The MLR 2019 guidelines mandate that the technology for use in the electronic CDD should offer suitable levels of assurance for identification and verification of the identity of the individual.

---

[227] See Regulation 4(11) MLR 2019, amending Regulation 24(1) MLR 2017, which mandates the training and development of the skills of the relevant persons involved in AML/CTF within the institutions, with specific focus on the existing laws on AML/CTF, and data protection.

[228] See Regulation 13,

[229] The discrepancies of interest include differences in the information about the beneficial owners as provided to the public under the register for People with Significant Control, and what was included during the registration of the company in the register at Companies House.

[230] See Braddick, and others n(73) p.13, who define the zero-value threshold as the value of a transaction which is considered large enough to warrant imposition of customer due diligence activities.

[231] Ibid, who define smurfing as the act of structuring transactions involving large amounts into smaller transactions, in different places, or at different times. This ensures that all transactions are below the regulatory reporting guidelines for the purpose of avoiding detection.

[232] See Regulation 5(2)(c) MLR 2019, which is an amendment to Regulation 28 MLR 2017. See also FCA, 'Discussion paper on Distributed Ledge Technology' (FCA, 2017). <https://www.fca.org.uk/publication/discussion/dp17-03.pdf>, the introduction of electronic CDD is attributed to the changes in the technological abilities of the institutions involved in the UK's AML/CTF regime.

[233] Cryptoassets firms rely on digitized and automated systems, which nullifies any form of manual AML/CTF activities.

The obligations under enhanced due diligence include the following measures for businesses in the UK. Under MLR 2019, regulated institutions have the responsibility to obtain additional information on customers, with a focus on the ultimate beneficial owners. Under 5MLD, the mechanisms for identifying beneficial owners for complex financial products, unusual corporate structures[234] and unique business arrangements. The entirety of the regulatory requirements regarding beneficial owners is introduced into the AML/CTF policies.

The 5MLD framework introduces a risk-oriented amendment to e-money thresholds under the CDD guidelines on account of the vulnerabilities associated with these forms of assets. In addition to including all categories of e-money products, MLR 2019 changes the maximum amount that a customer can store on electronic platforms.[235] The scope of entities that must perform CDD is also expanded under Part 3. Section 27(7)(D)[236] is introduced as a way of ensuring comprehensiveness in CDD and EDD through all fulfilment channels, specifically those automatic processes for transactions with cryptoassets. The measures under this novel amendment are in recognition of the decision by UK regulatory institutions to assign criminal liability for inaccurate CDD or EDD.

The 5MLD framework recognises the importance of EDD in the AML/CTF regime in the era of cryptoassets. Under the framework, enhanced monitoring as an alternative to EDD is proposed for any transactions or relationships that involve or are established in a high-risk country.[237] The changes to CDD mechanisms seek to prime and orient the UK financial institutions

[234] Regulation 5(2)(b) MLR 2019, amending Regulation 28(8) MLR 2017, which relates to CDD for corporate bodies whose beneficial owners cannot be readily identified. In such scenarios, the regulation mandates the verification of the identities of the senior management, since in practice, these individuals are required under Company law to keep records about the company, and with their access, they can provide answers where necessary. Similarly, Regulation 5(2)(a) MLR 2019, amends Regulation 28(3A) to MLR 2017, by mandating senior management persons, as well as persons considered relevant for AML/CTF, to take reasonable measures to understand the corporate structure of the company, as well as the control structure, so they can provide information on such, in case required under UK law.

[235] Regulation 5(5) MLR 2019, amending Regulation 38 MLR 2017. The amendment seeks to control the amount of money that customers can store or transact through electronic means, since these electronic money platforms have features that facilitate ease of transfer, which is a vulnerability for ML/TF risk.

[236] H Kostern n(130), a cryptoassets exchange provider of the kind who operates a machine which utilises automated processes to exchange cryptoassets for money, or money for cryptoassets, must also apply customer due diligence measures in relation to any such transaction carried out using that machine (and for the purposes of this paragraph "money" and "cryptoasset" have the same meanings as they have in regulation 14A (1)).

[237] Regulation 5(4)(b) MLR 2019, amending Regulation 33(1)(f) MLR 2017, which states that '5MLD extends the existing requirement to carry out enhanced monitoring of any business relationship or transaction with a person "established in" a high-risk third country so that it covers any relationship or transaction "involving" a high-risk country.' Essentially, indicated that the definition of 'involving' with reference to transactions and relationships includes most transactions that are subjected to CDD.

towards adopting the risk-oriented approach to AML/CTF. The measures to replace CDD requirements with EDD are attributed to the propensity of cryptoassets businesses to set up their operations in jurisdictions with weak regulatory frameworks.

The MLR 2019 provides sector-specific guidelines for AML/CTF, focusing on the various professional bodies that are professional services. Regulation 26 mandates the approval of the beneficial owners, officers and managers.[238] The approval of these individuals facilitates the acquisition of information for the determination of whether the key personnel involved in AML/CTF hold the necessary qualifications and whether they have a criminal history. The changes in the CDD guidelines have improved the capacity of UK financial institutions to detect money laundering and terrorism financing, increasing the overall resilience of the sector against financial crime.[239] Nonetheless, there are concerns among the practitioners that the UK government is not doing enough to improve the due diligence requirement in the financial sector.[240] Understanding the expansion of the CDD requirement is important for the thesis as it demonstrates how the countries have responded to the Financial War on Terrorism after the 9/11 attacks, which is the first sub-question that the thesis aims to address.

6.5.4 Changes to Reporting Requirements

The MLRs 2019 have introduced novel reporting requirements that are designed to enable the UK regulatory institutions to monitor and oversee the transactions and operations of high-risk entities, transactions and countries.[241] The measures are included in the 'Disclosure Requirements' under Regulation 60A of the MLRs 2019.[242] The changes mandate the supervisory and regulatory institutions to provide secure channels for communications to enable clients, customers and firms in the various sectors to report any actual or potential breaches to the AML/CTF policies.[243] The

[238] Commonly referred to as BOOMs

[239] H Chitimira and S Munedzi, 'An Evaluation of Customer Due Diligence and Related Anti-Money Laundering Measures in the United Kingdom' (2023) 26 Journal of Money Laundering Control 127

[240] *Ibid*

[241] Regulation 74B, which states that "This regulation applies where the FCA reasonably considers that a report by a skilled person, concerning a matter relating to the exercise of the FCA's functions under these Regulations, is required in connection with the exercise by the FCA of any of its functions under these Regulations in relation to a relevant person who is a cryptoassets exchange provider or custodian wallet provider".

[242] The MLRs Regulation 60A requires cryptoassets businesses that are not covered under the Financial Services Compensation Scheme (FSCS), or the Financial Ombudsman Services (FOS) are required by the FCA to inform their customers of that reality before getting involved in business with them.

[243] The Institute of Financial Accountants, which is a self-regulatory supervisor, has outlined a policy for whistleblowing, as which provides instructions on the secure channel for communication. See Schedule 4 of the MLR

secure communication channels have to be designed in a manner that ensures that the identity of the whistle-blower is revealed only to the supervisory authority. The amendments achieve two key objectives under the AML/CTF regime. First, by assigning the responsibility of reporting on the operations to a skilled person,[244] the regulatory institutions can be assured of quality reports with value for intelligence and decision-making. Second, it reduces the proportion of SARs with a low value for intelligence, thus increasing the utility of the reporting regime in the AML/CTF activities.[245]

The changes brought about by the transposition of the 5MLDs under the MLRs 2019 represent the application of additional levels in the legislative frameworks, thereby leading to the achievement of novel objectives, as well as the improvement of results in other domains of the AML/CTF regime.

6.7 The Risk-based Approaches

One of the key questions that this thesis was set to examine is whether the Financial War on Terrorism re-tackles the concept of terrorism financing. To answer this research question, the present section will discuss how AMF/CTF policies were redefined to have a more risk-based focus. This risk-based approach categorizes jurisdictions based on their risk levels, especially relevant in the era of cryptoassets, ensuring regulatory actions match perceived threats. Factors influencing the UK's AML/CTF policies include political commitment from entities, the strength and past enforcement of AML/CTF policies, and subjective judgments, which highlights the transformation of the approaches towards TF that the Financial War on Terror brought about.

The UK has taken measures to reinforce its AML/CTF policies in line with the risk-based approach. Under this methodology, the AML/CTF policies and practices are channelled towards where risks and vulnerabilities are highest, based on probability and impacts of occurrence.[246] The risk-based approach has become the cornerstone of compliance with AML/CTF policies in the UK

2019, which mandates all supervisory institutions have to indicate the number of resources allocated for AML/CTF supervision in their reports to the HM Treasury.

[244] Regulation 74B(5)(a) and (b), which defines a skilled person as an individual who, according to the FCA, has the right skills to report on the matters concerned, and is approved by the FCA for such a purpose.

[245] Ryder n(149), 1175.

[246] OPBAS, n(132) who indicates that the risk based approach leads to increased focus on where the risk of occurrence of ML/TF is highest, as well as areas where the impact of such occurrences is highest. Furthermore, there is recognition of the fact that risks and vulnerabilities evolve over time, hence the need for continuous improvement.

due to the following rationales.[247] First, the UK has introduced objectivity in the classification of jurisdictions based on their vulnerability to ML/TF risks. In the era of cryptoassets, the UK ensures that the preventive and enforcement activities are proportionate to the perceived risks and vulnerabilities. The approach leads to regulatory hierarchy. Second, in determining the ML/TF risks, the UK focuses on the presence of political goodwill from those entities, including the individuals, corporations and jurisdictions.[248] Third, the UK takes into account whether the country has robust AML/CTF policies in place and how well the policies have been enforced in the past.[249] Finally, despite the objectivity, the UK also exercises a high level of subjectivity and arbitrariness in its decision-making process, especially in designating 'High-Risk' individuals, corporations and jurisdictions.[250] There are challenges in conceptualising what the term risk denotes, especially within an environment of risk management and control where risk is often associated with returns.[251]

The application of the risk-based approach in the UK environment is also complicated by the fact that AML/CTF policies are designed to perform multiple tasks, some of which are more evident due to the increased use of cryptoassets. In addition to combating ML/TF, risk-based AML approaches also ensure the soundness and safety of operations within the institutions.[252] With the emergence of the various cryptoassets in the UK, regulatory institutions face the challenge of determining the optimal enforcement mechanisms, as well as how to assess compliance. On the other hand, financial institutions operate in an uncertain environment, where they have limited ability to determine whether their perspectives on risk are aligned with what is expected by the regulatory institutions.

---

[247] IMF, 'United Kingdom: Financial Sector Assessment Program-Based Core Principles for Effective Banking Supervision-Detailed Assessment Report, (IMF, 2016), 291

[248] T Parkman, *Mastering Anti-Money Laundering and Countering-Terrorist Financing: A Compliance Guide for Practitioners (*London, Pearson UK, 2020),

[249] A Dill, *Anti-Money Laundering Regulation and Compliance: Key Problems and Practice Areas* (Edward Elgar Publishing, 2021).

[250] Financial Services Authority, 'Final Notice: Habib b Bank AG Zurich' (2012) <http://www.fsa.gov.uk/static/pubs/final/habib-bank.pdf> accessed 16 March 2023 whereby the Habib Bank was fined for failing to list Kenya and Pakistan as High Risk Countries. On the contrary, see B Dolar, and W Shughart, 'Enforcement of the USA Patriot Act's anti-money laundering provisions: Have regulators followed a risk-based approach?' (2011) 22 Global Finance Journal, 1, 19.

[251] Rather than perceiving risky cryptoassets as elements of AML/CTF that should be controlled and regulated, some FIs perceive the high risk as the basis for charging higher fees.

[252] A Bello and J Harvey, "From a risk-based to an uncertainty-based approach to anti-money laundering compliance," (2017) 30 Security Journal, 1, 24., who indicates the soundness and safety of operations is integral in maintaining the reputation of the institution, keeping its integrity at the benchmark levels, and positively influencing profits.

6.8 Case law on crypto-related cases in the UK

An evaluation of the UK approach to ML and TF is not going to be complete without examining how the UK court has responded to the cases that have been brought to them for such offences. Such a discussion is also insightful as it can help identify the legal precedents that the court has developed to support the prosecution of ML/TF offences in light of the growing propensity of terrorist organizations to rely on cryptoassets to conceal their activities. A discussion on the current case law on crypto-related cases in the UK will also help the researcher address one of the key questions, namely: What are the legislative responses to terrorism financing in the UK, and how effective are they?

The decisions in the case laws above culminate in legislative approaches that can be traced to different levers based on the nature of the claims. The discussion herein reveals the extent to which UK courts have gone to apply existing legal principles in bringing injunctive relief to claimants in cases involving cryptoassets. It also highlights the potential challenges that claimants face concerning the burden of proof in unique cases involving unknown defendants and dealing with third parties who are faced with potential contractual breaches to facilitate judgements.

AA v Persons Unknown [2019][253]

The claimant, an insurer of a Canadian Company, was a victim of a ransomware attack, with payment demanded through Bitcoin.[254] The claimant obliged and transferred the Bitcoin to the designated wallet. After the successful decryption of the files, the claimant sought to recover the ransom and traced the cryptoassets to a wallet associated with and controlled by a crypto exchange entity called Bitfinex, which is operated in the British Virgin Islands. The claimant then sought a proprietary injunction over the Bitcoins. The decision of the courts included granting the proprietary injunction for third-party disclosure[255] since Bitcoin is considered property under English Law. Despite its intangibility, the UK Jurisdiction Taskforce[256] of Lawtech UK[257]

[253] EWHC 3556
[254] The hacker bypassed the firewall of the company that offers anti-virus software to the insurance company, then deployed an encryption software to the systems of the company, upon which they demanded $1200,000 in Bitcoin before sending the decryption key.
[255] In line with the FCA guidelines for all registered cryptoassets services providers, Bitfinex was mandated to provide information regarding the identity of the hackers on account of the fact that they held an account with the company.
[256] UKJT hereafter
[257] UKJT, '*Legal* Statement on Cryptoassets and Smart Contracts', (Nov 2019), <https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-

concluded that Bitcoin was a novel form of property since it can be defined identified, and has a high degree of permanence.[258] The departure from past provisions under UK law that property can only be chosen in possession or action,[259] the courts reiterated that such an approach is fallacious since technological advances had made it possible for a novel type of property outside the traditional conceptualisations. Finally, the proceedings were carried out in private, at the request of the plaintiffs, by applying the precedence from *Cape Intermediate Holdings Ltd v Dring* [2019].[260]

Ion Science v Persons Unknown [2020]

The claimant had paid a total of £577,002 in investments, contributions and commissions for participation in an ICO. The transactions involved 'unknown persons' who were linked to Neo Capital, a Swiss entity, with payments going through an association of Neo Capital, referred to as 'Ms Black'. However, the claimants discovered that Neo Capital was not a registered company under Swiss law and had no operations except a website. Furthermore, it was subject to warnings by Swiss regulators regarding its operations. Based on testimony by experts, it was discovered that the funds could be traced to two Bitcoin exchanges.[261] The claimant sought relief through three applications, which are of significance in the application of the existing laws on claims linked to the cryptoassets industry. First, this was the first case involving ICO Fraud[262] to be brought before

content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf> accessed 15 May 2024 which clarifies that Bitcoin can be treated as property since cryptocurrencies: are capable of being owned, can be defined and their owners identified, are permanent financial assets and exist as long as they are not cancelled, redeemed, repaid or exercised, are stable but subject to deterioration in value, loss and corruption and cannot be disqualified from being properties simply because of their distinctive features.

[258] The judge applied the Patents Act 1977 in arriving at the decision, whereby patents are considered intangible properties, even though they do not meet the standards for choses in action. The law further suggests that there may be a third category of property, which could be subjected to lien under common law, and where necessary, they can be defined as a hybrid form of property, with virtual choses in possession.

[259] The decision was also derived from the provisions under POCA 2002, Section 316(4) (c) which indicates that in principle, Bitcoin possesses all characteristics of property.

[260] *Cape Intermediate Holdings Ltd v Dring* [2019] UKSC 38, where the plaintiffs sought private hearings to ensure the success of the case. In *AA v Persons Unkown [2020*], the importance of conducting hearings in private enabled the court to achieve the objective of the hearing by ensuring that the Unknown persons did not dispose of the Bitcoin, and that the details provided on the mechanics of the fraudulent activities were not publicised in a manner that attracted copycat cybercrimes.

[261] Kraken Cryptocurrency Exchange and Binance Cryptocurrency Exchange

[262] See P Andres and others, 'Challenges of the Market for Initial Coin Offerings' (2022), 79 Int Rev of Fin Analysis, , who indicates that ICO lacks the right regulatory framework which is necessary for protecting the clients from fraud. From a legal perspective, due to lack of standards, third party verification, and lack of reliable audit trail to support legal claims, the limited requirements for disclosure lead to significant asymmetries in information, which can compromise judicial processes.

the commercial court. Second, it was the first case where a bankers' trust order[263] was issued against entities outside the UK jurisdiction.[264] The BTO served as a proprietary injunction[265] and a disclosure order.[266] Finally, it was the first time the principle of *lex situs* was applied in cases involving cryptoassets.[267] The justification for disclosure orders, and hence the determination of whether the UK courts had jurisdiction over the Person Unknown, was determined through the three-limb test.[268] Essentially, cryptoasset exchanges could be compelled to disclose information regarding details that are integral in the judicial decision through free-standing bankers' trust orders.[269] This decision is based on a 150-year-old practice whereby English courts assert their jurisdiction over defendants from other countries.[270] Through a multiplicity of jurisdictional 'gateways', the courts have identified the scope of circumstances under which the UK courts can take on claims targeting defendants from overseas, as outlined in the three-limb test. The legal precedence, which utilises provisions under the Civil Procedure Rules (1998) Practice Directions,[271] introduces a new legislative approach to AML/CTF measures. Aggrieved parties,

[263] BTO hereafter

[264] For a definition of Banker's Trust orders, see T C Hartley, *International Commercial Litigation: Text, Cases and Materials on Private International Law*, (CUP, 2009), 457, which cites the decision in *Bankers Trust v Shapira* [1980] 1 WLR 1274 (CA), whereby the plaintiff acquired orders to enable them to trace assets through the banking institution that was involved in the claim of fraud.

[265] This type of injunction sought to place a globally effective freezing order on the defendant, and to force ancillary disclosure of who the unknown persons were. the proprietary injunction was granted, on account of policies under UK law, as well as case law on the treatment of cryptoassets as property. See *AA v Persons Unknown* [2019] EWHC 3556 and a foreign case New Zealand case of *Ruscoe v Cryptopia Ltd (in liquidation)* [2020] NZHC 782.

[266] The disclosure orders are implemented through a Bankers Trust Order, which was sought against the Cryptoassets exchanges.

[267] In cases involving cryptoassets, the courts determined that the *lex situs* of the cryptoassets is the location where the relevant participants in the Bitcoin system, or rather the person, legal or natural, who owned the Bitcoin, is domiciled. Since the Bitcoin were in the UK, then the UK courts had jurisdiction over the case.

[268] See W Day. 'Jurisdictional Gateways in The CPR', (2018) 77 The Cambridge Law Journal, 1, 36 who indicates that based on the test, the court determined the following: first, England was the most appropriate forum for conducting the trial, there was a serious claim that merited concern, and there were arguable cases within one of the gateways under Civil Procedure Rules Practice Direction, 6B, specifically gateway relating to torts and Gateway 15 for equitable claims on property. The Decision is also based on an earlier decision in *American Cyanamid Co (No 1) v Ethicon Ltd* [1975] UKHL 1.

[269] Unlike the traditional banking trust orders, free-standing banking trust orders indicate the extent to which UK courts are willing to go in facilitating the recovery of assets by introducing flexibility into the judicial decisions in response to the ever-evolving legal landscape associated with cryptoassets.

[270] A Arzandeh, '"Gateways" Within the Civil Procedure Rules and the Future of Service=out Jurisdiction in England', (2019) 15 J of Private Int. L. 3, 518.

[271] CPR hereafter. See Statutory Instruments, 'The Civil Procedure Rules 1998-1998-No. 3132. (1998) <https://www.legislation.gov.uk/uksi/1998/3132/part/25.2/made/data.pdf> accessed 15 March 2023 CPR 25.1(g), which states that the court may grant the following interim remedies "an order directing a party to provide information about the location of relevant property or assets or to provide information about relevant property or assets which are or may be the subject of an application for a freezing injunction"

including individuals, can institute criminal proceedings that cover a broad range of alleged infringements.[272]

Fetch.ai Ltd v Persons Unknown [2021] EWCH 2254

The plaintiffs sought several remedies from the courts after being defrauded by "persons unknown". The fraud was perpetrated when the 'persons unknown' acquired access to their cryptoassets accounts valued at $2.6M held with Binance, then traded the cryptoassets held in the exchange with third-party buyers. Based on the validity of their claims, the plaintiffs obtained worldwide freezing orders[273] and orders to enable them to acquire information necessary for tracing the cryptoassets from the cryptoassets exchange (Binance).[274] The issuance of a Bankers Trust Order against a company situated outside the jurisdiction of the UK courts through free-standing orders provides an additional tool for UK courts to achieve injunctive relief. Furthermore, a review of the decision, in this case, provides criteria for determining when such an order may be provided upon application by claimants in a case involving cryptoassets fraud.[275]

Vorotyntseva v Money-4 Ltd [2018][276]

In this case, the claimant, Ms Vorotyntseva, had deposited over £1.5M in a trading platform called Nebus to acquire Bitcoin and Ethereum for retail trading purposes. However, following concerns that the operations of the company were not clear, she made inquiries that went unanswered. To recover her investments, she applied for a worldwide freezing injunction.

The courts granted a freezing injunction against Nebus and its directors, which is a cryptoassets trading company. The decision was based on proof that the claimant faced the risk of losing her assets. The court also honoured the argued balance of convenience when granting the injunction.[277]

---

[272] These civil cases include personal injury tort claims, contract disputes, equitable claims, class action suits and property disputes.

[273] As well as a proprietary injunction relief against the unknown fraudsters.

[274] Commonly referred to as Bankers Trust and Norwich Pharmacal order

[275] The applicant must prove that: they have lost money due to definite case of fraud; there is an actual prospective that the information sought from the bank can lead to determination of the whereabouts of the money, or recovery of the assets; the information sought relates to a specific range of subjects; the applicant can compensate the bank for any losses incurred; the application if in time and not delayed; there are provisions for gagging the bank to prevent it from tipping off the account holder; the application can be made without notifying the bank if it considered compromised; the applicant can provide any information deemed necessary by the courts relating to the case; and that the BTO is justified on its own, and not a secondary consideration in the ongoing case.

[276] *Vorotyntseva v Money-4 Ltd* [2018] EWHC 2596 (Ch),

[277] See A Seuba, *The Global Regime for the Enforcement of Intellectual Property Rights,* (CUP 2017), 238, who indicates that in favour of decisions to the plaintiff, the balance of convenience implies that if the injunction is denied

Robertson v Persons unknown CL-2019-000444

The plaintiff was the victim of a spear-phishing attack targeting email accounts of an institution where he had invested in the use of cryptoassets. The plaintiff then transferred 100 Bitcoin to a wallet owned by the fraudster, who subsequently transferred 80 Bitcoin to a wallet held by the crypto-exchange service provider. Upon establishing the presence of serious issues for judicial intervention regarding the proprietary claim, the judge granted an asset preservation order[278] over the cryptoassets. Although the judge failed to provide a freezing order against the fraudster's wallet in pursuit of the 20 Bitcoin, they recognised the argument that the claimant had a legitimate proprietary claim over the 80 Bitcoin held with the crypto exchange. The judgment clarified that the crypto-exchange wallet holder to whom the freezing order was served could be considered an innocent third party in the transaction.

Toma & True v Murray [2020][279]

In this case, a transaction involving the sale of Bitcoin failed to materialise, with the claimants, who were involved in the transaction as sellers, being left without Bitcoin or the money for the sale. They subsequently sought a proprietary injunction against the account held by the buyer. However, the courts determined that such an injunction for proprietary remedy was not necessary since damages were a sufficient remedy in the case.[280] Unlike in judicial precedence for interim claims on Bitcoin under *AA v Persons Unknown [2019],* the defendant was identifiable and available, and they provided evidence of unencumbered properties valuable enough to act as a security for personal remedy. Similarly, in this case, the decision by the court appears to have equated personal and proprietary remedies[281] due to the prevailing circumstances. The intangibility of Bitcoin facilitates the decision as a property, and that restitution can be made in monetary terms.

---

and the claim is ultimately decided in favour of the plaintiff, the inconvenience that they suffered is greater than what would have been caused to the defendants if the injunction is granted, but the claim is ultimately dismissed.

[278] APO hereafter. This is a provisional remedy designed to preserve monetary instruments or properties in a diversity of ways to prevent unlawful activities or ML offenses before a civil claim relating to that property can be concluded.

[279] *Toma & True v Murray* [2020] EWHC 2295(Ch)

[280] The judge considered a key characteristic of cryptoassets in making this decision in the fact that the value of the assets is highly volatile. As a result, placing the injunction on the bitcoin wallet posed the risk of disproportionate loss of the defendant losing if the value of the Bitcoin dropped. However, the decision would have been varied if there were disagreements on the price and value of the Bitcoin.

[281] See F McCarthy, J Chalmers, and S Bogle, *Essays in Conveyancing and Property Law in Honour of Professor Robert Rennie* (Open Book Publishers, 2015), 103, who defines personal remedy as a claim for monetary compensation that is sufficient to what the claimant lost, while proprietary remember involves attachment to a specific property, due to its unique characteristics.

Based on a review of these cases, it is apparent that the decisions reveal that victims of cryptoasset fraudsters can be assured of remedies since the UK courts have displayed amenability when granting injunctive relief. However, some of these decisions are devoid of opposing arguments since the discourse herein relates to the applicant's duty[282] rather than the contestation of defendants, such as innocent third parties and crypto exchanges.[283] Rather than being conclusive, the decisions in these cases provide a roadmap for plaintiffs to frame their claims for restitution. They also provide some clarity on the issues that arise during the judicial proceedings based on the characteristics of the claim. For instance, whereas the application of the lex situs principle is deemed integral in determining the rights and entitlements to property, the presumption of a single situs is challenging to apply in cases involving cryptoassets.[284] The process of tracing and recovering cryptoassets may be problematic if the traditional conceptualisation of lex situs is applied herein; hence, there is a need to apply the principle of lex fori.[285] Through the principle of lex fori, it is possible to apply elective situs, whereby the jurisdiction is determined when the contracts for the transaction are being carried out or determined by the participants in the distributed ledger technology. While none of the cases discussed above has addressed specifically how the UK court is approaching the TF offences carried out through cryptoasssets, the current jurisprudence demonstrates that the courts are not hesitant to impose injunctions and orders when cryptoassets are used for fraudulent purposes, showcasing that the current framework is robust enough to enable an effective prosecution of TF offences in the cyber realm.

The UK judiciary has addressed numerous cases involving cryptocurrencies, showcasing the evolving challenges in countering money laundering (ML) and terrorism financing (TF) in the context of digital assets. These cases illustrate the judiciary's adaptability in applying traditional legal principles to novel technologies and financial instruments. For example, in *R v Choudhary* (2015), although not directly related to cryptocurrencies, this case addressed terrorism financing

[282] Essentially, most of these cases do not feature contestation by the defendants, although it is unlikely that a fraudster, who is involved in ML/TF, will compromise their identity as they attempt to discharge the orders. The most common outcome is that the criminal will simply look for alternative ways to conduct their illegal affairs, rather than expose themselves to further liabilities. However, there are two categories of parties who are expected to contest the decisions.
[283] First, innocent third parties.
[284] Primarily due to the intangibility of cryptoassets, coupled with the fact that the digital assets are constituted on a distributed platform/network at any point in time.
[285] See A Maguire, 'Cryptoassets-Obtaining English Freezing and Proprietary Injunctions in Relation to Cyberfraud', (2020). <https://littletonchambers.com/wp-content/uploads/2020/10/Cryptoassets-AMG-Oct-2020.pdf>, accessed 15 May 2023 who defines *lex fori* as a principle of choice of forum where a law will be applied.

under the UK Terrorism Act 2000. The accused was prosecuted for using conventional methods to fund overseas terror operations. This ruling laid foundational precedents for prosecuting similar offences involving digital currencies, highlighting the flexibility of UK courts in adapting to evolving financial technologies.[286] In ISIS Crypto-Financing Investigation (2017), a pivotal case uncovered attempts to transfer funds to ISIS operatives in Syria using Bitcoin wallets. The investigation demonstrated the vulnerabilities of cryptocurrencies in bypassing traditional banking systems, leading to heightened awareness of the risks associated with digital assets in terrorism financing.[287] In Operation Kryptos, the Metropolitan Police and the Financial Conduct Authority (FCA) disrupted a network funnelling cryptocurrency to Middle Eastern terror groups. The operation highlighted weaknesses in peer-to-peer crypto exchanges and the dark web, showcasing the urgent need for stricter oversight in the cryptoasset market.[288] In collaboration with international partners, UK regulators uncovered a scheme in which individuals used Bitcoin to funnel money to ISIS operatives in Turkey. The case underscored vulnerabilities in cross-border cryptocurrency transactions and reinforced the need for robust international AML/CTF collaboration.[289]

In 2021, a UK-based individual used cryptocurrency donations to fund extremist propaganda online. Authorities successfully froze the individual's cryptocurrency wallet, marking a significant precedent in the application of freezing orders to combat terrorism financing in the digital asset sphere.[290] The European Cryptojihad Investigations involved a network financing terror cells across Europe through cryptocurrency wallets, with UK intelligence playing a critical role in uncovering the scheme. The investigation highlighted how digital currencies were being exploited to bypass traditional financial systems.[291] A joint investigation by the FCA and MI5 revealed a London-based group using Bitcoin to transfer funds to overseas terror cells. This case highlighted

[286] *R v Choudhary* (2015) <https://www.judiciary.uk/wp-content/uploads/2015/09/r-v-choudary-judgment.pdf > accessed 15 May 2023
[287] National Crime Agency, 'Annual Report 2017' (NCA, 2018) <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/45-nca-annual-report-2017/file> accessed 15 May 2023
[288] Financial Conduct Authority 'Operation Kryptos Report 2019' <https://www.fca.org.uk/publication/operation-kryptos.pdf> accessed 16 May 2024
[289] FATF, 'Annual Report 2020' (FATF, 2021) <https://www.fatf-gafi.org/publications/methodsandtrends/documents/annual-report-2020.html> accessed 15 May 2023
[290] National Crime Agency 'Annual Report 2021' <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/47-nca-annual-report-2021/file> accessed 24 May 2023
[291] Europol, 'Report on Cryptocurrencies in Terrorism Financing' (EUROPOL 2021 https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-terrorism-financing-2021.

innovative laundering techniques and drove updates to the UK's counter-terrorism financing protocols.[292] The UK played a supporting role in a multinational investigation into Hamas-affiliated groups using Bitcoin donations to fund militant activities. This case highlighted the risks posed by crypto donations and led to recommendations for tightening AML/CTF protocols in this area.[293] The Metropolitan Police uncovered the illicit use of cryptocurrency ATMs to fund overseas terrorism activities. The investigation emphasized the significant risks posed by poorly regulated crypto infrastructure, which led to calls for enhanced oversight of such services.[294] The FCA disrupted a network facilitating terrorism financing through anonymous cryptocurrency transactions on the dark web. This case underscored the growing complexity of tracing illicit crypto transactions and reinforced the importance of technological solutions in AML/CTF enforcement.[295]

6.9 Conclusion

The discussion herein reveals the trajectory of change in the UK's AML/CTF regime in the era of cryptoassets. Despite the variations in the perceptions towards the riskiness of cryptoassets among HM Treasury, the BoE and the FCA, all institutions involved in the supervisory and regulatory institutions recognise the need for improvement in the AML/CTF regime across all domains. Right from the start, it is apparent that the UK has adopted a 'watch and learn' approach to the regulation of cryptoassets, with the most decisive and comprehensive measures materialising as late as 2018. The lacklustre approach is attributable to the perception that cryptoassets have negligible importance in the financial system. There is also evidence that the diverse legislative approaches used herein are focused on acquiring an appreciation of the characteristics of the risks associated with cryptoassets in the UK financial sector, as well as the exposures to ML/TF due to such risks. The following conclusions are made.

[292] MI5, 'Annual Security Repor't' (MI5, 2022), <https://www.mi5.gov.uk/publications/annual-security-report-2022> accessed 15 May 2024

[293] National Crime Agency, 'Hamas Bitcoin Donations Investigation' (NCA, 2022), <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/55-hamas-bitcoin-donations-2022/file> accessed 16 May 2024

[294] Metropolitan Police 'Counter-Terrorism Unit Report (2023)' <https://www.met.police.uk/about-us/counter-terrorism/2023-report> accessed 16 May 2023

[295] Financial Conduct Authority, 'AML/CTF Annual Report (2023) <https://www.fca.org.uk/publication/aml-ctf-2023-report.pdf> accessed 15 May 2023

First, the regulations are designed in a manner that promotes the independence and interdependence of the regulatory institutions without compromising the supervisory functions. Independence plays a key role in how the regulatory, supervisory and oversight regimes are deployed to achieve the AML/CTF goals in the era of cryptoassets. The prominence of the primary and secondary institutions in the development of tertiary institutions that focus on private-public partnerships reveals how much the UK has sought to balance the two outcomes.

Second, the discussion reveals that the complex and novel nature of techno-legal regulation has led to the emergence of legislative approaches that combine hard and soft law elements. In deploying the hard and soft law elements, the UK has developed codes of industry practice, laws and regulations, guidance and standards, rules by regulators, and industry best practices, which help to synthesize the laws into guidelines that are more applicable in the practical world. The features arise due to the involvement of multiple institutions under the JMLIT model. The model creates a favourable environment for the implementation of the intelligence-oriented approach, which is integral in regulating the ML/TF risks arising from different jurisdictions. The JMLIT model is a befitting inclusion in the institutional framework under the AML/CTF regime since it addresses several of the weaknesses in compliance with FATF recommendations while also bridging the gaps associated with the SARs regimes. Third, it is also apparent that the legislative approaches utilised herein feature both sector-specific and generic elements that facilitate a forward-looking approach based on prudent regulation of conduct. Rather than impose restrictive regulatory regimes that focus on ‘zero failure’, the AML/CTF regime is designed to eliminate the possibility of significant interruption in the functioning of the financial services sector while also avoiding material adverse effects on consumers. The flexibility contributes to the increased agility of the UK judicial system, thereby adapting the existing legal framework to enable it to provide relief to claimants while also fulfilling the traditional AML/CTF objectives.

Fourth, the legislative approaches discussed herein are also indicative of measures to ensure that the existing legal framework is fit for regulating the dynamic cryptoassets economy. These include the introduction of strategies for consultation in its legislative approaches, with the goal being to utilise feedback from persons within the regulatory perimeter, as well as those who are directly involved in the cryptoassets industry. The legislative approaches also facilitate the improvement of the dysfunctional elements of the AML/CTF regime, such as improvements to customer due diligence through enhanced due diligence and identification of the ultimate

beneficial owner, changes to the SAR regime through digitisation, and the classification of cryptoassets based on the risk profiles.

Fifth, despite the multiplicity of recent reforms to the AML/CTF regime, there are still some inconsistencies in the AML/CTF in the UK in the era of cryptoassets. The inconsistencies start with the disparity in the perceptions of the key institutions involved in the AML/CTF activities. The variations in the assessed riskiness of cryptoassets against the backdrop of increasing efficiency in the AML/CTF systems reveal that the country has utilised legislative approaches that are complementary and supplementary in nature. The legislative approaches enable UK institutions at the primary, secondary, and tertiary levels to acquire and retain legitimacy while navigating the often uncertain environment of the cryptoassets industry.

Sixth, the legislative approaches are also adopted as a way of eliminating the practical bottlenecks whose presence in a regulatory regime can adversely affect businesses or relationships with clients. One of the most common approaches is through multi-stakeholder consultations that are adopted as guidelines and transposed as part of gold-plating regional and international frameworks. There is evidence of careful consideration and widespread consultations to ensure that the legislative approaches consider the impact of the supervisory, monitoring, regulatory and enforcement regimes for ML/TF purposes.

Seventh, in keeping with the goals of maintaining its status as the leading financial sector in the world, the UK has deployed an AML/CTF regime that is cognisant of the utility of the risk-based approach. However, it goes further by adopting and gold-plating the standards and propositions from other competent authorities, such as the FATF and EU. The gold-plating ensures that the UK remains ahead of its peer jurisdictions while also recognising that criminals and terrorist groups are interested in identifying loopholes in the most current regulatory frameworks.

Finally, the new approaches help to reduce the path dependence by regulators, who are still developing regulatory ontologies for cryptoassets. These path dependencies lead to narrow-mindedness and limit the proactivity of the regulatory institutions in adapting to new strategies in the AML/CTF regime. Evidence of the reduction in path dependence exists in the gradual introduction of the ‘failure to prevent’ model, which is represented by the assignment of personal accountability and liability for ML/TF that occurs due to their actions or omissions.

The present chapter has provided important insights into the evolution of the UK framework for fighting money laundering and terrorism financing and the changes that the UK has made to address the risks that cryptoassets pose for businesses and individuals. The chapter has also been helpful in addressing several research questions that the study seeks to address. First, it presents the CTF legislative responses towards terrorism financing in the UK, addressing the first research question of the study. Second, it discusses how the UK has applied the FATF recommendation and other relevant international and national frameworks on ML and TF, addressing the second research question. Third, it discusses the implementation and efficiency of the Financial War on Terrorism as it is carried out in the United Kingdom, which provides an answer to the third research question.

Chapter VII: Comparison between Bahrain and the United Kingdom

7.1 Introduction

The emergence and expansion of the cryptoassets economy is the most recent and conspicuous example of an industry that poses novel money laundering/terrorism financing (ML/TF) vulnerabilities and risk taxonomies that necessitate the extension or clarification of the anti-money laundering/counter-terrorism financing (AML/CFT) regime. In addition to magnifying pre-existing risk typologies, the change has thrust most jurisdictions into regulatory and supervisory uncertainty as they scramble to respond to the highly volatile situation. While most countries have preliminary infrastructure that can be fine-tuned to form the foundation for the required level of reactivity and proactivity to ML/TF risks, the velocity with which technology permeated most corners of the globe appears to overwhelm some countries, despite the available resources and capabilities for AML/CFT. Therefore, a comparative analysis of the situation in Bahrain and the United Kingdom (UK) is provided. The analysis relies on the input from the two previous chapters in comparing how the 'Financial War on Terrorism' has been implemented in Bahrain and the UK. The analysis compares the effectiveness of the measures under the Financial War on Terrorism in countering the potential threats from the use of digital currencies in the TF between Bahrain and the UK. In this aspect of the analysis, the comparison will focus on the Financial Intelligence Units (FIUs) and their roles, as well as the characteristics of the FinTech sectors in both countries.

Firstly, the mutual evaluation reports[1] for the UK and Bahrain are compared, with a focus on technical compliance. Secondly, the analysis involves benchmarking the UK and Bahrain against one another to identify what lessons each country can learn from the other. Thirdly, the acceptability of cryptocurrency exchanges is analysed on account of their centrality to the cryptoassets economy and the prevailing AML/CFT regimes. The fourth section entails a discussion of the FIU, whereby comparative analysis culminates in the identification of the operationalisation of FIUs for AML/CFT in the era of cryptoassets. Finally, the analysis branches to the FinTech sectors to determine their structure, goals, composition and drivers of growth within the current regulatory and supervisory regimes. A conclusion is provided based on the analysis.

[1] MER hereafter.

7.2 Analysis of FATF MER between Bahrain and the UK

The MER features measures under the intermediate outcomesand immediate outcomesto achieve FATF's high-level objectivefor the particular country. It also highlights the extent to which the two countries have implemented and complied with the measures based on the strengths and weaknesses identified in the previous MER.[2]

The comparison focuses on the initiatives, strategies and AML/CFT architectures, as well as the risk typologies concerning the market structure. Over time, despite the significant changes occurring in the cryptoassets sector, it is widely recognised that there is no justification for changes to the FATF standards, except for the technical enhancements in response to the changes in how the virtual assets and VASPs have proliferated. In most jurisdictions, concerns relate to how the standards are applied in practice rather than questions on the sufficiency and nature of the standards themselves.

7.2.1 Robustness of the Understanding of the ML/TF risks

Based on the National Risk Assessments (NRA) from both countries, there are differences in the extent to which the two countries understand the current ML/TF risks. The UK has a robust understanding of its ML/TF risks due to the sufficient cooperation and coordination of AML/CFT issues at the national level. The UK NRA reveals significant improvements in the AML/CFT policies and operations since the previous evaluation. The UK has a proven ability to understand the ML/TF risks, which inform the design and implementation of AML/CFT policies and strategies. The robust appreciation of risks is matched by an effective program for cooperation and coordination of AML/CFT issues at the operational and policy levels. Conversely, Bahrain is perceived as having a moderate appreciation of those risks since the NRA process was still ongoing at the time of the review. Furthermore, since the ML/TF risks in the country are still evolving, an accurate and comprehensive assessment can only be provided once the NRA process is complete.

7.2.2 Proactivity in Investigating, Prosecuting and Convicting Illegal Activity

The UK has shown proactivity in investigations, prosecutions and convictions for illegal activities associated with ML/TF.[3] A high level of proactivity is achieved through the robust system for

[2] UK's last MER was released in 2007, with a follow up report in 2009. Bahrain's first MER was published in 2006.
[3] T Keating and Others, n(4)

public-private partnerships to achieve TF objectives. Proactivity is also driven by the lessons learnt from experiences in implementing the AML/CFT obligations under various market conditions.[4] Bahrain displays proactivity in coordinating and cooperating concerning the exchange of information for operational purposes. Authorities in the country have introduced several initiatives and policy actions in response to the ML/TF risk exposures. However, the goals and actions under those initiatives and policy actions require strengthening and alignment with the relevant ML/TF risks.

7.2.3 Propensity to Identify, Pursue and Prioritise ML/TF Investigations

The UK is aggressive in the identification, pursuit and prioritisation of ML/TF investigations and prosecutions.[5] To improve its efficiency, the UK has prioritised investigations into high-end ML activities. The approach has led to auxiliary preventative effects, whereby criminals are cautious of getting caught due to the highly effective AML/CFT and counter-proliferation regime in place across the UK. On the other hand, Bahrain has a well-developed system for accessing financial intelligence and other forms of information necessary for initiating investigations targeting ML/TF and PF. The framework is linked to the associated predicate offences. The country initiated 43 ML investigations, some of which are still ongoing, which culminated in the sentencing of perpetrators in 9 of those investigations.[6] Bahrain's regulatory framework has sufficient capacity to implement targeted financial sanctions[7] against entities involved in TF and proliferation financing.[8] The requirement for prompt implementation of TFS is integral in enabling regulators to intervene by stopping the transactions, seizing or confiscating the assets of the perpetrators, and imposing other befitting sanctions on the perpetrators in accordance with the law and policy. However, as observed under Recommendations 21, whereby the country is assessed to be 'Largely Compliant', most of the DNFBPs, including legal and natural persons, operating in the country are not obligated

[4] N J Maxwell, 'Expanding the Capability of Financial Information-Sharing Partnerships' (2019) <https://www.futureis.com/uploads/3/7/9/4/3794525/pr%C3%A9cis_of_ffis_paperexpanding_the_role_of_fisps_-_march_2019.pdf >Accessed 3 December 2022

[5] See FATF, 'Anti-money laundering and counter-terrorist financing measures– United Kingdom, Fourth Round Mutual Evaluation Report, FATF,' (FATF, 2018), <http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-united-kingdom-2018.htm> Accessed 20 November 2022

[6] FATF-MENAFATF, Anti-money laundering and counter-terrorist financing measures - Bahrain, Fourth Round Mutual Evaluation Report, (FATF 2018), <http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-bahrain-2018.html > Accessed 3 December 2022

[7] TFS hereafter.

[8] PF hereafter.

to take such measures for TFS against PF and TF. They also lack the infrastructure and resources to perform such functions since there is no institutional framework to facilitate the processes.[9]

7.2.4 Availability of Reliable Financial Intelligence

The UK guarantees the availability of reliable financial intelligence, with the proper monitoring and analysis of the available data performed regularly by competent authorities in support of ML/TF offences. The amendments effected through section 145, which are referred to as Information Orders,[10] empower the NCA to require firms suspected of ML/TF to provide information relating to their operations and strategies without necessarily making the statutory SARs. The requirement makes it possible for the NCA to conduct investigations/gather intelligence from institutions perceived as being high risk at the earliest opportunity rather than waiting for the submission of SARs. The change in conditions is in response to the elevated risks posed by ML/TF in the era of cryptoassets. The analysis is integral in tracing assets (including cryptoassets), enforcement of confiscation orders, and identification of current and potential risk exposures.

Despite its structural and institutional capabilities, the UK has imposed limitations on the extent to which the FIUs can perform strategic and operational analyses of the data from organisations until such entities provide the SARs. The policy decision presents a challenge in initiative-taking AML/CFT in the era of cryptoassets and causes UKFIUs to miss the chance to search for and analyse information on suspicious activities that can be used for preventative purposes.

7.2.5 Promoting Corporate Integrity and Transparency

Both countries have adopted new legislation to enhance transparency of business operations and promote anti-corruptive measures. The UK leads in the promotion of corporate transparency[11] due to its broad appreciation of ML/TF risks posed by legal and natural persons. Through its legal frameworks, all FIs and DNFBPs are mandated to perform CDD, from which they obtain and maintain information on all beneficial owners of cryptoassets within its jurisdiction. The beneficial ownership information on complex financial arrangements such as trust is available to competent authorities that understand the structures of the assets and how they are stored and transferred.

[9] See FATF-MENA n(9)
[10] The changes to legislation come into force on or before 25th Nov 2022
[11] Keating and others n(4)

The information on beneficial ownership is available freely and on-demand through a central registry, which implies that any individual interested in making informed decisions on cryptoassets in the UK can do so using reliable and comprehensive information. Although the accuracy of the information is not verifiable, its reliability is guaranteed since it is sourced from institutions with robust oversight and management structures.

7.2.6 Promoting Effective Implementation of Proliferation-related Activities

The UK has taken measures to support the designation of terrorists at the regional (EU) and global (UN) levels through the promotion of effective implementation of the targeted financial sanction[12] regime. The TFS regime is deployed through the freezing of funds and assets in the process of pursuing the proliferation of ML/TF activities. The UK's TFS regime features several effective tools, including the establishment of an institutional framework under the Office of Financial Sanctions Implementation.[13]

In Bahrain, there are weaknesses in the CFT regime due to the exemptions under the terrorism offences law from which CTF guidelines are derived. The exemptions have a marked influence on the extent to which public and private establishments comply with the technical requirements under the FATF ML/TF guidelines. However, these concerns are validated mostly due to the application of the RBA in the determination of its effectiveness. LEAs have fulfilled their mandate to identify and investigate TF activities, most of which originate from terrorism investigations. LEAs have robust domestic coordination for the exchange of information and intelligence in TF cases.

7.2.7 Emergent Threats since the 2018 MER

Several post-evaluation efforts are included to highlight the measures in place to prevent the two countries from entering complacency in the post-evaluation period.[14] Structural innovations include increased political support for the establishment of the OPBAS, increased human, technical, and financial resources for the NECC, and improved LEAs' capacity to participate in the

[12] Hereinafter 'TFS'.
[13] OFSI hereafter. See FSA, "Anti-Money Laundering, Counter Financing of Terrorism, and Counter-Proliferation Financing" Current Status and Challenges' (2022),<https://www.fsa.go.jp/en/news/2022/20221007/20221007.pdf > accessed 29 December 2022
[14] Keating and others n(4)

AML/CFT regime.[15] The follow-up report[16] focuses primarily on the technical compliance ratings in 2022.[17]

First, the FUR provided an analysis of the progress made by the UK in addressing the deficiencies in technical compliance that were identified in the 2018 MER, specifically in relation to R13 (Correspondent banking) and R29 (FIUs). In the 2018 MER, the UK was rated 'PC' since it excluded the economies under the European Economic Area from the mechanisms for applying only EDD measures. The decision was based on the view that countries within the EU region have robust ML/TF systems, as opposed to countries outside the EU region, which were classified as 'third countries'. By 2022, the UK has deployed the mandatory EDD measures to all countries, leading to a rating of 'C' under Recommendation 13. Under Recommendation 29, the UK received a PC rating on account of the limited operational independence of UKFIU due to the lack of sufficient resources.

Between 2018 and 2022, the UK has improved the capacity to perform an operational assessment of its programs for reforming the SARs, by expanding its human resources capacity from 81 to 141. The changes also include improvements in IT capabilities for expanding the functions of UKFIU, including the acquisition of five additional strategic analysis teams, which has led to the capability to produce strategic analytical reports. However, these changes are insufficient in two ways. One, the increase in human resources falls short of the FATF recommendations for a minimum of 200 professionals.[18] This is commensurate to the growth in the financial sector, as well as risk exposures as evidenced by an increase in the SARs to over 270,000.

Furthermore, the transition to fully automated IT systems is yet to be achieved. These two weaknesses have limited the ability of UKFIUs to perform complex strategic analysis, such as bulk data search and processing capabilities that are required for the creation of SARs. The UKFIU is yet to interface its systems with the National Data Exploitation Capability[19] to facilitate the additional analysis of SARs and the development of new analytical products for the FinTech

[15] Ibid
[16] Hereinafter 'FUR'.
[17] Keating and others n(4)
[18] FATF, 'Financial Action Task Force: The United Kingdom of Great Britain and North Ireland' (2007), <https://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20UK%20FULL.pdf>Accessed November 25, 2022.
[19] Hereinafter 'NDEC'.

sector. While the improvements are noted, it is apparent that they are not commensurate with earlier requirements and the most recent changes in the operating environment; hence, the rating remained unchanged as 'PC'.

Secondly, the FUR provides the implementation progress and ratings where necessary, as well as commensurate recommendations under any new requirements introduced by the FATF since the previous MER. These changes are characteristic of the organic and dynamic nature of the FATF recommendations regime, which is adjusted in response to novel risks and exposures to ML/TF. The FUR relates specifically to two recommendations.

The FATF amended Recommendation 2 in October 2018 to mandate all countries to establish mechanisms for cooperating and coordinating the activities of data protection and privacy rules of the authorities involved in ML/TF. The recommendation also mandated the establishment of a mechanism for domestic institutions to share information. In response, the UK has elevated the extent to which its domestic AML/CFT actions and priorities are influenced by the appreciation of risks at all levels of government.[20] Based on the assessment, the UK was found to have met the new requirements; hence, the 'Compliant' rating was retained.

Under Recommendation 5, the FATF revised the requirements for New Technologies, specifically the obligations that countries have concerning VAs and VASPs. The UK was rated as LC in 2018 due to the lack of a legally binding requirement for financial institutions to perform a risk assessment for all new products and services as well as the fulfilment channels in the financial sector. Based on the assessment, the UK was thus mandated to fulfil most of the following requirements concerning cryptoassets: (i) Identify, assess and understand the ML/TF risks related to VAs activities and VASPs' operations,[21] (ii) Ensure that all VASPs are registered and licensed, (iii), apply sufficient supervisory and monitoring to achieve risk-based AML/CFT, including developing mechanisms for sanctioning through a competent authority and (iv), ensure sufficient preventive measures are conceptualised for VASPs, including instituting measures for international cooperation.

[20] FATF 'Anti-money laundering and counter-terrorist financing measures – United Kingdom 1st Regular Follow-up Report' (FATF 2022) http://www.fatf-gafi.org/publications/mutualevaluations/documents/fur-united-kingdom-2022.html > Accessed 25 November 2022

[21] See HM Treasury, 'Consultation on the Fifth Money Laundering Directive: Response To The Consultation' (2020) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/860491/5MLD_Consultation_Response.pdf >accessed 20 November 2022

Since 2019, the UK has met the revised requirements under Recommendation 15, with the primary focus of 'New Technologies' being the cryptoassets used within the jurisdictions.[22] The risk assessment activities culminated in the recognition of exposures from challenges in identifying the legal and natural persons that conduct VASP activities and operations in the country. In response, both legal and natural persons involved in VASP activities are registered under the FCA, with licensing maintained subject to periodic assessment and mitigation. Firms managing cryptoassets are subjected to supervision for compliance with a catalogue of requirements under the new set of AML/CFT obligations.[23] Other measures include protocols for cooperating with other countries on the supervision of VASPs or in case of legal matters. While the preventative measures targeting VASPs are comprehensive, VASPs are still treated as other regulated persons despite the diversity of how they can/ participate in the cryptoassets industry. Since the UK does not apply the Travel Rule[24] for virtual assets, the extent to which it can comprehensively assess the risks associated with custodial wallet service providers is limited. Based on the FUR, the UK has only managed to assess the risks associated with exchange activities that have high-risk exposures but have not placed safeguards for all activities linked to virtual assets. These measures culminated in the conclusion that the UK's ML/TF supervision cannot be outrightly termed as being risk-based.

7.3 Benchmarking UK and Bahrain

Both countries have undertaken some long-overdue remedial actions,[25] most of which were proposed under the previous MERs. Similarly, they have undertaken limited measures to account for the wider global acceptance of cryptocurrencies, which is a risk characteristic from the AML/CFT perspective. Alternative mediums such as blockchain facilitate the successful laundering of criminal funds, which can be generated and used without ever leaving the ecosystem until the integration phase ends. The utility of the RBA for AML/CFT in both countries is to facilitate the identification of causal trends. This leads to pinpointing the different vectors through which emergent technologies propagate ML/TF, thereby allowing the regulatory authorities to

[22] The actions include the identification and assessment of ML/TF risks linked to companies providing wallet and exchange services for cryptoassets

[23] In recognition of the possibility of risks that are not accommodated in the prevailing mandates, the UK has instituted a diversity of dissuasive and proportionate sanctions that apply to those who are licensed, those awaiting licensing, and those who have not sought licensing.

[24] See G Velkes, 'International Anti-Money Laundering Regulation of Virtual Currencies and Assets' (2020) 52 Int Law and Politics, 3, 8769.

[25] For instance, the establishment of the OPBAS in the UK.

focus on and assess the specific vulnerabilities. Overall, the clarity gained from the assessment offers industry stakeholders the ability to map how pre-emptive and initiative-taking efforts for preventing ML/TF can be deployed while making the RBA more efficient for the intended purpose. The analysis will focus on areas where one country outperforms the other based on the level of technical compliance under the Recommendations.

7.3.1 Lessons for the UK from Bahrain

The focus is directed towards the areas of effectiveness measures where the country faces purely technical deficiencies as well as areas where there is merit for attention by the policy and lawmakers.

7.3.1.1 Improve the Response by LEAs

A review of the AML/CFT Action Plan in the UK reveals a concerted effort to develop the capabilities of the law enforcement response to emergent and extant threats rather than the identification of potential risk exposures.[26] The weakness arises from the operating model of the UKFIUs, where LEAs play a limited role, which entails relying on data from past events to prevent ML/TF activities. The approach is ineffective in the face of emergent TF risks under the new financing models, as discussed in Chapter 2, as well as the threats from cryptoassets. Bahrain has avoided this problem by implementing a police-type FIU, which has secondary powers in investigating crimes.

7.3.1.2 Match Theory with Practice

Questions have been raised about the existence of gaps between the assessed effectiveness based on the proposed methodologies and the reality on the ground. The UK is ranked top in terms of effectiveness and technical compliance under FATF MERs. However, there are incidences of high-level ML incidences, thereby raising questions on the reliability of the assessment, as well as the propensity of the UK to implement its AML/CFT measures for 'passing the FATF test' rather than achieving real-life AML/CFT goals.[27] While Bahrain under-performs the UK in effectiveness and technical compliance, there is a close link between the assessed risks and outcomes.

[26] See Home Office/HM Treasury, 'Action plan for anti-money laundering and counter-terrorist finance. London: Home Office' (2016). https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/517992/6-2118-Action_Plan_for_Anti-Money_Laundering__web_.pdf >. Accessed 30 November 2022

[27] Keating and others n(4)

7.3.1.3 Improve the Contribution of LEAs to Financial Intelligence

The oversight and regulatory regime in the UK are reliant on spatial association in its risk-based analysis of ML/TF risks. The approach draws heavily on the conclusion from RBA on SOCs, which involve threats that are commonly managed through traditional policing operations. However, the spatial approach is evident from the broad AML/CFT regulations, whereby entities in the regulated sector from the EU are automatically classified as being at a 'low risk' compared to those from other locations. The approach represents a vulnerability from an AML/CFT risk, especially since there are differences in the regulatory and supervisory efficacy among EU organisations. To counter this threat, Bahrain applies a standard risk-assessment model for all regulated entities, hence limiting the possibility of regulatory capture.[28]

7.3.2 Lessons for Bahrain from the UK

7.3.2.1 Enhance the Assessment of Risk Exposures in Line with The RBA

The utility of the RBA under AML/CFT is determined by the extent to which it has been applied in the development of preventative approaches. In its AML/CFT regime, Bahrain's cryptoassets regulation relies extensively on the existing regulatory frameworks and institutions that were initially designed for contemporary financial institutions. Currently, the CBB Rulebook, Vol 1 to 7, offers guidelines for institutions involved in the cryptoassets sector. While the specific framework for Cryptoassets is contained in Vol 6, it is apparent that most of the provisions and the underlying principles are derived from the regulatory concerns for other assets and forms of money that predate Cryptoassets. This approach is also evident from the UK's approach, which, according to the 2018 MER, is a minor deficiency that potentiates lower-risk situations, most of which originate from businesses and clients located within the EU.[29] The challenge with this approach is the apparent limitations in the scope with which the regulatory mandate can achieve effectiveness against the extensive and emergent ML/TF risks associated with cryptoassets. Evidence of some of the complex risks includes the use of crypto dusting,[30] which is an automated process that mimics layering in traditional ML.

---

[28] S Hagan, 'Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT)-Report on the Review of the Effectiveness of the Program', (2011) <https://www.imf.org/external/np/pp/eng/2011/051111.pdf > Accessed 11 December 2022

[29] FATF n(8)

[30] E A Akartuna, S D Johnson and A E Thornton, 'The money laundering and terrorist financing risks of new and disruptive technologies: a futures-oriented scoping review', (2022)1 Security Journal

7.3.2.2 Remove Exclusions for Terrorism Offenses

The proposition is integral in ensuring that regulators are no longer encumbered by legacy frameworks that are not aligned with the emergent ML/TF threats and risk exposures. Bahrain should remove the exclusions for terrorism offences, specifically, those which outline that participation in certain transactions does not amount to aiding, abetting, or facilitating terrorist acts.[31] Through explicit exemptions and specific references in Bahrain law, the definition of terrorism offences is not aligned with the provisions under Article 6 of the TF Conventions.[32] While measures to address these exclusions are included in Articles 43 and 44 of the Penal Code, there are no specific penalties for corporate entities engaged in auxiliary terrorism offences. Similarly, there is no indication of the presence of policies in practice to ensure that the liability for such offences is transposed to the natural persons involved in the management of the organisation, as is the norm in other locations.

7.3.2.3 Change AML/CFT Guidelines for Legal Persons and Natural Persons

The propositions hereunder are partly derived from the successes and contributions of the OPBAS, which has introduced new legal and natural persons into the reporting and oversight remit, thereby solving a perennial weak spot in its AML/CFT.[33]

Bahrain has a framework that is indicative of similar perceptions towards the potential risks of delays in taking the necessary measures against proliferation and terrorism financing.[34] However, the provisions under the framework do not apply to all legal and natural persons in the country since some DNFBPs.[35] Natural persons have also been identified as key influences in the vulnerabilities and threats within the financial sector. After all, in the era of the 'new model' and 'cheap terrorism', it is apparent that it is not just the businesses in the regulated sectors that are at risk of ML/TF. Vulnerabilities for 'cash in' or 'cash out' in the unregulated sector or by natural

[31] See Article 2.2 (a)-(d) of Decree No. 4 of 2001.
[32] The Convention refers to the 'Convention of the Organisation of the Islamic Conference on Combating International Terrorism'. The exemption under Decree No 54 (2006) and Decree No. 58 (2006), whereby "peoples struggle, including armed struggle against foreign occupation, aggression, colonialism, and hegemony, aimed at liberation and self-determination in accordance with the principles of international law" are justifiable since they are considered part of the political, ethnic, racial, ideological, philosophical and religious activities of the Bahraini citizens.
[33] Under OPBAS, the supervision of non-financial regulated bodies is facilitated, at least in part, by professional bodies that are charge of establishes best practices for member institutions, while also raising operating standards at the institutional level., T Keating and others, n(4)
[34] IN line with UNSCR 1267 and 1988 UN Committee
[35] These include lawyers, real estate agents and brokers, and notaries.

persons can set off a chain of events that magnify ML/TF risks in ways that do not trigger the necessary interventions.

Bahrain should amend Art. 2 of MO 173,[36] which requires all legal and natural persons to freeze the funds or assets of designated entities or persons promptly and without prior notification to the targeted individual. There are gaps in the regulatory framework that is established to monitor and control TF risks associated with non-profit organisations.[37] In recognition of the opportunities for TF under the 'new model' terrorism, whereby terror groups adopt novel structures and utilise a diversity of financing portfolios that feature both financial and non-financial resources.[38] The gaps entail the absence of an RBA orientation in the measures to ensure compliance,[39] with weaknesses in the extent to which the NPOs in the country perform educational programs to inform about TF risk exposures and outreach to ensure proactivity in the management of risks.

7.3.2.4 Establish Domestic Taskforces

The UK relies on a diversity of task forces comprised of professionals from different disciplines in the financial and technology sector to design regulatory and oversight frameworks.[40] By relying on inputs from diverse perspectives, the task forces have provided recommendations that have so far worked beyond expectations. The advantages of using task forces include the objectivity of their activities and their ability to rely on a combination of conventional and unconventional methodologies in completing their tasks. Similarly, taskforces are fit-for-purpose entities formed with specific timelines and particular goals based on the problem at hand.[41] The singularity of focus contributes to their ability to provide results cost-effectively and efficiently while focusing

[36] Under the TFS guidelines provided by MOICT 2014
[37] NPOs hereafter. N Ryder, *The Financial War on Terrorism: A Review of Counter-Terrorist Financing Strategies Since 2001* (Routledge,, 2015).
[38] T Keatinge, and F Keen, 'Social Media and Terrorist Financing: What are the Vulnerabilities and How Could Public and Private Sectors Collaborate Better?' (2019) < https://rusi.org/sites/default/files/20190802_grntt_paper_10.pdf >Accessed 20 December 2022
[39] Based on a review of its NPOs in 2016, 95 were found to be a high risk of TF (with 55 having active TF risks due to high reserve amounts at hand, overseas transactions, and engagement in illicit fundraising and fund management practices), 106 were assessed to have a moderate risk, while 417 were assigned the low-risk status. 8.1a, c 8.2 8.4
[40] FSA, "Anti-Money Laundering, Counter Financing of Terrorism, and Counter-Proliferation Financing" Current Status and Challenges' (2022) <https://www.fsa.go.jp/en/news/2022/20221007/20221007.pdf > Accessed 29 December 2022
[41] T Keating and others, n(4)

on a particular set of challenges and then delivering custom solutions. Some of the key task forces in the UK that can be used as motifs for Bahrain include the JMLIT.[42]

7.3.2.5 Improve CDD Guidelines

The UK has recently introduced guidelines on the application of CDD and Enhanced EDD. While Bahrain has also introduced similar guidelines, there are several apparent gaps from the risk-based perspective. First, all regulated financial institutions should harmonise the factors that determine risk for customers and then specify the criteria for determining the categories of customers that should be subjected to Enhanced CDD.

Similarly, the Bahraini regulatory regime should enhance its confiscation and seizure regime, especially when customers fail to comply with the requirements for CDD. Currently, the provisions under the CBB Rulebook lack certainty in how to treat the assets of originators who fail to comply with the CDD requirements.[43] This lack of regulatory certainty contributes to a lack of consistency since the FI These provisions offer alternatives that do not address the reality of ML/TF risks, allowing for financial institutions to choose the best option based on their interests rather than utilising a standard approach. Second, there is a need to change the CDD and Enhanced CDD procedures to ensure that all reporting institutions do not tip off persons seeking to engage in ML/TF. FIs are allowed to pursue CDD in a manner that can tip off individuals, thereby compromising the possibility of LEA to target serious and organised crimes.

7.3.2.6 Focus on Politically Exposed Persons **(PEP)**

The ML/TF risks linked to PEPs are complicated by the role of political commitment to the process. In the UK, both domestic and foreign PEPs are perceived as high-risk individuals on account of their position of influence and their access to resources that can be tasked for ML/TF purposes. The measures are applied to relatives and close associates, who have in the past been used as strawmen for PEPs who are willingly or unwittingly used to facilitate illegal activities.

---

[42] N J Maxwell, 'Expanding the Capability of Financial Information-Sharing Partnerships' (2019),< https://www.futureis.com/uploads/3/7/9/4/3794525/pr%C3%A9cis_of_ffis_paperexpanding_the_role_of_fisps_-_march_2019.pdf > Accessed 6 December 2022

[43] The provisions include FC-1.1.11 (whereby the FI can freeze any funds and then file an STR with the FID), FC-1.1.12 (which gives the FI the option to terminate the relationship with the customer) or FC-1.1.13 (the FI can return the funds to the counterparty in the same method as received). The outcomes under options under FC-1.1.12 and FC-1.1.13, which are perceived as alternatives to FC-1.1.11, have significantly different implications from the AML/CFT perspective.

Bahrain should adopt a similar approach and then broaden it to all transactions involving financial resources and assets rather than limiting the regulatory scope to insurance-related transactions.[44]

7.3.2.7 Improve STRs (Suspicious Transaction Reporting)

The UK changed its SARs regime to capture details about organisations that tried to engage in ML/TF activities, as well as the types of businesses, their locations, and whether the attempt to launder was genuine or not. The new SARs regime facilitates the management of risks and vulnerabilities, in addition to serving the traditional role of identification and categorisation.[45]

Under Bahrain legal principles, some instances of criminal intent or unsuccessful attempts at committing crimes are not recognised as 'crimes' punishable under law, and no further actions are recommended. While this serves to limit the possibility of instituting investigative proceedings against persons who unwittingly contravened the laws and regulations, it also offers potential criminals and terrorists the opportunity to adjust their ML/TF approaches to avoid detections. While all FIs are mandated to report suspicious transactions related to ML[46] and TF,[47] only banking institutions have been provided with specific reporting guidelines under the CBB Rulebook.[48]

The imposition of RBA contributes to self-regulation. To achieve optimal orientation towards the RBA, both the UK and Bahrain rely on regulators drawn from the industries to be regulated. Such a decision is based on the goal of ensuring that regulators have technical acuity in identifying suspicious transactions, as well as keeping in stride with the changes in industry trends. However, such a strategy presents the potential danger of the lack of ascendancy while also propagating regulatory capture. Ascendancy compromises superiority and hence limits the power of the regulatory, with market leaders and key market players contributing to the challenges facing regulatory institutions. The most common outcome is the 'mis-spelling' of cases, whereby despite direct regulatory interventions and measures to name and shame perpetrators, those very entities

[44] See CBB Rulebook, *Enhanced Customer Due Diligence: Politically Exposed Persons ('PEPs'), Vol 6-Capital Markets*, (CBB 2022) <https://cbben.thomsonreuters.com/rulebook/aml-15-enhanced-customer-due-diligence-politically-exposed-persons-peps> Accessed 12 December 2022

[45] Home Office/HM Treasury, *Action plan for anti-money laundering and counter-terrorist finance*. (Home Office (2016)<https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/517992/6-2118-Action_Plan_for_Anti-Money_Laundering__web_.pdf.> accessed 30 November 2022

[46] Article 4 and 5of Decree Law No. 4 (2001).

[47] Amendments to Decree Law No. 54 (2006, under Article 5.

[48] Additional clarifications are provided in the CBB Rulebook Vol 2 (section 5), Section 4 of Vol 3 and 4, Section 5 of Vol 5, and Section 4 of Vol 6. accessed 15 March 2022

deny any misconduct. The goal for benchmarking the UK and Bahrain is to facilitate the disruption of ML activities, starting with timely detection of the threats, followed by commensurate sanctioning of the criminals, and depriving them of access to the illicit proceeds through the seven propositions. Similarly, by detecting and disrupting the plans of those involved in TF to deprive them of the resources and ability to finance terror, then sanction those who are involved directly and indirectly. The propositions are also integral in limiting cases of jurisdictional arbitrage, whereby the comparative AML/CFT weaknesses in one jurisdiction function as a factor that attracts the perpetrators of illegal activities.

7.4 Acceptability of the cryptocurrency exchanges

Tensions in the regulation of cryptocurrency exchange arise from the reality that, while regulated entities must capture the information on originators and beneficiaries,[49] most virtual currencies are designed to be instruments of privacy. The intrinsic measures to limit intermediation in cryptoassets transactions are antithetical to the AML/CFT mechanisms, which are at the core of the financial war against terror. While there are arguments that the concept of transparency is structurally incompatible with the cryptoassets ecosystems, both the UK and Bahrain have found it necessary to insert regulatory mandates to limit the opaqueness, albeit at the 'cash in' and 'cash out' phases. The discussion hereunder reveals how these institutions are regulated and supervised in both locations.

7.4.1 The UK Approach

The UK has adopted a 'watch-and-learn' approach[50] to regulating cryptoassets, with the most comprehensive and decision measures introduced as recently as 2018. The decisions are designed to avoid stifling innovation while also ensuring the safety of the users and the financial systems.[51] The foundationally customer-oriented approach seeks to protect consumers from exploitation by unscrupulous cryptocurrency exchanges while also protecting the domestic financial sector from exploitation for illegal activities on a case-by-case basis. The primary focus of the FCA is to ensure

[49] N Pocher, 'The open legal challenges of pursuing AML/CFT accountability within privacy-enhanced IoM ecosystems', Proceedings of the 3rd Distributed Ledger Technology Workshop (2020)< https://ceur-ws.org/Vol-2580/DLT_2020_paper_2.pdf > accessed 15 March 2022

[50] C Feikert-Ahalt, 'Regulatory Approaches to Cryptoassets in Selected Jurisdictions', (2019), https://tile.loc.gov/storage-services/service/ll/llglrd/2019668148/2019668148.pdf >Accessed 12 December 2012

[51] K Braddick and others 'Cryptoassets Taskforce: Final Report'. (2018). <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf> Accessed 15 March 2022

that cryptocurrency exchange advertisements do not mislead consumers, much like it is for other financial services sector firms.[52]

Through licensing,[53] the UK focuses on regulating cryptocurrency exchanges that are involved in fiat-to-virtual currency exchange to limit the propensity of the firms to exploit the existing AML/CFT guidelines through stringent CDD measures.[54] Possession of the licenses provides the cryptocurrency exchanges with the authority to operate in the UK while also marketing their services and products in line with the guidelines of the FCA. Most of the measures applied to such exchanges are derived from the traditional financial sector regulatory mandates, whereby transparency is perceived as an indicator that the cryptocurrency exchange is willing to abide by the AML/CFT regime. This explains why the UK restricts the licenses for handling certain categories of cryptocurrencies.[55] The mandates for CDD under the licensing and regulatory measures limit the possibility of those exchanges using the convenience of cryptoassets as a way of perpetrating ML/TF activities.[56] Similarly, crypto exchanges that are dedicated to fulfilling the AML/CFT objectives benefit from the increased oversight while also contributing to the maintenance of an effective financial services sector by sharing information as designated and regulated institutions under the FCA.[57]

The UK has also sought to broaden its regulatory mandates to cover the entirety of the VASPs with the emergence of virtual-to-virtual exchanges. The broadening of the regulatory and oversight mandates is necessitated by the realisation that these types of exchanges present novel risk exposures under ML/TF.[58] These risks include the globalised nature of the services provided by the virtual-to-virtual exchanges, whereby the cryptocurrencies used in the transactions exist in the blockchain ecosystem without interacting with the traditional financial systems.[59]

The UK has also recognised the importance of establishing technical standards for all cryptoassets exchanges operating in the country as a way of reinforcing their resilience to cybercrime and

[52] FCA, n(83)
[53] *Ibid*
[54] *Ibid*
[55] Akartuna and others n(33)
[56] CDD contributes to traceability, which is possible for most cryptoassets, including those which are pseudonymous, such as Bitcoin.
[57] Keating and others n(4)
[58] K Braddick, and others n(54)
[59] A case where the perpetrator of illegal activities is involved in mining the cryptoassets, then uses them to fund the illegalities.

exploitation by rogue actors as well as state sponsors of terrorism.[60] The changes are indicative of the scope and scale at which UK regulatory institutions view the virtual assets as viable for ML/TF, which is in line with the RBA. Most of the guidelines are designed to achieve two goals: to protect customers and investors in line with the goals of the FCA and to limit the possibility of the use of the UK financial system to facilitate crimes and other illicit activities.

The extensive utilisation of consultations with industry stakeholders has enabled the UK to adopt a dynamic set of regulatory and oversight standards that are responsive to the emergent ML/TF risks.[61] The approach has led to a tailored approach, which considers the relevant innovations rather than simplified linear extensions of the existing rules. Furthermore, consultations contribute to the increased acceptability of the regulatory and supervisory mandates across the industry.[62]

While the HM Treasury, the HMRC, and the Home Office have outlined their position vis-à-vis cryptocurrency exchanges in the UK, the responsibility for oversight and regulation lies with the FCA and the PRA.[63] At its core, the FCA is designed to protect the interests of customers across the UK. The PRA, which is a quasi-governmental entity, is designed to regulate and supervise banking institutions to ensure that their actions, governance and discipline are reasonable. Under the regulation of the PRA, cryptocurrency exchanges in the UK adhere to three approaches in their operations: a focused approach,[64] a judgement-based approach,[65] and a forward-looking approach.

---

[60] D Nelson, 'Sanctioned Crypto Wallet Linked to North Korean Hackers Keeps Laundering', (2022), <https://www.coindesk.com/tech/2022/04/15/sanctioned-crypto-wallet-linked-to-north-korean-hackers-keeps-on-laundering/ > accessed 15 December 2022

[61] FCA, 'Discussion paper on Distributed Ledge Technology' Discussion Paper DP 17/3, (2017). <https://www.fca.org.uk/publication/discussion/dp17-03.pdf> Accessed 25March, 2022.

[62] The measures are also designed to enable cryptocurrency exchanges operating in the country to get oriented with the regulatory and supervisory mandates, while also contributing to the policy decisions that affect their operations.

[63] HM Government and UK Finance 'Economic Crime Plan 2019-22 (HM Government 2022) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/816215/2019-22_Economic_Crime_Plan.pdf> accessed 23 February 2021

[64] The PRA focuses on the cryptocurrency exchanges that pose the greatest risks to the stability of the UK financial system, as well as the policy makers.

[65] Through the judgment approach, the PRA relies on its judgment to determine if the cryptocurrency exchanges operate in a safe manner, and whether they provide sufficient protections for its customers, as well as meeting the financial threshold conditions.

7.4.2 Bahrain's Approach

Bahrain's approach to the regulation of cryptocurrency exchange is informed by the policies aimed at placing the government at the forefront of novel and innovative industries, such as DLT.[66] Bahrain's approach is fundamentally 'cryptocurrency-exchange-focused', considering that it has established a conducive environment for the establishment of cryptocurrency exchanges under the regulatory sandbox framework.[67] Under the framework, both foreign and domestic cryptocurrency exchanges benefit from the favourable operating environment.[68] The AML/CFT measures under the approach entail ensuring that the cryptocurrency exchanges are 'fit-for-purpose' before entering the market. The conservative approach accounts for the ability of the country to authorise cryptocurrency exchanges to offer over-the-counter (OTC) payments and settlement services through the conversion of fiat-to-crypto assets and crypto-fiat currencies.[69]

In Bahrain, cryptocurrency exchanges are regulated by the CBB, which is an indication of the perception that it is integral to the stability of the domestic financial systems. In line with Legislative Decree 21 of 2001, all exchanges must be registered in the country with an official operating entity.[70] The approach is a methodology that is widespread among most MENA countries, whereby the central banks are directly involved in the AML/CFY issues.[71]

Through CBB guidance, Bahrain has adopted a meritocratic regulatory approach that is more responsive to the quality and quantity of cryptoassets that the exchanges handle, the services that

---

[66] An empirical study by A H Othman, and others, 'The impact of cryptocurrencies market development on banks' deposits variability in the GCC region' (2020) 12 J of Fin Econ Policy 2 162, found that in Bahrain, the emergence of cryptocurrencies had a negative impact on bank deposits..

[67] F Alsebaie, 'GCC: Promoting Blockchain Technology Adoption in the Financial Services Sector: Insights from Bahrain's Experience' (2020) <https://www.iga.gov.bh/Media/Pdf-Section/Share/GCC-Promoting-Blockchain-Technology-Adoption-in-the-Financial-Services-Sector.pdf > Accessed 25 November 2022.

[68] N Alam, and S N Ali, *Fintech, Digital Currency and the Future of Islamic Finance: Strategic, Regulatory and Adoption Issues in the Gulf Cooperation Council* (Switzerland, Springer, 2020), 233, who indicates that domestic cryptocurrency exchanges benefit from reduced start-up costs, as well as access to a platform that eliminates the technological and technical challenges. They are also offered guidance on how to fulfil the regulatory and legislative requirements. See also A Dethe, 'Sandbox Policy Successful, Bahrain Grants Licence to Two FinTechs', (2019) <https://bfsi.economictimes.indiatimes.com/news/fintech/sandbox-policy-successful-bahrain-grants-license-to-2-fintechs/72233931>Accessed 13 December 2022

[69] The Report, 'Capital Markets Overview: Bahrain Bourse-An Oasis of Investment Opportunities (2020) <https://bahrainbourse.com/resources/files/Thought%20Leadership/OBG_05BH20_Capital%20Markets.pdf > accessed 12 December 2022

[70] F Alsebaie 'GCC: Promoting Blockchain Technology Adoption in the Financial Services Sector: Insights from Bahrain's Experience' (2020)< https://www.iga.gov.bh/Media/Pdf-Section/Share/GCC-Promoting-Blockchain-Technology-Adoption-in-the-Financial-Services-Sector.pdf > accessed 19 November 2022

[71] CCAF, 'FinTech Regulation in the Middle East and North Africa', (2021) < https://www.jbs.cam.ac.uk/wp-content/uploads/2022/02/ccaf-2022-02-fintech-regulation-in-mena.pdf > accessed 19 November 2022

it offers, and its country of origin.[72] The approach starts with the establishment of four categories of licenses that each cryptocurrency exchange has to hold before venturing into the market.[73] The combination of regulations under each category of the exchange facilitates the implementation of the RBA, thereby limiting the regulatory and legislative ambiguity in supervising cryptocurrency exchanges.

Bahrain imposes additional mandates for cryptocurrency exchanges designed to mitigate risks of failure and to insulate the customers and investors from unforeseen losses.[74] The measures are necessitated by the decision by the CBB to allow the use of certain cryptoassets for payments and settlements, hence paying the way for cryptocurrency exchanges to work with traditional financial sector institutions.[75] Additional measures related to the management of paid-up capital by ensuring that not more than 50% of the available assets are used as collateral.

Both countries have adopted the risk-based approach, whereby the response to cryptocurrency exchanges is dependent on the probability of adverse events occurring and the potential impact of those adverse events. However, the risk-based approach also considers the scale and scope of the operations of the cryptocurrency exchange. The dynamic risk exposures and the vulnerabilities in the regulatory and supervisory frameworks inform this approach to the RBA. First, as cryptocurrency exchanges gain market share, their influence on the market grows; hence, the association of ML/TF risks increases. Second, larger cryptocurrency exchanges are more attractive investment targets, hence the potential to generate seismic shifts in the market in the short run. Third, large cryptocurrency exchanges are targets for cybercrime, hence the need for commensurate oversight. The comparative analysis herein reveals the challenges linked to the rapidly evolving risk exposures from the virtual economy, as well as the opportunities that have emerged for updating AML/CFT regulations from the experiences of the regulators and cryptocurrency exchanges alike. The analysis herein reveals that the regulatory and legislative actions targeting cryptocurrency exchanges are lacking in the recognition of context-specific

[72] S Reback, 'Binance's Bahrain License Upgraded for More Crypto Services', (2022) <https://www.coindesk.com/business/2022/05/26/binances-bahrain-license-upgraded-for-more-crypto-services/ > Accessed 12 December 2022

[73] CBB Rulebook, *Crypto-Asset Module: Central Bank of Bahrain Rule Book, Vol 6: Capital Markets.* (CBB 2019)

[74] Licensees are required to have a designated business place in the country, and to operate in line with the domestic business practices.

[75] While the approach exposes the country's financial sector to novel ML/TF risks.

technical aspects. On one hand, the AML/CFT obligations under the traditional financial systems are insufficient or unsuitable for the crypto landscape.

On the other hand, those systems targeting traditional risk exposures are integral in laying the foundation for preventing a significant proportion of ML/TF risks. Both countries recognise the integral nature of cryptocurrency exchanges in the crypto-asset ecosystem. While their prominence resembles that of cryptoassets, the exchanges have not generated sufficient concerns from the perspective of financial stability. The primary concern of both countries is to protect consumers, who may face losses during transactions or by investing in these assets. Both countries face challenges in regulating cryptocurrency exchanges due to the complex corporate structures that the exchanges adopt as part of their business models. Some exchanges combine traditional financial services with IT-driven services, which is a novel operating model. As a result, while both countries have achieved different levels of success in monitoring transactions, use and ownership of cryptoassets, it is evident that a huge amount of cryptoassets are laundered through untraceable over-the-counter transactions by professional entities and brokers for the facilitation of crime.

7.5 The Rule in FIU in Bahrain and the UK

FIUs are independent entities that have the legal mandate and resources to serve as centres for receiving and analysing reports on suspicious transactions from reporting agencies,[76] specifically those relating to ML/TF activities. By positioning themselves between the public sector (LEAs) and the private sector (financial institutions), FIUs establish a crucial middle link for the exchange of data, information and intelligence between the public and private sectors as part of the mechanisms for the financial war against terror. They also facilitate the convergence of the efficiency that is characteristic of private-sector entities and public-sector institutions.

The establishment of FIUs in both countries can be traced to the inputs from the FATF, following the 2003 version of the 40 recommendations,[77] specifically under Recommendations 29.[78] To fulfil

[76] Reporting agencies include financial institution, (such as banking and insurance firms, and more recently, VASPs), and DNFBPs, such as accountants, lawyers and casinos.
[77] FATF 'Guidance on Risk-Based Supervision' (FATF, 2021) <www.fatf-gafi.org/publications/documents/Guidance-RBA-Supervision.html> accessed 25 March 2022
[78] Ibid

the mandate, FIUs are designed to have the authority to acquire any necessary additional information from the regulated entities that provide the reports.

The UKFIU, which is an operationally independent entity established under the NCA based on the current state of play, focuses on the transactions and activities of legal and natural persons while monitoring the operations of payment systems across the country.

In Bahrain, the Anti-Money Laundering Unit (AMLU),[79] which is established under the Financial Intelligence Directorate,[80] performs the usual duties of an FIU in the country, with the legal mandates derived from the obligations under DL 4/2001. The AMLU, which is a police-type FIU, performs its own investigative roles based on the information collected from all the reporting entities.[81] In addition, it is responsible for executing ML-related court orders, including soliciting additional information from the reporting entities. However, it lacks the mandate to investigate or obtain information from the public other than what is mandated under the reporting regime. The AMLU has the power to seize and confiscate the assets of suspected criminals, albeit upon acquiring an authorised court order. However, when faced with urgent cases, the AMLU can retain the assets for up to three days on its authority.

7.5.1 Mandates of the FIUs

The roles of FIUs are recognised under FATF.[82] Most jurisdictions have sought to design their FATF in line with these formal roles while also implementing customised reforms in response to domestic risk exposures and threats.[83]

7.5.1.1 Collecting Information on Transactions

FIUs are established to perform financial surveillance for a multiplicity of supervisory and regulatory obligations.[84] Essentially, the surveillance mechanisms are designed to investigate the

[79] Bahrain's AMLU has the vision to achieve excellence in security performance to combat ML, TF and the illegal transfer of funds across borders, as well as achieving regional and international advancement in these outcomes.
[80] FID hereafter
[81] IMF, 'Kingdom of Bahrain: Detailed Assessment on Anti-Money Laundering and Combating the Financing of Terrorism',(IMF 2007)< https://www.imf.org/external/pubs/ft/scr/2007/cr07134.pdf > accessed 29 December 2022
[82] Interpretive Note to FATF Recommendation 29 A.1, which states that FIUs are "… part of, and plays a central role in, a country's AML/CFT operational network, and provides support to the work of other competent authorities".
[83] NCA 'UK Financial Intelligence Unit: Suspicious Activity Reports-Annual Report 2020' (NCA 2020). < https://www.nationalcrimeagency.gov.uk/who-we-are/publications/480-sars-annual-report-2020/file > Accessed 15 December 2022
[84] P Lagerwaard, 'Financial surveillance and the role of the Financial Intelligence Unit (FIU) in the Netherlands' (2022) 26 J of ML Control,

'chain of financial security' by identifying the series of actors who are involved in every financial transaction.[85] The surveillance mechanisms are cognisant of the reality that the financial transaction information changes as the assets move from one actor to another since it has to be translated to mirror the characteristics and meanings of the particular professional domain. The collection of transaction information is a core function of FIUs in both countries, which it uses to contribute to investigations and prosecutions as and where necessary as part of the financial surveillance system.[86] This role makes FIUs the gatekeepers of financial institutions in the country. The UK has moved from the contemporary compliance-driven SAR regime to a shared-ownership model, which is facilitated under the JMLIT,[87] to expand the perimeter of the regulated sector, reinforce the legal foundations,[88] and accommodate the conflicting policy goals under obligations for data privacy and financial intelligence.[89]

The information collected by the FIUs contains supporting elements, including the originator and beneficiary, as well as other objective and subjective indicators, to put the information into context. The approach to reporting has led to the yielding of data sets that contain valuable threats and data on vulnerabilities, thus increasing its utility for AML/CFT purposes. To ensure quality SARs, FIUs in both countries have outlined the reporting formats for what constitutes a high-quality SAR.[90] SARs enable FIUs to fulfil two key functions: first, to stop criminal actions and arrest the perpetrators; second, the contents of the SARs provide the FIU with useful intelligence that facilitates the formulation of strategies.

Bahrain's AMLU receives reports and notifications on suspicious financial transactions from regulated industries to combat ML/TF and the illicit transfer of money across borders. Its functions include the receipt and processing of disclosures on ML/TF-related crimes, as well as information on predicate offences such as the narcotics trade.[91] However, in Bahrain, the AMLU performs two unique roles relating to the collection of information that is not part of the UKFIU's mandate. First,

[85] These actors include legal and natural persons, banking institutions that facilitate payment.
[86] Based on Locard's exchange principle, when applied to forensic financial analysis, every transaction leaves a trace.
[87] Keating and others n(4)
[88] The establishment of the Criminal Finances Act of 2017, as well as the primary gateway for sharing information under the JMLIT under Section 7 of the UK Crime and Courts Act of 2013.
[89] Under FISP model.
[90] SARs under the UKFIU are managed and processed by the SAR administration and control team.
[91] IMF, n(84)

the receipt and processing of disclosures of suspected terrorist acts. The responsibility differs from what UKFIU participates in due to the differences in the countries.

Similarly, the difference in the composition of DNFBPs in the two countries accounts for a significant disparity in their role in collecting information. Similarly, the assignment of the responsibility to supervise the DNFBPs to the Ministry of Industry and Commerce[92] limits the effectiveness of the AML/CFT regime. The supervisory scope of the MOIC revolves around the provisions of the Commercial Companies Law, which relates to general management, rather than oversight of AML/CFT obligations.[93]

While the two countries engage in the collection of information, UKFIUs deal with SARs, while the AMLU manages STRs. The difference in the type of information contained therein arises since SARs cover 'activities', which is a broader range of data points than the 'transactions' that the AMLU targets. The difference originates from the operating models as well as the fundamental goals of the FIUs. While UKFIU focuses on a broad range of illegal activities that include the achievement of the AML/CFT obligations, the AMLU is dedicated to ML risks and other illegalities that are linked to the financial services sector.

7.5.1.2 Cooperating with Domestic and Foreign Entities

The strategic landscape of both the UKFIU and AMLU features goals of cooperation with domestic entities in its AML/CFT action plans. Cooperation is integral in ensuring that all elements of financial intelligence from the SARs are understood within the context of the industry-specific risk exposures from the ML/TF perspective. The UKFIU has undertaken measures to reinforce its cooperation with other domestic entities to achieve force multiplication in the prevention and disruption of organised crime and ML/TF activities.[94] The enhancements to the reporting regime have made it possible for the HMRC to identify ways through which it can achieve tax recovery goals based on the information on hidden overseas incomes and undeclared assets in the SAR. Bahrain's AMLU, which is a police-type FIU, performs the combined roles of a generic FIU and an LEA. As a result, after analysing the information from STRs, the findings are forwarded to the

[92] MOIC hereafter
[93] CCL hereafter.
[94] UKFIU works with the UK National Central Office for the Suppression of Counterfeit Currency (UKNCO). See also NCA, 'SARs Regime Good Practice: Frequently Asked Questions-Suspicious Activity Reports', (2020), < https://www.nationalcrimeagency.gov.uk/who-we-are/publications/462-sars-faq-july-2020/file > Accessed 15 December 2022

Public Prosecutors Office,which performs further investigations and subsequent prosecution of the perpetrators. The close link between the AMLU and PPO ensures the legality of the FIU's actions by offering legal guidance as needed. Its cooperation with the Ministry of Social Development[95] facilitates corporate governance standards for vulnerable institutions that are outside the financial services sector. AMLU has an articulate mechanism for cooperating with entities such as MOIC, the Bahrain Monetary Agency,[96] and the Office of Public Prosecutor.[97] The separation of responsibilities among these institutions arises from the prominence of confidentiality in the fulfilment of their legal and customary mandates. The siloed approach has, however, not limited the frequent and systematic cooperation between LEAs and FIUs for operational and strategic purposes.

The two FIUs have also expanded their operating mandates across domestic borders. UKFIUs have also asserted their right to cooperate at a supranational level by cooperating with foreign counterparts under the Egmont Group of FIUs.[98] The establishment seeks to achieve optimal efficiency in the sharing of intelligence among jurisdictions, considering that a significant proportion of suspicious transactions involve foreign entities.

Under the Egmont group, FIUs have achieved significant success through interactions and cooperation in sharing information. Both countries attribute their success to the establishment of hybrid FIUs, which fit into at least two of the following three FIU models.[99] For FIUs created under the judicial model, the process of disclosing suspicious transactions and financial activities involves the agencies involved in investigations from the financial sector to enable the judiciary to take the necessary measures.[100] For those FIUs using the law enforcement model, the AML/CFT measures are implemented alongside the existing LEAs.[101] Under the administrative model, FIUs are centralised administrative entities with unique responsibilities designed to receive and process

[95] MSD hereafter.
[96] BMA hereafter.
[97] OPP hereafter.
[98] HM Treasury, n(72)
[99] K Stroligo, C-H Hsu, and T Kouts, 'Financial Intelligence Units Working with Law Enforcement Authorities and Prosecutors', (World Bank, 2018),< https://star.worldbank.org/sites/default/files/fius-report-04-sk1.pdf > Accessed 3 December 2022
[100] See S D Jayasekara, Administrative model of financial intelligence units: an analysis of effectiveness of the AML/CFT regime", (2022) 25 J of Money Laundering Control, 3, 514.
[101] M Brewczynska, 'Financial Intelligence Units: Reflections on the applicable data protection legal framework', (2021) 43 Computer Law & Security Review, 1, 1.

information from the financial sector. The FIUs function as a buffer by transmitting their findings to the judiciary or LEAs for subsequent actions. International cooperation occurs through one or more of the following channels, with the choice of the FIU depending on the technical capacity, geographic location, and legal framework.[102]

The AMLU is responsible for executing foreign assistance requests,[103] which are designed in an unrestricted manner for all ML/TF cases. The primary challenge for international cooperation for the AMLU is the ability to accommodate the often diametrically opposite understanding of what ML/TF is from some GCC countries, especially where institutions are classified as terrorist organisations. The FID has gone a step further in facilitating international cooperation by aiding countries seeking to join the Egmont Group, offering professional training, and facilitating the transfer of information.

7.5.1.3 Establishing Disclosure Procedures

Both FIUs have glossary codes, with most of the recent changes informed by changes in the environment. The glossary codes are part of the good practice standards and enable other associated institutions to analyse data more effectively and rapidly, thereby identifying trends in ML/TF. The codes, which facilitate the classification of transaction categories, also facilitate the identification of high-risk cases in line with the RBA and facilitate a timely response.[104] In 2020, the UKFIU proposed new codes to target the criminal exposures associated with the COVID-19 pandemic, thereby enabling LEAs and reporters to distil the information on suspicious activities more effectively and rapidly.[105]

In recognition of the potential risks associated with the 'crime-terror' nexus, both FIUs focus on collecting different forms of information from regulated institutions.[106] The FIUs act as intermediaries for intelligence collection between LEAs and private sector entities, thereby

[102] First, the FIU.NET, which is a platform designed for EU member states only. Second, under the Egmont Secure Web (ESW) which serves as an information-sharing link national FIUs. The platform is an FIU-to-FIU communication channel, which facilitates the exchange of information. Finally, there are other custom channels that facilitate the secure exchange of information between FIUs do not hold membership under the Egmont Group and are outside the EU.
[103] The AMLU has been involved in 18 outgoing requests and 36 incoming requests for information from foreign strategic partners. Under the FID, the AMLU performs additional duties under international cooperation.
[104] The codes facilitate rapid exchange of information as and when necessary. HM Treasury, n(72)
[105] UKFIU, 'Suspicious Activity Report (SAR) Glossary Codes and Reporting Routes', (2022), <– Government Priority Schemes, and XXCVDXX – General code.
[106] P Lagerwaard, n(87)

facilitating the disclosure process through an intricate reporting framework.[107] Through the mandatory disclosures, UKFIU achieves the evidential obligations and goals from both the regulated and unregulated sectors, which are integral to achieving the outcomes under the RBA. Similarly, UKFIU can engage in evidential requests, including clarifications relating to authorised or mandatory disclosures.

However, the UKFIU, under the consent regime, has introduced a novel approach under authorised disclosures,[108] which can either be under the Defence Against Money Laundering[109] or Defence Against Terror Financing.[110] Under the 'Authorised Disclosures' regime, the UKFIU facilitates the receipt of information from private individuals who are not under any regulatory framework other than being interested in preventing ML/TF and other criminal activities from occurring. There has been an expansion of the DAML/DATF since 2014, showing the extent to which the push forward for this reform under whistleblowing generates actionable intelligence.[111] In addition to transaction reports, the UKFIU also receives and investigates reports on the breach of confidentiality under the SAR regime, which is a measure to protect the integrity of the financial surveillance program.

An increase in the number of SARs has triggered a response from the UKFIU, whereby, in conjunction with the OPBAS, new reporting guidance has been developed. The changes are designed to achieve 'quality over quantity' for reporting outcomes through the introduction of

[107] M Hopkins and N Shelton, 'Identifying Money Laundering Risk in the United Kingdom: Observations from National Risk Assessments and a Proposed Alternative Methodology', (2019) 25 Eur J Crim Policy Res, 63.

[108] Regulated/ mandatory disclosures are presented as required by law and policy and occurs when a reporter suspects that another person is engaged in ML/TF. Failure to make such a disclosure automatically leads to criminal liability to the individual. For authorized disclosures, the reporter takes measures to report suspected activities that, based on how/her professional opinion and capacity, appear to be criminal, to protect themselves from potential criminal liability while making a voluntary disclosure, in line with Part 7 of POCA 2002. From the authorized disclosures, the UKFIU can initiate investigation, and two, the reporter can insulate themselves against liability.

[109] DAML hereafter. DAML is regulated by Section 327 -329 of POCA. These refers to authorised disclosures whereby the suspicious transactions relate to ML Formerly known as Consent SARs, DAML relates to defence of offenders under the Proceeds of Crime Act 2002. Under the 2018 Reform Programme, the UKFIU has introduced a review of the DAML regime and provides guidelines to enhance the effectiveness of the consent regime, by improving how well the reporters understand their obligations and responsibilities.

[110] DATF hereafter, which is regulated under Section 21ZA of TACT 2000. These are authorized disclosures by UKFIU to denote that the disclosure in reference relates to TF activities. DATF relates to offenses under Terrorism Act 2000

[111] NCA, 'Requesting a defence from the NCA under POCA and TACT UK Financial Intelligence Unit' (2018), <https://service.betterregulation.com/sites/default/files/upload/2018-05/Requesting%20A%20Defence%20Under%20POCA%20TACT%20-%20v4%200.pdf > Accessed 15 December 2022

initiative-taking reporting guidelines designed to minimise the propensity of firms to engage in defensive reporting.

7.5.1.4 Analysis of Trends

The FIUs are responsible for the detection of financial (ML/TF, fraud, corruption, misuse of virtual assets, drug-related activities) and non-financial crimes. Due to the increase in the number of transactions, driven by the growth in the reporting entities, the type of items being transacted, as well as the customers (domestic, regional and global), it has become apparent that most reporting entities are faced with large volumes of hard-to-manage data, which is qualitative (unstructured), and quantitative (structured). Through proper analytics strategies and techniques, financial services and regulatory institutions can acquire the specific insights that facilitate decision-making in accordance with the goals at the sector level. The analysis of trends enables FIUs to identify the changes in the threat levels for ML/TF and other proliferation threats and then use those insights to reframe their strategies and operations.

In the UK, SARs are integral intelligence resources in tackling ML/TF, as well as serious organised crimes, fraud and corruption. The analysis of trends, which is performed by the intelligence team,[112] serves three purposes under AML/CFT interventions, including the initiation of new/enhancement of existing operations or investigations, revealing new targets based on the density of reports on particular subjects or organisations, provide predictive abilities such as a geographical picture for potential terrorist or criminal activities.[113] The analysis of trends focuses on the identification of the cross-cutting threat enablers,[114] which play a role in the resurgence of the use of contemporary tools for current ML/TF activities.[115]

The 2021 12-month report captures the industry metrics sourced from blockchain analytics companies for all peer-to-peer[116] transactions involving cryptoassets. Since such transactions do

[112] The analysis is performed through strategic, operational and tactical analysis, based on the type of criminal techniques, trends and typologies to increase the value of information extracted from the SARs.
[113] Keating and others n(4)
[114] L Owens, 'National strategic assessment of serious and organised crime 2018,' (NCA, 2018). <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/173-national-strategic-assessment-of-serious-and-organised-crime-2018/file> accessed 20 November 20220
[115] FATF 'Opportunities and Challenges of New Technologies for AML/CFT' (FATF 2021)< https://www.fatf-gafi.org/publications/fatfrecommendations/documents/opportunities-challenges-new-technologies-aml-cft.htm > Accessed 23 December 2022
[116] P2P hereafter. P2P transactions of virtual assets occur between individuals, without necessarily involving a VASP or cryptocurrency exchange.

not involve entities that are under regulatory oversight, most of the AML/CFT measures in place are not captured. The originator is unable to perform the necessary risk-based approaches before finalising the transactions.

The metrics reveal that a substantial proportion of the transactions involving certain cryptoassets occur on a P2P basis. Based on the metrics, the P2P transactions exceed those by VASPs based on the direct transaction value. However, there are variations in the data, which make it challenging for unanimity on the size of the P2P cryptoassets sector, as well as the ML/TF risks that can be attributed to this sector.

The efficacy of financial surveillance is dependent on the ability and propensity of the FIUs to achieve optimal engagement with the reporting entities and to analyse the reports from the regulated sectors.[117] The analysis of trends is designed to identify good practices, create typologies of the suspicious activities that are targeted, and red flag any transactions of concern for further review.[118] The after-action reports from such analysis culminate in the design of interventions, including the use of seminars, case studies and flag-it-up campaigns.

Through its access to a wide range of databases from the private and public sectors, the AMLU utilises its high-level security systems to circulate information securely and confidentially.[119] Based on the analysis, it is apparent that Bahrain is a target for the layering phase of ML.[120] In response, Bahrain's AMLU has had to adjust its AML/CFT strategies to deal with scenarios where investigations involve tracing the assets back to the perpetrators.

FIUs in both countries are designed to provide insights into which parameters of the supervisory, regulatory and enforcement regimes should be adjusted to contain the current and potential threats. For instance, Bahrain's AMLU has the power to request additional information, over and above what is legally mandated, from the entities in the regulated industries to facilitate investigations,

---

[117] K Stroligo, C-H Hsu and T Kouts, 'Financial Intelligence Units Working with Law Enforcement Authorities and Prosecutors' (2018) <https://star.worldbank.org/sites/default/files/fius-report-04-sk1.pdf. > Accessed 3 December 2022

[118] In 2016, the UKFIU performed a forward work plan, which culminates in the identification of high-risk areas, such as professional enablers, corruption, property market deals, charity sectors, legal and accountancy sectors, and trade-based ML.

[119] K Humaidan, and Y Al Sharaf, 'Bahrain FinTech Ecosystem Report 2022', (2022). <https://theblockchaintest.com/uploads/resources/Bahrain%20FinTech%20bay%20%20FinTech%20Ecosystem%20Report%20-%202022%20Feb.pdf> accessed 15 December 2022

[120] Due to the large network for financial sector companies, with extensive foreign branches and subsidiaries.

as well as for operational and strategic analysis. Based on the analysis, the AMLU provides strategic analysis reports that inform the measures against ML/TF and the illegal transfer of funds across borders. However, Bahrain's AMLU lacks the high-profile status with all reporting entities, especially DNFBPs. Under the AML/CFT framework, these DNFBPs are mandated to first submit their STRs to their primary supervising entity, which in most cases has a closer oversight relationship compared to the AMLU. The approach limits the ability of the FIU to promptly intervene in certain forms of risks from this category of regulated entities.

7.5.2 The Operating Models

The operating model adopted by the FIU influences how its activities are organised, as well as the kind of relationships it exploits in achieving the goals under the four mandates stated above. The UKFIU relies primarily on the distributed model for analysing SARs, whereby each of the LEAs has a responsibility to analyse the reports included in the SARs database.[121] The distributed model ensures prompt response to time-critical intelligence by the responsible LEA. However, with the increase in the number of SARs, as well as the increased complexity of the contents,[122] most LEAs are not equipped to fully exploit the contents of the SARs in response to emergent threats. In response to the challenges under the distributed model and the changes in the SARs regime, the UK has adopted the Target Operating Model (TOM), which is an outcome-oriented model that is more responsive to the type of intelligence gathered while assimilating the strategic goals of the UKFIU.[123]

7.5.3 The impact of Pre-Existing Legal Institutional Framework

Legal and institutional frameworks originate from decades of development and calibration of public policy, as well as the application of case law. Eventually, policy options and legal options that impose harsh measures tend to be less acceptable. The pre-existing legal context is of integral

[121] UKFIU, 'Suspicious Activity Report (SAR) Glossary Codes and Reporting Routes' (UKFIU 2022), <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/597-sar-glossary-codes-and-reporting-routes-june-2022/file> accessed 5 December 2022

[122] Due to the emergence of cross-jurisdictional ML/TF schemes

[123] NCA, 'UK Financial Intelligence Unit: Suspicious Activity Reports-Annual Report 2020', (NCA, 2020). < https://www.nationalcrimeagency.gov.uk/who-we-are/publications/480-sars-annual-report-2020/file >accessed 2 December 2022 which states that the model makes the UKFIU a more intelligent, engaged and strategically focused institution.

importance in the determination of the actual enforcement mechanisms utilised by FIUs in the two countries.

The FIUs are responsible for developing solutions for non-compliance.[124] In line with the regulatory frameworks under the traditional financial systems, UKFIU functions as an administrative body that identifies the SARs that warrant further action and then forwards them to the LEAs.[125] In Bahrain, the FIU performs unique functions compared to the UKFIU, including investigating the STRs through access to information from regulated entities. The AMLU executes court orders against individuals suspected of ML activities and, where necessary, self-authorises them to investigate urgent cases.[126]

In summary, FIUs in both countries perform generic functions, with peculiarities in the procedures through which the mandates are fulfilled. The procedural peculiarities are attributed to the operating models, as well as the risk exposures and vulnerabilities relevant to the environment. Through these three roles, FIUs in both countries play a vital role as a buffer for LEAs by filtering out potentially illegal financial transactions, thereby easing the investigative activities among the LEAs.

7.5.4 Propositions for Improvements

In response to emergent ML/TF risks under the crypto economy, the following propositions are made for both the UKFIU and AMLU.[127] First, the templates for capturing and reporting transactions should be adjusted to accommodate the novel transaction details and customer information that is explicitly associated with cryptoassets transactions. The novel details that are specific to cryptoassets include login details such as IP addresses, transaction details such as hash information for both the originator and recipient transactions, mobile device details, and wallet account information.[128]

---

[124] While non-compliance is the primary focus of FIUs, it has become apparent that semi-compliance presents similar risks.

[125] F Mouzakiti, Cooperation between Financial Intelligence Units in the European Union: Stuck in the middle between the General Data Protection Regulation and the Police Data Protection Directive (2020) 11.New J of Euro Criminal Law, 3, 351.

[126] IMF, n(84)

[127] While the AMLU is rated as compliant under the 2018 MER, several changes have occurred that necessitate a review of the risk-exposures and vulnerabilities.

[128] Details such as wallet account information as part of the novel information that FIUs must capture with reference to cryptoasset transactions.

Second, FIUs in both countries have also recognised the need to acquire additional information and knowledge on how cryptoasset transactions operate on virtual platforms.[129] The staff members are required to have extensive knowledge of the nature of transactions and operations, such as the techniques for anonymising transactions, as well as how VAs are utilised to fulfil the goals of criminals and terrorists.

7.5.5 Challenges Facing FIUs

First, a cross-section of stakeholders has recognised the potential for a reduction in the quality of disclosures by the reporting entities. The two-pronged challenge arises when, in the process of enhancing their enforcement mandates, LEAs cast the net wide, thereby increasing the amount of raw data and intelligence that they receive. While the increased volume of SARs is not a guarantee of the quality of financial intelligence, it compromises the efficiency and effectiveness of the FIUs from a cost and resources perspective.[130] However, any measures to reduce the volume of SARs limit the utility of the oversight function of the FIUs.

Second, the FIUs in both countries face the perils of having to rely on self-reported statistics. While UKFIU is perceived as a global trendsetter, there is limited evidence to assess the effectiveness of its operations due to a lack of independent review of the quality of disclosures by the reporting entities.[131]

Third, FIUs in both countries lack the requisite quality and quantity of human, financial and technical resources to perform their functions, which limits the extent to which SARs are exploited for intelligence.[132] UKFIU, which relies on the devolved analysis operating model,[133] has a total of 80 employees, thus making it challenging to perform its functions fully.[134] The UKFIU has also

[129] Akartuna, and others n(33)
[130] See F Mouzakiti, 'Cooperation between Financial Intelligence Units in the European Union: Stuck in the middle between the General Data Protection Regulation and the Police Data Protection Directive' (2020) 11 New J of Euro Criminal Law, 3, 361.
[131] See Law Commission, 'Anti-Money Laundering: The SAR Regime', (Law Commission, 2019) <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2019/06/6.5569_LC_Anti-Money-Laundering_Report_FINAL_WEB_120619.pdf.> accessed 19 December 2022
[132] The limitations in resources makes it challenging for LEAs to practice the often touted approach whereby they integrate the information in SARs from other financial intelligence sources.
[133] Keating and others n(4)
[134] FATF GAFI, 'Financial Action Task Force: The United Kingdom of Great Britain and North Ireland', (FATF, 2007) https://www.fatf- gafi.org/media/fatf/documents/reports/mer/MER%20UK%20FULL.pdf >accessed 19 November 2022

inherited several pitfalls from the LEAs involved in its operations.[135] The challenge limits the ability of the UKFIU to perform deep-dive analyses on the strategic, operational, and tactical issues identified in the SARs that are in line with the national control strategy.[136]

Fourth, in designing the regulatory frameworks, FIUs in both countries are faced with the challenge of appreciating the relevant metrics for determining the economic significance of cryptocurrencies. These metrics are integral in framing the legal basis for the regulatory mandates, as well as justifying the commensurate interventions in the achievement of AML/CFT obligations.

Fifth, FIUs in both countries face challenges in determining whether and how to draw the line between intelligence-relevance reporting and defensive reporting. Furthermore, in line with the RBA, SARs do not have clear-cut thresholds[137] since regulated firms, as well as regulators, must adjust to prevailing conditions. For instance, UKFIU has received an increasing number of SARs from year to year since 2011, with a 70% increase in volume over that period. Between 2019 and 2020, a total of 573,085 SARs were received, representing a 20% increase from the previous year.[138] Such an increase is unsustainable from the perspective of resources. In the absence of such clarity, defensive reporting from regulated institutions culminates in over-reporting[139] or under-reporting.[140]

Sixth, the limited methodological approaches utilised by the FIUs are specifically due to overreliance on reactive strategies rather than implementing initiative-taking measures, such as SAR data mining in conjunction with LEAs involved in the oversight of organised crime units in various regions. The response of the FIUs towards SARs by produced regulated institutions is informed by the suspicion-based model of denunciation.[141] While suspicion is central to the practices of the FIUs, there are no standards for how it is operationalised in different locations and

[135] Hopkins and N Shelton, n(11) who indicates that the LEAs in the UK are underfunded, which limits the ability to implement the SOC Strategy of 2018. Keating and others n(4)
[136] L Owens, n(118) which is based on the threats identified from an assessment of the key crime and terror threats in the UK.
[137] The establishment of stringent thresholds transforms the approach to a rule-based system, which both countries have transitioned out of.
[138] See HM Treasury n(72)
[139] Over-reporting, which leads to the creation of more noise than the actionable intelligence for law enforcement entities.
[140] Under-reporting occurs when the regulated institutions provide SARs only when they lack alternatives to avoid sanctions.
[141] The model is derived from the provisions under Section 327 to 329 of POCA 2002.

times. The absence of specificity as to what differentiates a 'well-founded' suspicion from an 'unqualified' suspicion leads to the introduction of a *de facto* margin of interpretation.

Seventh, FIUs in both countries are focused on regulating ML purposes (in addition to TF purposes under UKFIU) without a more intricate framework to govern all the activities performed on the exchange platforms. Regulatory input only occurs when the market participants cross the line into regulated financial activities.

Eighth, there is extensive documentation of the involvement of professionals, such as lawyers, in the facilitation of ML.[142] The UK established the OPBAS to establish mechanisms through which professional responsibility can be translated into AML/CFT mandates. While the obligations to report suspicious activities and transactions through regulated and authorised disclosures are articulated, Recommendation 23 of FATF provides that certain legal professionals are not mandated to report suspicious transactions if such a report would contravene guidelines on attorney-client privilege.

Ninth, in the recent past, FIUs have focused on identifying ways to ensure that SARs meet the 'quality over quantity' criteria, which limits the potential to identify the highly complex ML/TF schemes designed to beat the existing countermeasures.[143] The approach is attributed to limitations in human and capital resources when processing all the SARs. The objective further arises from the reality that the roles of the FIUs are primarily operational, with the focus on identifying actions that entail the abuse of the financial systems for criminal goals. The lack of strategic mandates under the SARs regime implies that most of the AML/CFT responses based on the actions of FIUs lack a key determinant of effectiveness.

Finally, FIUs in both countries appear to lack set-ups and strategies for the highly elusive techniques that can be deployed for ML/TF purposes.[144] For instance, the use of chargeback fraud, whereby illicit funds are transferred through a payment processor or cryptocurrency exchange, and then the requested refund is treated as clean money, offers opportunities for criminals. A different,

---

[142] FSA, 'Anti-Money Laundering Supervision by the Legal and Accountancy Professional Body Supervisors: Progress and Themes from Our 2020/21 Supervisory Assessments' (2021). < https://www.fca.org.uk/publication/opbas/supervisory-assessments-progress-themes-2020-21.pdf > accessed 27 November 2022

[143] For instance, crypto dusting, as identified by Akartuna, and others n(33)

[144] P Bains, and others, 'Regulating the Crypto Ecosystem: The Case of Unbacked Cryptoassets' (IMF 2022) < https://www.imf.org/en/Publications/fintech-notes/Issues/2022/09/26/Regulating-the-Crypto-Ecosystem-The-Case-of-Unbacked-Crypto-Assets-523715> accessed 16 December 2022

referred to as transaction laundering,[145] whereby criminals transfer cryptocurrency assets from one exchange to another so they can fundraise from the fees accrued from the services provided.

7.6 The FINTECH: Bahrain vs UK

FinTech companies combine technology with innovative business models to enable, improve and disrupt financial services. They leverage technological innovations to create new capabilities and expand existing capabilities to discover, distribute, operate, and service financial products and services. The convenience-enhancing automation to improve the delivery and use of financial services unintentionally reduces the capacity of oversight institutions to conduct effective identification checks on new customers and every transaction.

UK's FinTech sector has developed across three key eras.[146] In the current era, FinTech 3.0 is a non-linear phase that is defined by the entities that participate in the industry rather than the products and services that are delivered. These changes, which include the harmonisation of products and services at a global scale, represent a challenge for regulatory institutions and service providers alike.[147] The current era features a multiplicity of strict regulatory compulsions that became necessary under FinTech 2.0. The rapid expansion of the UK's FinTech sector is attributable to the advanced FinTech ecosystem. The FinTech ecosystem is comprised of the FIs, consumers, regulatory institutions, learning institutions, start-ups and investors.[148] Bahrain's FinTech sector[149] is currently changing on an upward trajectory, driven by the introduction of open banking and increased demand for a better customer experience.

7.6.1 Structure of the FinTech Sectors

Based on the analysis, it is apparent that there are differences in the main FinTech vertical in the country, with personal financial management being the primary vertical in the UK, while payments, transfers and remittances make up the bulk of the verticals in Bahrain. UK's FinTech

[145] Akartuna, and others n(33)
[146] D W Arner, J N Barberis and R P Buckley, 'The Evolution of Fintech: A New Post-Crisis Paradigm?' (2015) https://core.ac.uk/download/pdf/38088713.pdf> accessed November 29, 2022.
[147] Y Hyoeun, 'The UK's Fintech Industry Support Policies and its Implications' (2017) 7 World EconomyBrief, 5, 1.
[148] A Sung, and others. 'An exploratory study of the FinTech (Financial Technology) education and retraining in UK' (2019) 11 J of Work-Applied Management, 2, 187.
[149] R Aburaya, and others, 'FinTech Global Outlook and The Bahraini Landscape: Empirical Exploratory Analysis and Documentary Evidence," 2021 International Conference on Decision Aid Sciences and Application (DASA), 2021 1007-1015

ecosystem is comprised of 23 sub-segments, with over 2500 firms.[150] Recent innovations have led to the emergence of FinTechs that further deepen the interconnections between traditional and advanced technological features through cutting-edge platforms.[151] Bahrain's Fintech sector is comprised of 120 firms, most of which are in the cryptoassets and payments services sector.[152] The disruption caused by the FinTech sector in Bahrain exceeds any other event in the 21st century, as it influences the operational and cost efficiency of the banking sector.[153]

Bahrain's FinTech is best described as an accelerator-oriented collaborative ecosystem[154] on account of the willingness of incumbents to cooperate with newcomer ventures. The propensity to cooperate rather than compete is attributable to the characteristics of the regulatory jurisdiction.

The characteristics of the FinTech sectors in both countries are influenced by the changes in customer expectations of the providers of financial services. Customers perceive technology as a driver of growth, thereby enabling those firms to create solutions that enhance efficiency. Similarly, customers look towards the FinTech sector as a source of solutions to the limitations in the traditional financial services model. While domestic factors are the primary determinants of the FinTech sectors, Both Bahrain's and UK's FinTech are cognizant of the integral nature of international cooperation in delivering additional value under the AML/CFT obligations. International cooperation for FinTechs is organised under the Global Financial Innovation Network.[155] Bahrain's FinTech has entered several regional memoranda of understanding designed to facilitate mutual growth and expansion.

---

[150] Department for International Trade, 'UK FinTech State of the Nation', (2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_ data/file/801277/UK-fintech-state-of-the-nation.pdf > Accessed 12 December 2022; HM Treasury and EY, 'UK FinTech: On the Cutting Edge: An Evaluation of the International FinTech Sector' (HM Treasury, 2016). https://euagenda.eu/upload/publications/untitled-107589-ea.pdf > Accessed 7 December 2022

[151] N Pocher, 'The open legal challenges of pursuing AML/CFT accountability within privacy-enhanced IoM ecosystems', Proceedings of the 3rd Distributed Ledger Technology Workshop (2020)< https://ceur-ws.org/Vol-2580/DLT_2020_paper_2.pdf > accessed 7 December 2022 such as Internet of Money landscape, Internet of Value, decentralised autonomous organisation (DAOs)

[152] K Humaidan, 'Bahrain Fintech Ecosystem Report 2022', (2022) <https://30402333-6bc3-4539-9672-6f0d4f7f6ead.usrfiles.com/ugd/304023_bb24749371464f7986c1b0e08dad5899.pdf > accessed 26 November 2022

[153] Hassan and others. 'Islamic Fintech and Bahrain: An Opportunity for Global Financial Services' in: Hassan, M.K., Rabbani, M.R., Rashid, M. (eds) *FinTech in Islamic Financial Institutions* (Palgrave Macmillan 2022)

[154] J Mueller and M S Piwowar, 'The rise of Fintech in the middle east: An analysis of the emergence of Bahrain and the United Arab Emirates' (2019) <https://milkeninstitute.org/sites/default/files/reports-pdf/FinTech%20in%20the%20Middle%20East-FINAL-121119_0.pdf > accessed 20 December 2022

[155] GFIN hereafter

7.6.2 Drivers of Growth

The drivers of growth of FinTech in both locations can be attributed to the potential for IT-based and digital systems to provide solutions to problems that have plagued the financial services sector.[156] The differences in the drivers of growth are dependent on which applications, methods and technologies are adopted in the particular country, as discussed hereunder.

First, sustained demand from consumers, FIs and corporations.[157] UK's FinTech sector serves customers from across the EU; the growth potential for Bahrain's FinTech sector is marked by the presence of sufficient demand due to a large population of over 450M people in the MENA region, which increases to 3B people when the Africa and Asia are included, most of who do not currently have access to financial services and a total market potential for over US$8Trillion.[158] Most banking institutions in the country have digitised their operations, thereby driving their private and corporate customers to follow suit. Similarly, the growth of the FinTech sector can be attributed to the assertions that these novel forms of money can be perceived as being consistent with Sharia law if they are organised accurately.[159]

Second, access to capital, including strategic, growth and risk capital, facilitates the acquisition of resources and capabilities. UK's FinTech sector has attracted significant interest from investors, leading to an annual increase in funding by 113% between 2014 and 2019.[160] The mature equity[161] and debt capital markets provide access to FinTech ventures regardless of scale and scope of operations. Additional measures, such as tax breaks for qualifying companies, also function as economic incentives for different phases of growth. In Bahrain, investors have shown increased interest in the FinTech sector on account of its potential for delivering returns, as well as an

[156] F Naz, and others, 'Fintech Growth during COVID-19 in MENA Region: Current Challenges and Future prospects' (2024) 24 Electron Commer Res,
[157] KPMG, 'FinTech Focus: UK (2020)'< https://assets.kpmg/content/dam/kpmg/uk/pdf/2020/07/fintech-pulse-report-2020.pdf > accessed 30 November 2022
[158] Mueller and Piwowar n(158)
[159] A Aliyu, et al., 'Review of Some Existing Shariah-Compliant Cryptocurrency', (2020), 6, J of Contemporary Islamic Studies, 1, 5 cites the publication titled 'The Shariah Factor in Cryptocurrencies and Tokens'..
[160] KPMG, n(161), found that there was an increase in the sector funding from £20.1B in 2018 and £38.4B in 2019.
[161] KPMG, 'FinTech: Transforming-Financial Services in the UK', (2019), <https://www.innovatefinance.com/wp-content/uploads/2019/09/kpmg-fintech- transforming-financial-services-in-the-uk.pdf >Accessed 30 November 2022

alternative avenue for diversification of investment portfolios.[162] The most common sources of funding include venture capitalists,[163] angel investors and banking institutions.

Third, availability of talent, with measures to upskill the current workforce and attract and retain the employees.[164] Currently, Bahrain lacks sufficient local talentdue to the absence of people with the requisite skillset to develop and grow the FinTech ecosystem to par with the expectations.[165] The establishment of the National FinTech Talent Program seeks to inculcate the foundations of technical expertise, as well as an entrepreneurial mindset among the Bahraini youths. However, Bahrain faces challenges in the extent to which it can deploy human resources with technical knowledge, skills, and experience to solve any emergent issues promptly and effectively in its FinTech sector.

Finally, regulatory openness promotes competition to create a favourable regulatory environment through FinTech laws. London and the UK are ranked top in terms of FinTech-friendliness due to their ability to support a broad spectrum of businesses at different phases of their lifecycles.[166] In the UK, the Revised Payment Services Directive[167] was introduced to promote a culture of innovation. The UK FinTech sector supplements the contribution of the PSD2 with regulatory technical standards, which feature robust mechanisms for authenticating customers, secure communication standards, and standard reporting mechanisms for all incidents. The regulatory openness is derived from the advanced financial services sector as well as the information technology sector. In Bahrain, government support and regulation mostly occur through the

[162] Mueller and Piwowar n(158) who identifies the Al Waha Fund of Funds, which is a $100M venture capital fund established in the 2018 investment cycle to fund access to Bahrain start-up industry. In the same year, the Global Fintech Fund, a $100M dollar fund available for investment in the US, Europe, Asia and GDD, was availed for Bahrain's FinTech Sector.

[163] While J Mueller and M S Piwowar, 'The rise of Fintech in the middle east: An analysis of the emergence of Bahrain and the United Arab Emirates', (2019) <https://milkeninstitute.org/sites/default/files/reports-pdf/FinTech%20in%20the%20Middle%20East-FINAL-121119_0.pdf > accessed 20 December 2022

[164] K Humaidan, 'Bahrain Fintech Ecosystem Report 2022' < https://30402333-6bc3-4539-9672-6f0d4f7f6ead.usrfiles.com/ugd/304023_bb24749371464f7986c1b0e08dad5899.pdf > accessed 25 November 2022

[165] The challenge is attributed to the inability of learning institutions to respond to the market demands. For instance, while there is an overabundance of finance and management graduates in the country, there are limited qualified and experienced ICT personnel, and an even smaller number have qualifications and experiences in both areas.

[166] KPMG, n(165)

[167] PSD2 hereafter. The PSD2, which is an updated and enhanced version of the PSD that was adopted in 2007, was established in 2016, with EU member states given until 2018 to transpose it to domestic law. See, K Sadowski, 'Impact of PSD2 on The Payment Services Market –General Objectives and Evidence from Polish and UK Legal Systems', (2021), 11, Wroclaw Review of Law, Admin and Eco, 1, 1.

establishment of the Regulatory Sandboxes.[168] The regulatory sandbox is a facilitative regulatory approach whereby regulators work together with the industry participants to achieve similar goals. Other measures include the establishment of a legislative framework for the protection of personal data, as well as the introduction of the open-banking framework.

Ultimately, while most of the dimensions of drivers of growth factors were planned, it is also recognised that the COVID-19 pandemic played a key role in the unplanned expansion of the sector.[169] While there was an increased demand for FinTech services, there are concerns about whether the growth trajectory will change and whether and how it will affect the commensurate ML/TF risks as the sector reorganises itself.

7.6.3 Goals of the FinTech Sector

The goals of the FinTech Sectors in the UK are analogous to those of Bahrain despite the differences in scope and scale. Bahrain's FinTech sector is geared towards becoming a regional hub for cryptocurrencies through a multipronged strategy. First, it has established a regulatory framework for cryptoassets platforms, including measures for the licensure of cryptoassets start-ups and exchanges.[170] Both countries are cognisant of the reality that new technologies do not necessarily eliminate the challenges associated with the old financial systems. Similarly, there is evidence that both countries recognise the weaknesses in the technological solutions to financial sector problems, such as that the information and intelligence generated through algorithmic solutions are not immune to manipulation and interventions by humans.

7.6.4 Regulatory Framework for FinTech

Regulatory institutions in both countries have displayed reluctance to issue final guidance on the interpretation and application of AML/CFT measures before fully understanding novel products

[168] See His Majesty King Hamad bin Isa Al Khalifa, "*Bahrain Economic Vision 2030*," Government of Bahrain, (2019), < https://www.bahrain.bh/wps/wcm/connect/38f53f2f-9ad6-423d-9c96-2dbf17810c94/Vision%2B2030%2BEnglish%2B%28low%2Bresolution%29.pdf?MOD= AJPERES> Accessed Dec 1, 2022.

[169] K Humaidan, 'Bahrain Fintech Ecosystem Report 2022 <https://30402333-6bc3-4539-9672-6f0d4f7f6ead.usrfiles.com/ugd/304023_bb24749371464f7986c1b0e08dad5899.pdf > Accessed November 25, 2022.

[170] R Mogielnicki, 'Bahrain and Abu Dhabi Compete to be Gulf's Cryptocurrency Hub., (The Arab Gulf States Institute in Washington, 2019), https://agsiw.org/bahrain-and-abu-dhabi-compete-to-be-gulfs-cryptocurrency-hub, > accessed 20 December 2022 who identified Rain, MidChains, BitOasis and Arabian Bourse as some of the licensed cryptoasset exchanges.

and services.[171] There are, however, differences in the methodologies of the two countries. In the case of the UK, the FCA has customarily focused on offering cautions and caveats to the customers regarding most of the FinTech products and services on account of novelty, with clear guidance released after analysis of the relevant risks.[172]

While the two countries employ the risk-based approach in the regulation of the FinTech sectors, the methodologies adopted differ significantly. The methodologies are built around ingratiating protections for consumers as well as the traditional financial systems. In Bahrain, the establishment of a regulatory sandbox enables market players to evaluate novel ideas in a controlled virtual platform. Under the framework, cryptocurrencies are adopted in a pragmatic manner that contributes to increased safety for both new and established cryptocurrencies.[173]

In Bahrain, the dominance of regulatory sandboxes enables the regulatory institutions to offer short-term exemptions to enable the technology firms to experiment, albeit with limited legal risk. The application of a one-size-fits-all approach to this pre-regulation mechanism is designed to ensure parity in the promotion of. While the two approaches have similar effects from the risk-based perspective, Bahrain's structured experimentalism, which involves the suspension of regulatory mandates under the test environment, leads to the development of a FinTech sector that excludes the participation of consumers in calibrating the scope of regulatory and oversight interventions for AML/CFT.

Despite the differences in approaches in the two countries, the FinTech regulatory framework revolves around the identification of concealment enhancers, which are techniques and strategies employed by offenders to facilitate further anonymisation of the exchange of cryptoassets for ML/TF purposes.[174] Concealment enhancers are often packaged as part of the DLT and deployed as part of FinTech and new payment methods (NPMs). These strategies highlight the multiplicity of ways through which DLT can be deployed to modernise ML/TF capabilities. Concealment enhancers include minor alterations to the structure of finances across multiple accounts to the

[171] The UK has adopted the framework for 'Compromise Amendments' which involves introduction of stand-in measures for emergent FinTech innovations until they appreciate the ML/TF risks.
[172] Keating and others n(4)
[173] CCAF, 'FinTech Regulation in the Middle East and North Africa' (2021) <https://www.jbs.cam.ac.uk/wp-content/uploads/2022/02/ccaf-2022-02-fintech-regulation-in-mena.pdf> accessed 20 December 2022
[174] Akartuna, and others n(33)

large-scale operational and strategic measures, including the establishment of illegal platforms for exchanging and trading in alternative mediums.[175]

Both countries are faced with the need to assess the risks linked with NPM, starting with determining what types of evidence to look for, the relevance of the risks to ML/TF under the two regimes, and clarity of the crime implications from their use.

In summary, the key difference between FinTech in the UK and Bahrain lies in the stage of evolution that the sector is currently in, vis-à-vis the traditional financial sector. The goals of the FinTech sectors in both countries are analogous in several ways. A review of Bahrain's FinTech ecosystem reveals that its goal is to facilitate cost-effectiveness in the creation of customised, data-intuitive and convenient solutions. Bahrain's FinTech growth is linked to the multistate ecosystem, which features institutions from Bahrain, Singapore and Dubai. Within this ecosystem, which the CBB facilitates, multiple stakeholders, including investors, financial institutions, entrepreneurs and government institutions, can interact.

7.7 Conclusion

The comparative review of the 2018 MERs reveals the areas of weakness in both jurisdictions from the regulatory and supervisory perspective, as well as the identification of the risk typologies and the respective interventions. While there are differences in the performance of both countries from the perspective of effectiveness and technical compliance, the analysis reveals that both the UK and Bahrain display sufficient levels of recognition of the ML/TF and proliferation financing risk exposures where necessary. The emergent risks on account of the developments under the cryptoassets economy have been moderately recognised in the MERs, as well as the FUR for the UK. In the case of Bahrain, its widespread adoption of cryptocurrencies occurred at a time when other jurisdictions had experienced potential vulnerabilities. Its design of AML/CFT is reflective of proactivity and reactivity to those vulnerabilities, with evidence from the utilisation of regulatory sandboxes, as well as an intricate CBB-led campaign to match progress in adoption with acuity in regulatory and supervisory excellence. The input from the 2022 FUR provides insight into the extent to which post-evaluation complacency influences the achievement of

[175] Case in point, the Liberty Reserve, based on Costa Rica, which facilitates the laundering of US$6B. See also, S Farrugia, E Joshua, and G Azzopardi, 'Detection of Illicit Accounts over the Ethereum Blockchain', (2020) 150 Expert Systems with Applications, 113318.

propositions by FATF MERs. While the UK has achieved significant success in its 2018 MER, its commitment to improving effectiveness and technical compliance is not evident from the FUR. While this can be attributed to the slow way AML/CFT obligations are framed and implemented, it also highlights the extent to which a more frequent approach to assessment, including periodic monitoring, is needed for jurisdictions under FATF. This is in response to the changing threat landscape, especially under the cryptoassets economy.

While both jurisdictions have achieved remarkable domestic success, Bahrain can learn several lessons from the UK. The propositions can be attributed to the perspective that the UK has benefited from the market- and industry-specific experiences drawn from the regulation of traditional financial services. These experiences are integral in the AML/CFT obligations in the era of cryptoassets due to the propensity of perpetrators of ML and TF to utilise a combination of traditional and modern tactics when implementing their illegalities. The measures in place have thus played an integral role in preventing the production of a balloon effect, whereby the increased focus on tackling the illicit financial flows in certain sectors (such as the emergent cryptoassets economy) generated vulnerabilities that encourage criminals to exploit the engage in other ML/TF alternatives (such as traditional financing models), which have been overlooked. The propositions for benchmarking Bahrain against the UK should be done in a fit-for-purpose approach by considering the circumstances rather than simply expanding the scope and extending the current rules.

In the implementation of the compliance infrastructure for AML/CFT, the role of FIUs and the FinTech sector has become magnified in both countries. The FIUs, whose primary goal is to perform financial surveillance for the detection and, hence, prevention of ML/TF and PF activities, achieve these goals through four key objectives. The similarity in the roles of FIUs in both countries is attributable to the standardisation achieved under the FATF mandates. However, a few differences emerge from the analysis due to legacy-based practices from the financial intelligence oversight procedures that preceded the current FATF-oriented FIUs. The efficacy of the FIUs emanates from the operating models, as well as the level of technical compliance by the various regulated institutions in the country. Among the ten challenges facing FIUs in both countries, albeit in varying intensities, it is apparent that in the era of FinTech, there is an increase in the quantity and quality of data. In response, FIUs have taken measures to enhance their ability to analyse all

the data effectively and to identify the ML/TF risks that warrant further interventions, including sanctioning, prosecution and seizure of the assets, in line with AML/CFT guidelines.

While the FinTech sector has introduced novel channels for service delivery, such channels have the potential to be repurposed in ways that facilitate novel ML/TF risks while magnifying the complexity of existing risk typologies. These changes are responsible for the transformation in the threat landscape through the introduction of novel channels for products and service delivery. However, the technological component of FinTech has also enabled both countries to adopt better strategies for financial intelligence and surveillance. Both countries have achieved significant growth in the FinTech sector. The risk exposures from this expansion are not necessarily commensurate since a significant portion of the market participants is covered under the pre-existing regulatory and supervisory mandates in the financial and technology sectors. However, both countries must adjust their focus and perspective on account of the dynamic nature of the FinTech sector since crime groups are always known to be head of the regulatory regime curve as they identify novel ways to facilitate ML/TF, whether by exploiting the loopholes in the existing systems.

Chapter VIII: Conclusion

This research sought to address the legislative responses and frameworks in Bahrain and the United Kingdom (UK) to counter-terrorism financing (CTF) involving cryptocurrencies. Thus, the investigation strived to evaluate the effectiveness of international and national regulations in combating cryptocurrency-related terrorism financing (TF), to examine the implementation of the 'Financial War on Terrorism' in both countries and to analyse the strengths and weaknesses of their current CTF legal frameworks. The study also aimed to propose enhancements to these frameworks based on the Financial Action Task Force (FATF) Recommendations to better tackle modern challenges in preventing the misuse of cryptocurrencies for TF and other interconnected financial crimes, such as money laundering (ML).

To this end, this study embarked on a comprehensive examination to dissect and compare the strategic frameworks employed by the UK and Bahrain in addressing the intricate challenges posed by the use of cryptocurrencies for TF. With a keen focus on evaluating the efficacy and relevance of the UK and Bahraini approaches, this research aimed to uncover the legislative responses crafted by both jurisdictions, delving into the international and national regulatory landscapes that govern efforts against the misuse of cryptocurrencies in terror activities.

This final chapter synthesises the main conclusions derived from the analysis of the CTF framework within Bahrain and the UK against the backdrop of the growing challenge posed by cryptocurrencies. Drawing from a nuanced examination of both jurisdictions' financial systems and legislative responses to TF and cryptocurrency use, this chapter outlines a suite of policy recommendations. These proposals are influenced by the individual assessments of each jurisdiction (chapters five and six) and from the comparative analysis of the CTF responses in both Bahrain and the UK (chapter seven), aiming to bolster the effectiveness of CTF efforts in both countries. Finally, the chapter acknowledges the limitations inherent in this research, paving the way for outlining avenues for future research.

8.1.Summary of Main Findings

8.1.1. Evolution of CTF Frameworks

The study revealed that the UK exercises caution in regulating cryptocurrency exchanges, as informed by a regulatory framework introduced in 2018.[1] This framework mandates uniform licensing, reporting and supervisory requirements for all exchanges, aiming to protect innovation, ensure user safety and maintain financial system compliance.[2] This strategy, borrowing from traditional financial sector norms, emphasises transparency as a guiding regulatory value and extends to virtual-to-virtual exchanges to deter misuse of illicit activities. Conversely, Bahrain's regulation of cryptocurrency exchanges is proactive and focused, leveraging a regulatory sandbox to foster the growth of cryptocurrency exchanges. Regulated by the Central Bank of Bahrain (CBB), the approach is tailored to the specific needs of each exchange, including the types of services offered and the origin of the cryptoassets, through a meritocratic system that categorises licenses to streamline supervision.[3] Ultimately, both countries employ a risk-based approach, tailoring their regulatory response to the likelihood and impact of potential risks associated with cryptocurrency exchanges.

With this in mind, the analysis of the UK and Bahrain Mutual Evaluation Reports (MERs) highlights both strengths and weaknesses in both jurisdictions from a regulatory and supervisory standpoint. Despite differences in effectiveness and technical compliance, both countries demonstrate an adequate yet still limited understanding of the risks of TF (including any associated financial crimes, such as ML and proliferation financing) – given the numerous investigative, legislative and regulatory challenges faced by both countries – with the rise of the cryptoassets economy being moderately acknowledged in the MERs and the Follow-Up Report (FUR) for the UK. More specifically, the UK exhibits a sufficient grasp of its existing TF risks under the current circumstances, marked by proactive investigation, prosecution and conviction efforts in alignment

[1] Launch of the Inter-Institutional Taskforce.

[2] HM Treasury, 'Transposition of the Fifth Money Laundering Directive: Consultation', (2019), <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/795670/20190415_Consultation_ontheTransposition_of_5MLD_web.pdf> accessed 13 March 2023 which states the Taskforce was created in response to the growing concerns that the cryptoassets markets had grown to an extent that influenced the state of the economic and financial infrastructure of the UK.

[3] Central Bank of Bahrain and Financial Institutions Law, <https://www.cbb.gov.bh/wp-content/uploads/2018/12/THE_CENTRAL_BANK_OF_BAHRAIN_AND_FINANCIALINSTITUTIONS_LAW_ENGLISH.pdf > accessed 13 March 2023

with the identified risks, significantly bolstered by effective public/private partnerships through the Joint Money Laundering Intelligence Task Force (JMLIT). This contrasts with Bahrain's moderate understanding and evolving risk landscape, where not all TF-related risks are addressed through policy and legislation despite the proactive coordination for operational information sharing. Furthermore, the UK's prioritisation and successful reduction of high-end ML demonstrates the deterrent effect of its robust legal framework and public/private collaboration.

Meanwhile, Bahrain has a developed system for leveraging financial intelligence but sees fewer prosecutions of ML and TF. It also lacks a comprehensive institutional framework for implementing targeted financial sanctions (TFS) against entities involved in TF and proliferation financing. Even more so, the UK's enhanced cooperation strategy and legal provisions empower the National Crime Agency (NCA) to gather intelligence efficiently, while Bahrain relies solely on suspicious transaction reports (STRs) prepared by financial institutions for further investigations.

Notably, Bahrain's proactive and reactive measures to the vulnerabilities exposed by its early adoption of cryptocurrencies are evident through its use of regulatory sandboxes and a comprehensive campaign led by the CBB to ensure that regulatory and supervisory standards keep pace with technological advancements. Conversely, the UK's FUR acknowledges the progress the UK has made in addressing compliance issues. However, it highlights significant gaps in the regulation of virtual assets (VAs) and virtual asset service providers (VASPs), notably the Travel Rule's non-application to VAs, which limits risk assessment capabilities. This underscores the need for continuous improvement in regulatory frameworks and international standards adherence to effectively combat TF challenges in the dynamic financial landscape, particularly in countries with a myriad of transactions and with existing financial risks, such as the UK.

The study also found that the implementation of CFT and related compliance frameworks (i.e. on ML) has significantly underscored the importance of financial intelligence units (FIUs) and the FinTech sector in both jurisdictions. The FIUs in the UK and Bahrain (i.e. UKFIU and AMLU) aim to conduct financial surveillance to detect and prevent TF, ML and proliferation financing (PF) activities, guided by the FATF Recommendations to standardise data collection procedures, to increase domestic and foreign cooperation, to establish disclosure procedures and to analyse ongoing trends in order to track and identify suspicious transactions. This standardisation resulted

in uniform roles for FIUs across different countries, promoting enhanced international cooperation. However, discrepancies arose from local practices inherited from older financial intelligence operations that existed before the adoption of FATF-centric FIUs. Additionally, the effectiveness of FIUs is influenced by their operational frameworks and the degree to which regulated entities adhere to technical standards, further impeding potential investigations and prosecutions.

Notably, the study identified ten common challenges faced by FIUs in both the UK and Bahrain, impacting their effectiveness in combating TF and its associated risks. These common challenges include the concern over the potential decline in disclosure quality from reporting entities, the reliance on self-reported statistics, and the shortage of human, financial and technical resources hampering the comprehensive utilisation of SARs for intelligence purposes. Additionally, it is impossible for FIUs in both jurisdictions to accurately determine the economic impact of cryptocurrencies due to unclear or insufficient metrics while distinguishing between intelligence-relevant and defensive reporting. Even more so, financial authorities seem to rely upon reactive strategies, such as waiting for SARs, instead of engaging in proactive data mining, which limits the effectiveness of preventive measures. At the same time, in both countries, the regulatory focus of FIUs is often too narrow, primarily targeting TF or ML activities without addressing the broader range of exchange platform operations. The focus on regulating only certain aspects of cryptocurrency exchanges leaves gaps in oversight, allowing unregulated activities to flourish until they pose significant risks; thus, a more comprehensive regulatory framework is needed for the early detection and prevention of financial crimes across all exchange activities. Among other investigative challenges, the role of professionals, such as lawyers, in aiding ML activities is well-documented but remains a challenge that the regulators struggle to address in both the UK and Bahrain. At the same time, similarly recent efforts to prioritise the quality of SARs over their quantity may inadvertently overlook complex TF schemes. Lastly, FIUs in both countries lack the means and methods to tackle the sophisticated techniques used in ML/TF activities – due to the lack of novel technologies to support the operation, underscoring the need for improved strategies and resources. Despite facing these common challenges, the one that stands out the most is the advent of FinTech – which has led to an exponential increase in the volume and sophistication of data available. Consequently, FIUs in both the UK and Bahrain have adopted strategies to improve their data analysis capabilities, enabling them to more accurately identify TF and related risks (i.e.

ML) necessitating actions such as sanctions, prosecutions and asset seizures, thereby aligning their operations more closely with CFT and AML regulations.

Thus, a key finding was the realisation that the FinTech sector has ushered in innovative methods for delivering services in both Bahrain and the UK. However, these new channels also introduced novel threats and amplified existing ML/TF risks, complicating the landscape of risk typologies by offering new avenues for product and service delivery. Even so, the technological advancements inherent in FinTech have empowered both countries to enhance their financial intelligence and monitoring strategies. Despite this expansion, the risk exposure does not necessarily increase proportionately, as many market participants already fall under existing regulatory and oversight frameworks within the financial and technology sectors. Nonetheless, the evolving nature of FinTech demands ongoing adaptation in regulatory focus and approach, considering criminal groups often outpace regulatory measures by finding innovative methods to facilitate TF by exploiting the existing loopholes in the regulatory regime existing system loopholes. Fundamentally, while FinTech introduces more complex TF risk profiles, it also provides potent solutions – which, while not tailor-suited to specific contexts such as Bahrain or the UK – can be integrated and adapted within legislative, regulatory and oversight frameworks to strengthen defence and prevention mechanisms against TF activities.

Finally, the study concludes that while both Bahrain and the UK have seen significant domestic achievements, Bahrain stands to gain valuable insights from the UK's approach and vice-versa. Bahrain should consider the UK’s extensive experience in regulating traditional financial markets and services to reform its regulatory approach. Conversely, the UK should strive to enhance its information-sharing and collaborative capacities to facilitate investigations by emulating Bahrain’s integrated approach. Considering the blend of traditional and innovative tactics employed by terrorists, it is crucial to introduce legislative and regulatory updates tailored for the cryptoassets economy while ensuring that a concentrated focus on emerging sectors does not unintentionally create loopholes in financial systems for criminals to exploit. Consequently, each nation must devise a strategy that is customised to its specific circumstances, balancing attention between novel and conventional financial avenues. To this end, the following section provides a comprehensive list of policy recommendations for both Bahrain and the UK.

8.2. Policy Recommendations

As indicated by the findings of this research, the intersection of technology and global finance presents both opportunities and challenges in the fight against TF, necessitating a comprehensive and adaptive approach to regulatory frameworks and enforcement strategies. The following policy recommendations emerge from a detailed analysis of the current landscape of Bahrain and the UK, identifying key areas where the two jurisdictions can enhance their CTF efforts. These recommendations are designed to help policymakers address the nuanced complexities introduced by digital currencies, leveraging technology for greater transparency and efficiency, fostering international and regional collaboration, and enhancing public and private sector partnerships. The overall aim of these suggestions is to fortify defences against the misuse of cryptocurrencies for illicit purposes and, notably, for TF and its associated risks (i.e. ML), ensuring that regulatory bodies are not only reactive but also proactive in anticipating and mitigating potential threats.

This study found that many of the challenges associated with TF and cryptocurrencies stem from the transnational and transjurisdictional nature of digital currencies; this aspect is further enhanced by the lack of regional collaboration. However, as coordinated regulatory efforts and intelligence sharing across regions can help prevent the exploitation of jurisdictional gaps, deterring the efforts of terrorists to use digital currencies across borders, both Bahrain and the UK should be driving forces in developing regional collaboration frameworks, sharing insights and harmonising regulations to address CTF challenges across borders effectively. Related to this is the need to expand the training programs on CTF for financial institutions in both countries, with the focus of these training being the use and misuse of, as well as the challenges and opportunities associated with cryptocurrencies. This is a necessary step in the preventive stage, as educating financial professionals about the specific challenges and risks associated with digital currencies enhances their ability to identify and report suspicious activities, thereby reducing the anonymity that terrorists typically rely on for financing.

Furthermore, the study found that both Bahrain and the UK should pursue innovative regulatory strategies for managing digital currency risks and, most importantly, that the two countries should share insights to support the sector's growth while ensuring security across both jurisdictions. To emphasise, developing regulations that address the unique challenges of digital currencies – such as anonymity and cross-border transactions – can significantly limit their use for illicit purposes,

and Bahrain and the UK could both learn from each other's experiences in managing the risks associated with these assets.

To this end, an important step towards enhancing preparedness in both countries would be the efficient use of the right resources – specifically referring to readily available information that is currently not utilised. For instance, both Bahrain and the UK could invest in the creation of a publicly accessible and constantly updated database of CTF cases involving cryptocurrencies, which would improve transparency among stakeholders, facilitate academic and professional research and help refine CTF strategies. This resource could deter TF by rendering information about past cases and methods publicly available, thus improving understanding and awareness of the tactics used by terrorists among regulators, financial institutions and the public. Therefore, such a database would help identify patterns and techniques used in TF, facilitating the development of more effective CTF prevention and detection strategies and policies based on lessons learned.

To further facilitate information dissemination, the adoption of the OECD's Crypto-Asset Reporting Framework (CARF) and the subsequent development of a centralised Crypto-Asset Reporting Platform (CARP) for reporting suspicious cryptocurrency transactions should also be introduced across both Bahraini and British jurisdictions, leveraging data analytics for automatic detection of TF profiles, facilitating information sharing and enabling rapid mitigation actions between the two countries. This recommendation is based on the fact that such a centralised reporting mechanism would streamline the process of flagging suspicious transactions and would facilitate information sharing between Bahrain and the UK, enhancing the ability of authorities to quickly respond to potential TF/ML activities, thereby deterring the misuse of cryptocurrencies for such purposes.

Another recommendation related to the use and sharing of information in both Bahrain and the UK is the need to launch financial sandboxes for CTF compliance testing within the cryptocurrency sector of both countries, which could enable collaborative experimentation among regulators, FinTech companies and financial institutions, fostering innovation in detecting and preventing TF. By testing new technologies and methodologies in a controlled environment that emulates real-time scenarios without the immediate pressures of regulatory compliance, regulators and financial

institutions can learn to quickly adapt to the evolving landscape of digital currency use in TF, ensuring that future countermeasures are effective and up-to-date.

Additionally, this study also identified unique recommendations for each jurisdiction. On the one hand, Bahrain should bolster its CTF framework by integrating best practices highlighted in the UK's MERs with the FATF, emulating areas of high compliance in the UK and emphasising effective implementation strategies that have been already tested. Adopting international standards and best practices will strengthen the overall framework against TF in Bahrain, address potential issues in advance, and close gaps that could be exploited using cryptocurrencies, thus creating a more formidable barrier to illicit financing activities. To further enhance and centralise collaboration in Bahrain, a Joint Digital Currency Task Force (JDCTF) must be established that is focused on CTF and its associated activities (i.e. AML). More specifically, the purpose of the JDCTF would be to continuously seek out solutions for detecting and addressing cryptocurrency misuse by employing innovative technologies, such as blockchain analytics, machine learning algorithms for transaction monitoring and cross-jurisdictional digital identity verification systems. As such, this specialised task force would be at the forefront of developing and implementing new technologies and strategies for detecting TF, which would help ensure that Bahraini policymakers and investigators are staying ahead of the methods used by terrorists.

Similarly, Bahrain should consider implementing the Joint Money Laundering Intelligence Taskforce (JMLIT) model, which could enhance collaborative financial intelligence sharing between the public and private sectors, mirroring the UK's approach to combating TF threats. By fostering collaboration and intelligence sharing between the financial sector and law enforcement, the JMLIT model allows for quicker responses to emerging threats, which would enhance the early detection of suspicious activities related to cryptocurrencies, effectively halting many TF activities in their incipience. Even more so, Bahrain should tap into FinTech advancements, drawing on the UK's FinTech sector experience and insights to strengthen its CTF measures through tech-based regulatory compliance and monitoring. For instance, leveraging technology can automate the detection of suspicious transactions, significantly reduce human error and substantially increase the scale at which financial transactions are monitored, making it more difficult for terrorists to exploit digital currencies without detection. The final policy recommendation for Bahrain is to expand its public awareness program, learning from the UK’s efforts to raise awareness of the dangers of TF and the potential risks associated with cryptocurrencies, as informing the public

about such risks can lead to increased vigilance and reporting of suspicious activities, acting as a deterrent to potential financiers.

Conversely, the UK could enhance its regulatory efficiency by emulating Bahrain's integrated approach with its Central Bank, public prosecutor's office, and FIU. To emphasise, creating a more cohesive regulatory environment in the UK would enhance the speed and effectiveness of identifying and acting upon suspicious transactions, given that simplified processes across the different stakeholders could enable faster, more coordinated responses to TF activities involving cryptocurrencies. Another suggestion that could improve the UK's CTF efforts would be the adoption of Bahrain's methods for increasing transparency in digital transactions, notably employing blockchain technology for transaction tracking and reporting, which can make it more difficult for terrorists and their supporters to conceal their financial activities. A final recommendation for the UK is to strengthen its CTF initiatives by adopting Bahrain's strategies for international cooperation, particularly in exchanging financial intelligence and best practices with neighbouring countries. Focusing on global CTF collaboration by sharing intelligence and strategies with a broader network of countries would significantly increase the global efforts towards identifying and disrupting international financing networks, thereby both limiting the ability to move funds across borders via cryptocurrencies and also broadening the scope of the UK's international CTF efforts.

8.3. Research Limitations and Recommendations for Further Research

The study has several methodological and practical limitations that may affect its breadth and depth. Firstly, the reliance on the black letter methodology, while thorough in dissecting legal texts, may not capture the nuances of law enforcement and its real-world impacts on deterring TF via cryptocurrencies. Supplementing these findings via those from the socio-legal approach filled this gap to a significant degree. However, this method also could not fully account for the intricate cultural, economic and political influences on the efficacy of CTF measures in distinct jurisdictions, such as in Bahrain and the UK. Furthermore, the dynamic nature of digital currency technology and its rapid evolution poses a significant challenge. As a result, the study's findings could quickly become outdated – however, this is a general risk for both IT and criminal researchers alike, particularly when studying legislation that is already lagging behind the existing

criminal practices. Additionally, access to comprehensive and reliable data on the clandestine use of cryptocurrencies for TF is inherently challenging due to the secretive nature of such transactions and the anonymity digital currencies provide. Lastly, the comparative analysis, while enlightening, may overlook broader regional and international dynamics affecting TF, considering the constantly shifting geopolitical and regulatory landscapes.

In response to these limitations, future research would aim to investigate the evolving legal and regulatory frameworks, with a focus on enforcement practices and their real-world implementation and efficacy, which can provide a more accurate picture of the battle against TF through digital currencies. Exploring the potential of blockchain technology to enhance transparency in digital transactions and its impact on tracking and reporting suspicious activities in the context of CTF could also help uncover the intricacies of this phenomenon. Moreover, a deeper dive into the socio-economic and cultural contexts that influence both the legitimate and illicit uses of cryptocurrencies across various regions could enrich the socio-legal analysis, offering a more rounded understanding of the challenges and opportunities present in each jurisdiction. To this end, future research could also aim to assess the role and impact of public awareness campaigns on the risks of TF through digital currencies, drawing comparisons between Bahrain's and the UK's strategies. A further step to expanding this research into new avenues would be a comparison of Bahrain's CTF efforts to those of other Gulf States, seeking to shed light on regional ideologies and practices based on the region's unique socioeconomic, political and legal landscapes. This comparison can reveal best practices, identify gaps in current strategies, and even foster regional cooperation, thus enhancing the overall effectiveness of CTF measures in a region that faces specific threats and challenges related to TF. Even more so, expanding the comparative analysis to include more jurisdictions with diverse regulatory approaches would also offer a richer landscape of effective strategies against TF, while investigating the impact of adopting best practices from FATF evaluations would also provide clear data on which are the most efficient strategies. To be able to more accurately capture the intricacies and distinctions of the socio-cultural, economic and political factors influencing the efficiency of CTF measures within diverse jurisdictions, primary data from participants should also be gathered. For instance, semi-structured

interviews could help in both assessing known characteristics and testing hypotheses while also allowing for the capture of novel data that was not considered a priori.[4]

Future research could also delve into the impact of publicly accessible databases on improving the transparency and effectiveness of CTF efforts, as this research could assess how these databases influence policy development and academic understanding of TF trends, particularly in the context of digital currencies. Another avenue could explore the outcomes of implementing the Joint Money Laundering Intelligence Taskforce model in Bahrain, focusing on the enhancement of public-private partnerships and its effectiveness in identifying and mitigating TF risks associated with cryptocurrencies. Additionally, keeping pace with technological advancements and the shifting trends in cryptocurrency use is vital for maintaining the relevance and applicability of research findings. Considering the fast-changing landscape of cryptocurrencies and TF, there is also a need to examine how financial technology innovations can bolster CTF measures, drawing insights from the world's leading FinTech sectors to identify technology-driven regulatory compliance and monitoring solutions. Related to this, another potential expansion of the research scope could tackle the effectiveness of expanded CTF training programs, especially considering those that address the challenges and opportunities presented by digital currencies.

Each of these research avenues not only aligns with the policy recommendations provided but also offers a pathway to deepen the understanding of the complexities involved in combating TF in the digital age, highlighting the need for ongoing innovation and collaboration across jurisdictions, among various sectors and stakeholders.

8.4. Final Remarks

Cryptocurrencies and digital assets present unique challenges in the realm of TF due to their decentralised, pseudonymous and often borderless nature. Unlike traditional financial systems, cryptocurrencies can facilitate the swift and semi-anonymous transfer of funds, making it difficult for authorities to trace and intercept illicit transactions. Terrorist organisations often exploit these features to solicit donations and to move funds across jurisdictions or to purchase goods and

[4] Anne Galletta (2013) *Mastering the Semi-Structured Interview and Beyond: From Research Design to Analysis and Publication.* New York: New York University.

services via obscure channels without relying on the conventional banking system – which is subject to rigorous regulations. Additionally, the rise of privacy-focused cryptocurrencies further complicates efforts to monitor and track financial flows associated with terrorism. Thus, the use of cryptocurrencies in TF (as well as for other interconnected criminal activities such as ML) severely undermines global security efforts by providing a financial lifeline that is less detectable and more resilient to intervention. Consequently, regulatory bodies – such as the FATF – emphasise the need for robust CTF measures tailored to the specific challenges posed by cryptocurrencies, as addressing these vulnerabilities is crucial to curtailing the misuse of these currencies for TF, in effect protecting global financial stability.

Bibliography

Statutes

Anti-Terrorism, Crime and Security Act 2001 (ATCSA 2001)

Anti-terrorism, Crime and Security Act 2001, s 4 (2)(a).

Counter-Terrorism Act 2008 (CTA 2008)

Crime and Security Act 2001

Decree Law No. (4) of 2001

Law No. (25) of 2013

Law No. (54) of 2006

Law No. 58 Of 2006 'With Respect to Protection of the Community Against Terrorist Acts'. (2006). Available at http://www.vertic.org/media/National%20Legislation/Bahrain/BH_Law_No_58_Protection_Community_against_Terrorist_Acts.pdf Accessed on January 29, 2021.

Legislative Decree No. (36) of 2017

Legislative Decree No. (4) Of 2001 'With Respect to Prohibiting and Combating Money Laundering and Terrorism Financing'. Available at https://www.mofa.gov.bh/Portals/0/pdf/AntiTerrorist/LEGISLATIVE%20DECRE%E2%80%99S%20NO.%20(4)%20OF%202001%20amended%20by%20law%20(54)%20and%20(25)%20and%20(36).docx%20PDF%201.pdf Accessed on January 29, 2021.

Northern Ireland (Emergency Provisions) Act 1973

Prevention of Terrorism (Temporary Provisions) Act 1974

Proceeds of Crime Act, 2002

Protection of Freedoms Act 2012

Resolution No. 83 of 2020

Statutory Instrument No. 1511, 'Financial Services: The Money Laundering and Terrorist Financing (Amendment) Regulations 2019' 19th Dec, 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/860279/Money_Laundering_and_Terrorist_Financing__Amendment__Regulations_2019.pdf Accessed March 25, 2022.

Statutory Instrument No. 692, 'Financial Services: The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017' 22nd Jun, 2017. https://www.legislation.gov.uk/uksi/2017/692/pdf Accessed March 25, 2022.

Statutory Instruments, 'The Al-Qaida (Asset Freezing) Regulations 2011 (SI 2011/2742), (2011). Available at < https://www.legislation.gov.uk/uksi/2011/2742 >Accessed on January 29,

Statutory Instruments, 'The Civil Procedure Rules 1998-1998-No. 3132. (1998) https://www.legislation.gov.uk/uksi/1998/3132/part/25.2/made/data.pdf.

Terrorism Act of 2000

Terrorism Prevention and Investigations Measure Act 2011

Terrorist Asset Freezing (etc) Act 2010 (TAFA (2010)

The Afghanistan (Asset Freezing) Regulations 2011 (SI 2011/1893)

The Al-Qaida (Asset Freezing) Regulations 2011 (SI 2011/2742)

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

UN General Assembly, *Security Council resolution 2161 (2014) [on threats to international peace and security caused by terrorist acts by Al-Qaida]*, 17 June 2014, S/RES/2161 (2014), Available at < https://www.refworld.org/docid/53aaa1af4.html >Accessed on January 29, 2021

United Nations, 'United Nations Convention Against Transnational Organised Crime and the Protocols Thereto. (2004). Accessed December 20, 2020 https://www.unodc.org/documents/middleeastandnorthafrica/organised-

crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THERETO.pdf

 Law Commission, 'Anti-Money Laundering: The SARS Regime Consultation Paper' (2018) https://www.lawcom.gov.uk/project/anti-money-laundering/ accessed 29 January 2021

 Law No. 58 Of 2006 'With Respect to Protection of the Community Against Terrorist Acts' (2006) http://www.vertic.org/media/National%20Legislation/Bahrain/BH_Law_No_58_Protection_Community_against_Terrorist_Acts.pdf accessed 29 January 2021

 Legislative Decree No. (4) Of 2001 with Respect to Prohibiting and Combating Money Laundering and Terrorism Financing https://www.mofa.gov.bh/Portals/0/pdf/AntiTerrorist/LEGISLATIVE%20DECRE%E2%80%99S%20NO.%20(4)%20OF%202001%20amended%20by%20law%20(54)%20and%20(25)%20and%20(36).docx%20PDF%201.pdf accessed 29 January 2021

UN Resolution

International Convention for the Suppression of the Financing of Terrorism (adopted on 9 December 1999, entered into force on 10 April 2002), 2178 UNTS

UN General Assembly, *Security Council resolution 2161 (2014)*

UN Security Council, *Security Council resolution 2133 (2014)*

UN Security Council, Security Council Resolution 2133 (2014) [on Threats to International Peace and Security Caused by Terrorist Acts], 27 January 2014, S/RES/2133 (2014) https://www.refworld.org/docid/52f104754.html accessed 29 January 2021

UN Security Council, *Security Council resolution 2170 (2014)*

UN Security Council, Security Council Resolution 2170 (2014) [on Threats to International Peace and Security Caused by Terrorist Acts by Al-Qaida], 15 August 2014, S/RES/2170 (2014) https://www.refworld.org/docid/53f729b84.html accessed 29 January 2021

UN Security Council, *Security Council resolution 2199 (2015)*

UN Security Council, Security Council Resolution 2199 (2015) [on Threats to International Peace and Security Caused by Terrorist Acts by Al-Qaida], 12 February 2015, S/RES/2199 (2015) https://www.refworld.org/docid/54ef1f704.html accessed 29 January 2021

UN, International Convention for the Suppression of the Financing of Terrorism (1999) https://treaties.un.org/doc/db/terrorism/english-18-11.pdf accessed 27 January 2021

United Nations General Assembly Resolution (UNGA), 'Measures to Eliminate International Terrorism' UNGA A/RES/51/210, 16 January 1997 https://undocs.org/en/A/RES/51/210 accessed 27 January 2021

United Nations Security Council, 'Resolution 2133 (2014): Prevention of Kidnapping and Hostage-Taking Committed by Terrorist Groups' (2014) https://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/2133%20(2014) accessed 27 January 2021

Case law

United States v. Hammoud, 483 F. App'x 865 (4th Cir. 2012)

R v Yahya Rashid [2016] EWCA Crim 568

Books

Acharya, A. 'Targeting Terrorist Financing: International Cooperation and New Regimes'. (London; New York: Routledge, 2009).

Adams, J. *The Financing of Terror*. (London: New English Library, 1986), pp. 42, 73–75.

Adetunji, J.A. 'Rethinking the internal mechanism of the EGMONT group in financial crime control', (2019). Journal of Money Laundering Control. 22, 2, 327.

Alam N, and Ali S N, 'Fintech, Digital Currency and the Future of Islamic Finance: Strategic, Regulatory and Adoption Issues in the Gulf Cooperation Council', (Switzerland, Springer, 2020), 231.

Ali N T, *Regulatory Counterterrorism: A Critical Appraisal of Proactive Global Governance* (Routledge, 2018).

Andenas, M., and Chiu, I., 'The Foundations and Future of Financial Regulation'. London: Routledge.

Azinge-Egbiri N V, *Regulating and Combating Money Laundering and Terrorist Financing: The Law in Emerging Economies* (Routledge, 2021).

Banakar R and Travers M (eds) *Theory and Method in Socio-Legal Research* (Hart Publishing, 2005).

Barberis J, Arner D W, and Buckley R P, 'The RegTech Book: *The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries in Regulation'*, (John Wiley & Sons, New Jersey, 2019).

Başaranel B U and Türkşen U, *Counter-Terrorist Financing Law and Policy: An Analysis of Turkey* (Routledge, 2019).

Beckett P, *Ownership, Financial Accountability and the Law: Transparency Strategies and the Law: Transparency Strategies and Counter-initiatives* (Routledge, 2019).

Bennett, H. 'Fighting the Mau Mau: The British Army and Counter-Insurgency in the Kenya Emergency'. (Cambridge University Press, 2013).

Boitan I am, and Bartkowiak K*, 'Fostering Innovation and Competitiveness with FinTech, RegTech and SupTech*', (Pennsylvania, IGI Global, 2020).

Boon K E, Huq A and Lovelace D C, *Terrorist Financing and Money-Laundering* (OUP, 2010).

Burke, J. *Al-Qaeda: The True Story of Radical Islam*. (London: I.B. Tauris, 2003), p. 145.

Campbell A M, *Money Laundering, Terrorist Financing, and Tax Evasion: The Consequences of International Policy Initiatives on Financial Centres in the Caribbean Region* (Plagrave Macmillan, 2021).

Chatain P-L, van der Does de Willebois E and Bökkerink M, *Preventing Money Laundering and Terrorist Financing* (2nd edn, World Bank Group, 2022).

Choo, K. R. 'Cryptocurrency and Virtual Currency'. Handbook of Digital Currency. (2015). 283–307. doi:10.1016/b978-0-12-802117-0.00015-

Claire, S. 'The Terror Network: The Secret War of International Terrorism'. (New York: Holt, Rinehart, and Winston, 1981).

Clarke C P, *Terrorism, Inc: The Financing of Terrorism, Insurgency, and Irregular Warfare* (Praeger Security International, 2015).

Cowan D and Wincott D (eds) *Exploring the 'Legal' in Socio-legal Studies* (Palgrave, 2016).

Creutzfeldt N, Mason M and McConnachie K (eds), *Routledge Handbook of Socio-Legal Theory and Methods* (Glasshouse, 2020).

Davis, J. ‘Women in Modern Terrorism: From Liberation Wars to Global Jihad’. (Lanham: Rowman & Littlefield, 2017).

Dawson, M., Kisku, D. R., Gupta, P., Sing, J. K., and Li, W. ‘Developing Next-Generation Countermeasures for Homeland Security Threat Prevention’. (2016). IGI Global.

Dill A, *‘Anti-Money Laundering Regulation and Compliance: Key Problems and Practice Areas’* (Chicago, Edward Elgar Publishing, 2021).

Dion-Schwarz C, David Manheim and Patrick B. Johnston, *Terrorist Use of Cryptocurrencies: Technical and Organisational Barriers and Future Threats* (RAND Corporation, 2019).

D'Souza J, *Terrorist Financing, Money Laundering, and Tax Evasion: Examining the Performance of Financial Intelligence Units* (CRC Press 2012).

El Khoury C, *Countering the Financing of Terrorism: Good Practices to Enhance Effectiveness* (IMF Library, 2023).

English, R. ‘Does Terrorism Work? A History’. (Oxford: Oxford University Press, 2016).

ESMA, *Advice Initial Coin Offerings and Crypto-Assets* (ESMA, 2019)

Esoimeme E E, Deterring and Detecting Money Laundering and Terrorist Financing: A Comparative Analysis of Anti-money Laundering and Counterterrorism Financing Strategies (DSC Publications, 2018).

Essex A, Matuo S, Kulyk O, Gudgeon L, Klages-Mundt A, Perez D, Werner S, Bracciali A and Goodell G (eds) *Financial Cryptography and Data Security: FC 2023 International Workshops* (Springer, 2024).

Feenan D (ed) *Exploring the 'Socio' of Socio-legal Studies* (Palgrave, 2013).

Feinberg, M. ‘Sovereignty in the Age of Global Terrorism: The Role of International Organisations’. (Boston: Brill, 2016).

Freeman M, *Financing Terrorism: Case Studies* (Ashgate, 2012).

Galletta A, *Mastering the Semi-Structured Interview and Beyond: From Research Design to Analysis and Publication* (New York University, 2013).

Girlado J K and Trinkunas H A (eds) *Terrorism Financing and State Responses: A Comparative Perspective* (SUP, 2007).

Goldbarsht D, and Koker L, ‘Financial Technology and the Law: Combatting Financing Crime’, (Sydney: Springer Nature, 2022), 142.

Goldbarsht D, *Global Counter-Terrorist Financing and Soft Law: Multi-Layered Approaches* (Edward Elgar Publishing, 2020).
Gurule, J. 'Unfunding Terror: The Legal Response to the Financing of Global Terrorism'. (Edward Elgar, 2008).
Haines, J. 'Embargoes and Economic Sanctions: Does the Hand Fit the Glove?' (2006). Company Lawyer. 27(10), 289, 290.
Hartley T C, 'International Commercial Litigation: Text, Cases and Materials on Private International Law', (United Kingdom, Cambridge University Press, 2009)
Hassan M K., Jreisat A, Rabbani M R, and Al-Mohamed S. Islamic Fintech and Bahrain: An Opportunity for Global Financial Services (2022). In: Hassan, M.K., Rabbani, M.R., Rashid, M. (eds) FinTech in Islamic Financial Institutions. Palgrave Macmillan, Cham.
Hazard G C and Dondi A, *Legal Ethics: A Comparative Study* (SUP, 2004).
IMF, 'Review of the Fund's Strategy on Anti-Money Laundering and Combating the Financing of Terrorism', (Washington DC, IMF, 2019).
IMF, 'United Kingdom: Financial Sector Assessment Program-Based Core Principles for Effective Banking Supervision-Detailed Assessment Report, (Washington DC IMF, 2016).
Imobersteg Harvey I, *Anti-money Laundering and Counterterrorism Financing Law and Policy* (Brill Nijhoff, 2019).
Jolly D (ed) *Exploring the 'Socio' of Socio-legal Studies* (Palgrave Macmillan, 2013).
Jørgensen N H B *The International Criminal Responsibility of War's Funders and Profiteers* (CUP, 2020).
K Harrison and N Ryder, 'The Law Relating to Financial Crime in the United Kingdom' (2nd Edn, Routledge, 2016) 21.
Kaur G, Lekhi P and Popli S, *Exploring Central Bank Digital Currencies: Concepts, Frameworks, Models, and Challenges* (IGI Global, 2024).
Koh J, *Suppressing Terrorist Financing and Money Laundering* (Springer, 2006).
Krieger T and Meierrieks D, 'Terrorism: causes, effects and the role of money laundering' in Brigitte Unger and Daan van der Linde (eds) *Research Handbook on Money Laundering* (Edward Elgar, 2013).
Kuo Chuen D L (ed) *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data* (Academic Press, 2015).

Kyriakos-Saad N and others, *Islamic Finance and Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT)* (International Monetary Fund, 2016).

Lemma V, 'FinTech Regulation: Exploring New Challenges of the Capital Markets Union', (Springer Nature, 2020).

Levitt, M. 'Hezbollah's Criminal Networks: Useful Idiots, Henchmen, and Organized Criminal Facilitators.' (2016), In Beyond Convergence: World Without Order, edited by H. Matfess University.

Lewis, P.'Guerrillas and Generals: The "Dirty War" in Argentina' (Westport, CT: Praeger,2001), p. 57

Liddick D R, *Transnational Organized Crime and Natural Resources Trafficking: Funding Conflict and Stealing from the World's Most Vulnerable Citizens* (Lexington Books, 2020).

Lord N and others, 'European White-Collar Crime: Exploring the Nature of European Realities', (United Kingdom, Policy Press, 2021).

Madinger J, *Money Laundering: A Guide for Criminal Investigators* (CRC Press, 2012).

Madir J (ed) *Fintech: Law and Regulation* (2nd edn, Elgar Financial Law and Practice, 2021).

Martin, G. 'Understanding Terrorism: Challenges, Perspectives, and Issues'. (Thousand Oaks, CA: Sage Publications, 2016).

May O and Curwell P, *Terrorist Diversion: A Guide to Prevention and Detection for NGOs* (Routledge, 2021).

McCarthy F, Chalmers J, and Bogle S, 'Essays in Conveyancing and Property Law in Honour of Professor Robert Rennie', (United Kingdom, Open Book Publishers, 2015), 103.

McConville M and Chui W H (eds) *Research Methods for Law* (2nd edn, EUP, 2017).

Monateri P G (ed) *Methods of Comparative Law* (Edward Elgar, 2012).

Mousourakis G, *Comparative Law and Legal Traditions: Historical and Contemporary Perspectives* (Springer, 2019).

Mugarura N, *The Global AML Regulatory Landscape in Less Developed Countries*, (Routledge 2016)

Muller W H, Kalin C H and Goldsworth J G (eds) *Anti-Money Laundering: International Law and Practice* (John Wiley, 2007).

Napoleoni L, *Merchants of Men: How Kidnapping, Ransom and Trafficking Fund Terrorism and ISIS* (Atlantic Books, 2018).

Neumann, P. ‘Old and New Style Terrorism’, (1st Edn, Polity Press 2009) [3].

Odeh I A, *Anti-Money Laundering and Combating Terrorist Financing for Financial Institutions* (Dorrance Publishing, 2010).

Parkman T and Peeling G, *Countering Terrorist Finance: A Training Handbook for Financial Services* (Gower Publishing Limited, 2007).

Parkman T, ‘Mastering Anti-Money Laundering and Countering-Terrorist Financing: A Compliance Guide for Practitioners’, (London, Pearson UK, 2020).

Pigman G, *Contemporary Diplomacy* (Polity Press, 2010).

Prabhakar H, *Black Market Billions: How Organised Retail Crime Funds Global Terrorists* (FT Press, 2012).

Rafay A, *Money Laundering and Terrorism Financing in Global Financial Systems* (IGI Global, 2021).

Raymond Choo K K, 'Cryptocurrency and Virtual Currency: Corruption and Money Laundering/Terrorism Financing Risks?' in Kuo Chuen D L (ed) *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data* (Academic Press, 2015).

Rébé N, *Counterterrorism Financing: International Best Practices and the Law* (Brill Nijhoff, 2020).

Rebovich D and Byrne J M (eds) *The New Technology of Financial Crime: New Crime Commission Technology, New Victims, New Offenders, and New Strategies for Prevention and Control* (Routledge, 2023).

Reimann M and Zimmermann R (eds) *The Oxford Handbook of Comparative Law* (2nd edn, OUP, 2019).

Richardson, J. ‘Paradise Poisoned: Learning About Conflict, Terrorism and Development from Sri Lanka's Civil Wars’. (International Center for Ethnic Studies, 2005. p.29)

Ridley N, *Terrorist Financing: The Failure of Counter Measures* (Edward Elgar, 2012).

Romaniuk S N, Kaunert C and Fabe A P H (eds) *Countering Terrorist and Criminal Financing: Theory and Practice* (CRC Press, 2024).

Russo C A, Lastra R M, and Blair W, ‘Research Handbook on Law and Ethics in Banking and Finance’, (Northampton, Edward Elgar Publishing, 2019).

Ryder N *White Collar Crime and Risk: Financial Crime, Corruption and the Financial Crisis* (Palgrave Macmillan, 2018).

Ryder N, *Financial Crime in the 21st Century: Law and Policy (*Edward Elgar Publishing 2011)

Ryder, N. *The Financial War on Terrorism –a Review of Counter-Terrorist Financing Strategies since 2001* (Routledge 2015).

Sackheim M S, and Howell N A, 'The Virtual Currency Regulation Review', 2nd Eds. (London, Law Business Research Ltd., 2019).

Sackheim, M. S., and Howell, N. A., 'The Virtual Currency Regulation Review', 2nd Eds. (2019). London: Law Business Research Ltd.

Samuel G, *An Introduction to Comparative Law Theory and Method* (Hart Publishing 2014).

Scarciglia R, *Methods and Legal Comparison: Challenges for Methodological Pluralism* (Edward Elgar, Publishing 2023).

Schott P A, *Reference Guide to Anti-money Laundering and Combating the Financing of Terrorism* (2nd edn, The World Bank, 2006).

Sidel M, *Regulation of the Voluntary Sector: Freedom and Security in an Era of Uncertainty* (Routledge, 2010).

Siswantoro, D., Handika, R., and Mita, A. F., 'The Requirements of Cryptocurrency for Money, an Islamic View'. (2019). Heliyon. 6. https://doi.org/10.1016/j.heliyon.2020.e03235

Skoczylis J.J. (2015) Is CONTEST Innovative? Counter-Terrorism and Prevent. In: The Local Prevention of Terrorism. Palgrave Macmillan, London. Available at < https://doi.org/10.1057/9781137499011_3 >Accessed on January 29, 2021

Sonderegger, D. 'A regulatory and economic perplexity: bitcoin needs just a bit of regulation'. (2015). Washington University Journal of Law & Policy. 47:175–216.

Sood K and others, *Big Data: A Game Changer for Insurance Companies* (Howard House, 2022).

Stabile Pand Hinkes AM. *Digital assets and blockchain technology: US law and regulation.* (Edward Elgar Publishing; 2020)

Stora, B. *Algeria, 1830–2000: A Short History* (Cornell University Press 2004).

Thomas, M. *Blackstone's Statutes on Property Law 2019-2020* (Oxford University Press 2019).

Tupman, W. A., 'Ten Myths About Terrorist Financing'. (2009). Journal of Money Laundering Control. 12, 189.

Unger B and van der Linde D (eds) *Research Handbook on Money Laundering* (Edward Elgar, 2013).

van der Does de Willebois E, *Nonprofit Organisations and the Combatting of Terrorism Financing: A Proportionate Response* (The World Bank, 2010).

Van Hoecke M (ed) *Epistemology and Methodology of Comparative Law* (Hart Publishing, 2004).

Walker, C. *Terrorism and the Law* (Oxford University Press 2011).

Williams, P. "Terrorist Financing and Organized Crime: Nexus, Appropriation, or Transformation?" in Thomas Biersteker and Sue Eckert, eds., *Countering the Financing of Terrorism* (New York: Routledge, 2008).

Wittig T, *Understanding Terrorist Finance* (Palgrave Macmillan, 2011).

Workneh T and Haridakis P, *Counterterrorism Laws and Freedom of Expression: Global Perspectives* (Lexington Books, 2021).

Yin R K, *Case Study Research and Applications: Design and Methods* (6th edn, SAGE, 2018).

Zimmer, K. "Propaganda by the Deed." In Immanuel Ness ed. *The International Encyclopaedia of Revolution and Protest* (Blackwell 2009).

Journals

Abdeldayem, M. M., and Aldulaimi, S. H., 'Cryptocurrency in The GCC Economy'. (2020). International Journal of Scientific & Technology Research. 9(2) 1.

Aburaya R, and others, 'FinTech Global Outlook and The Bahraini Landscape: Empirical Exploratory Analysis and Documentary Evidence,' 2021 International Conference on Decision Aid Sciences and Application (DASA), 2021, pp. 1007-1015, doi: 10.1109/DASA53625.2021.9682218.

Adetunji, J.A. 'Rethinking the internal mechanism of the EGMONT group in financial crime control', (2019), 22, Journal of Money Laundering Control, 2, 327.

Adeyemi A, 'Slipping Through the Net: The Financial Conduct Authority's Approach in Lessening the Incidence of Money Laundering in the UK', (2018), 21, J of ML Control, 2, 1.

Ahmed S, and Chavaly K, 'Blue Print of FinTech Regulatory Sandbox Law: Preparing for the Future of FinTech Innovation (2020)'. https://vidhilegalpolicy.in/wp-content/uploads/2020/03/20200313_Blueprint-of-a-Fintech-Regulatory-Sandbox-Law.pdf Accessed August 28, 2021.

Ai L, "'Rule-based but risk-oriented" approach for combating money laundering in Chinese financial sectors", (2012), 15, J of ML Control, 2, 198.

Ai L. '"Rule-based but risk-oriented" approach for combating money laundering in Chinese financial sectors', (2012), 15, Journal of Money Laundering Control, 2, 198.
Aidrous, I. 'Role of Financial Sector In Bahrain Economic Development, (2020). https://air.ue.katowice.pl/pdf/2020a/01Aidrous.pdf Accessed August 30, 2021.
Akartuna E A, Johnson D S, and Thornton A E, 'The money laundering and terrorist financing risks of new and disruptive technologies: a futures-oriented scoping review,' (2022), Secur J. https://doi.org/10.1057/s41284-022-00356-z
Akartuna E A, Johnson S D and Thornton A E, 'The money laundering and terrorist financing risks of new and disruptive technologies: a futures-oriented scoping review' (2022) 36 Secur J 615.
Akram, M., Nasar, A., and Rehman, A., 'Misuse of charitable giving to finance violent extremism; A futuristic actions study amidst COVID-19 pandemic' (2021), Social Sciences & Humanities Open, 4, 1.
Ali W, Muthaly S, and Dada M, 'Adoption of Shariah Compliant Peer-To-Business Financing Platforms by SMEs: A Conceptual Strategic Framework for FinTechs in Bahrain,' (2018), Int J of Inno Tech & Exploring Eng, 2, 1.
Aliyu A and others, 'Review of Some Existing Shariah-Compliant Cryptocurrency,' (2020), 6, J of Contemporary Islamic Studies, 1, 1.
Almutawa, A., 'Terrorism Measures in Bahrain: Proportionality and the Interplay between Security, Civil Liberties and Political Stability. (2018). The International Journal of Human Rights. 22(8) 949.
Al-Rashdan M, 'An analytical study of the financial intelligence units' enforcement mechanisms,' (2012), 15, J of ML Control, 4, 483.
Alsebaier, F., 'GCC: Promoting Block Chain Technology Adoption in the Financial Services Sector: Insights from Bahrain's Experience', (2020), Strategic Studies, https://www.iga.gov.bh/Media/Pdf-Section/Share/GCC-Promoting-Blockchain-Technology-Adoption-in-the-Financial-Services-Sector.pdf Accessed August 30, 2021.
Andres P, and others, 'Challenges of the Market for Initial Coin Offerings', (2022), 79, Int Rev of Fin Analysis, 1, 1.
Argyrou A, "Making the Case for Case Studies in Empirical Legal Research" (2017) 13(3) *Utrecht Law Review* 95-113.

Arner D W, Barberis, J., and Buckley R P., 'The Emergence of RegTech 2.0: From Know Your Customer to Know Your Data', (2016), 44, Journal of Financial Transformation, 79.
Arner, D W and Others, 'FinTech and Regtech: Enabling Innovation While Preserving Financial Stability (2017), 18, Georgetown Journal of International Affairs, 3, 47.
Arzandeh A, '"Gateways" Within the Civil Procedure Rules and the Future of Service-out Jurisdiction in England', (2019), 15, J of Private Int. L. 3, 516.
Awan, I. 'Glorifying and encouraging terrorism: preserving the golden thread of civil liberties in Britain'. (2012). Journal of Aggression, Conflict and Peace Research. 4, 3, 144.
Ayling J, 'Criminalising organisations: Towards Deliberative Lawmaking. (2011), 33, Law and Policy, 2, 149.
Azani, E. 'The Hybrid Terrorist Organisation: Hezbollah as a Case Study'. (2013). Studies in Conflict and Terrorism. 36, 11, 899.
Azgad-Tromer, S. 'Crypto securities: on the risks of investments in blockchain-based assets and the dilemmas of securities regulation'. (2018), Am. Univ. Law. Rev. 68(1):69–137.
Becker M, Merz, K and Buchkremer R, 'RegTech—the application of modern information technology in regulatory affairs: areas of interest in research and practice', (2020), Intell Sys Acc Fin Mgmt, 1.
Bello A, and Harvey J, "From a risk-based to an uncertainty-based approach to anti-money laundering compliance," (2017), 30, Security Journal, 1, 24.
Bergstrom M, 'The Many Uses of Anti-Money Laundering Regulation-Over Time and into the Future', (2018), 19, German Law Journal, 5, 1150.
Binning, P. 'In safe hands? Striking the balance between privacy and security -anti-terrorist finance measures' (2002) 6, *European Human Rights Law Review* 737, 747
Carrapico, H., Irrera, D., and Tupman, B. 'Transnational organised crime and terrorism: different peas, same pod?' (2014). Global Crime. 15, 4, 213.
Carroll, P., and Windle, J. 'Cyber as an enabler of terrorism financing, now and in the future'. (2018). Journal of Policing, Intelligence and Counter Terrorism. 13, 3, 285.
Cassella S, 'Illicit finance and money laundering trends in Eurasia.' (2019) 22 Journal of Money Laundering Control, 388-399.
Cassella S, 'Money laundering, terrorism, regulation, laws and legislation. (2004) 7 Journal of Money Laundering Control 92-94.

Çelik M E, "Regulated sector professionals and reporting suspicion of money laundering: is it a disproportionate burden?", Journal of Money Laundering Control, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/JMLC-01-2022-0018

Chaikin D, 'Risk-Based Approaches to Combating Financial Crime', (2009), 8, J of Law and Fin Mgmt, 2, 19.

Chaikin D, 'Risk-Based Approaches to Combating Financial Crime', (2009), 8, J of Law and Fin Mgmt, 2, 19.

Chatain, P. 'The World Bank's role in the fight against money laundering and terrorist financing'. (2004). International Law and Development. 6, 190.

Chiu I H, 'Decrypting the Signs of Regulatory Competition in Regulating Cryptoassets', (2020), 7, European Journal of Comparative Law and Governance, 3, 297.

Choo, K. R. 'Money Laundering and Terrorism Financing Risks of Prepaid Card Instruments'. (2009). Asian Criminology. 4, 11.

Choo, K. R., and Lui, L. 'An Analysis of Money Laundering and Terrorism Financing Typologies'. (2012). In *Journal of Money Laundering Control*, 15(1), 85-111.

Clunan, A. L. 'The Fight against Terrorist Financing'. (2006). Political Science Quarterly. 121, 4, 569.

Coelho P The Construction of the Legal Definition of Crypto-Asset under MiCAR, Including the Legal Subcategories: A Very Brief Summary SRNN Electronic Journals https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4884719

Coelho R, Fishman J, and Ocampo D G, 'Supervising Cryptoassets for Anti-Money Laundering, FSI Insights on Policy Implementation', (2021). https://www.bis.org/fsi/publ/insights31.pdf Accessed August 25, 2021.

Coelho R, Fishman J, and Ocampo D G, 'Supervising Cryptoassets for Anti-Money Laundering, FSI Insights on Policy Implementation', (2021). https://www.bis.org/fsi/publ/insights31.pdf Accessed August 25, 2021.

Costa, H., and Baños, J. 'Bioterrorism in the literature of the nineteenth century: The case of Wells and The Stolen Bacillus'. (2016). Cogent Arts & Humanities. 3, 1.

Crisanto J C, and Prenio J, 'Financial crime in times of Covid-19—AML and cyber resilience measures' (2020). https://www.bis.org/fsi/fsibriefs7.pdf Accessed August 22, 2021.

Crisanto J C, and Prenio J, ‘Financial crime in times of Covid-19—AML and cyber resilience measures’ (2020). https://www.bis.org/fsi/fsibriefs7.pdf Accessed August 22, 2021.

Dale, S. F. ‘Religious Suicide in Islamic Asia: Anticolonial Terrorism in India, Indonesia, and the Philippines’. (1988). The Journal of Conflict Resolution. 32, 1, 37.

Day W, ‘Jurisdictional Gateways in The CPR’, (2018), 77, The Cambridge Law Journal, 1, 36.

De Koker L, ‘Identifying and managing low money laundering risk: perspectives on FATF's risk-based guidance’, (2009), 16, J of Fin Crime, 4, 334.

De Koker L, ‘Identifying and managing low money laundering risk: perspectives on FATF's risk-based guidance’, (2009), 16, J of Fin Crime, 4, 334.

de Koker, L. ‘Identifying and managing low money laundering risk’, (2009), 16, J of Financial Crime, 4, 334.

Dei, G. J., and Asgharzadeh, A. "The Power of Social Theory: The Anti-Colonial Discursive Framework." (2001). The Journal of Educational Thought (JET). 35, 3, 297.

Dei, G. J., and Asgharzadeh, A. "The Power of Social Theory: The Anti-Colonial Discursive Framework." (2001). The Journal of Educational Thought (JET). 35, 3, 297.

Delston, J. B., ‘The Criminalisation of Money Laundering and Terrorism in Global Contexts: A Hybrid Solution. (2014). Journal of Global Ethics. 10, 326.

Demertzis, M., and Wolff, G. B., ‘The economic potential and risks of cryptoassets: is a regulatory framework needed?’ Policy Contribution. (2018).

Deng H. et al., ‘The regulation of initial coin offerings in China: problems, prognoses and prospects’. (2018) Eur. Bus. Org. Law. Rev. 19(3):465–502.

Dnes, A. W., and Brownlow, G. ‘The Formation of Terrorist Groups: An Analysis of Irish Republican Organisations’. (2017). Journal of Institutional Economics. 13, 3, 699.

Dolar, B. and Shughart, W. F, I. I. ‘Enforcement of the USA Patriot Act’s anti-money laundering provisions: Have regulators followed a risk-based approach?’, (2011) 22, Global Finance Journal, 1, 19.

Douglas T, "Notes on new Joint Money Laundering Steering Group (JMLSG) guidance", (2006), 7, J of Investment Compliance, 1, 64.

Emmanuel E, ‘Money laundering: An assessment of soft law as a technique for repressive and preventive anti-money laundering control’ (2016) 19, J of ML Control, 4, 346.

Esoimeme E, ‘Identifying and Reducing the Money Laundering Risks Posed by Individuals Who Have Been Unknowingly Recruited as Money Mules’, (2020), 24, J of ML Control, 1, 201.

Esoimeme, E, ‘Identifying and Reducing the Money Laundering Risks Posed by Individuals Who Have Been Unknowingly Recruited as Money Mules’, (2020), 24, Journal of Money Laundering Control, 1, 201.

FATF' International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations' (2023). <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf> accessed 17 January 2024.

FATF, 'Mutual Evaluations' (2023) <https://www.fatf-gafi.org/en/publications/Mutualevaluations/More-about-mutual-

Freeman, M. ‘The Sources of Terrorist Financing: Theory and Typology’. (2011). Studies in Conflict & Terrorism. 34, 6, 461.

Gandal, N., Hamrick, J. T., Moore, T., and Oberman, T., ‘Price Manipulation in the Bitcoin Ecosystem’. (2017). Journal of Monetary Economics. https://tylermoore.utulsa.edu/jme17.pdf

Giudici, G., Milne, A. and Vinogradov, D. ‘Cryptocurrencies: market analysis and perspectives. (2020). Journal of Industrial and Business Economics. 47, 1.

Goldby, M. ‘The Impact of Schedule 7 of the Counter-Terrorism Act 2008 on Banks and Their Customers’. (2010). Journal of Money Laundering Control. 13, 4, 351.

Grignon A, and Ascione Le Dréau C. ‘Anti-money laundering and counter terrorist financing under the EU–UK Trade and Cooperation Agreement’, (2021), 12, New Journal of European Criminal Law, 2, 283.

Grynkewich, A. ‘Welfare as Warfare: How Violent Non-State Groups Use Social Services to Attack the State’. (2008). Studies in Conflict and Terrorism. 31, 4, 350.

Haddadm C., and Hornuf, L,’ The Emergence of Global FinTech Market: Economic and Technological Determinants’, (2019). 58, Small Bus Eco, 81.

Haddadm C., and Hornuf, L,’ The Emergence of Global FinTech Market: Economic and Technological Determinants’, (2019). 58, Small Bus Eco, 81.

Haffke L, Fromberger M, and Zimmermann P. ‘Cryptocurrencies and anti-money laundering: the shortcomings of the fifth AML Directive (EU) and how to address them’. (2019), 21, J of Banking Regulation, 2.

Hamin Z and others, ‘Conceptualizing terrorist financing in the age of uncertainty.’ (2016) 19 Journal of Money Laundering Control 397-406.

Hasan R, Hassan M K, and Aliyu S, ‘Fintech, Blockchain and Islamic Finance: Literature Review and Research Agenda’, (2020), 3, Int J of Islamic Eco and Fin, 1, 75.

Hasan R, Hassan M K, and Aliyu S, ‘Fintech, Blockchain and Islamic Finance: Literature Review and Research Agenda’, (2020), 3, Int J of Islamic Eco and Fin, 1, 75.

Hassan A, and Sabirzyanov R, ‘Optimal Shariah Governance Model in Islamic Finance Regulation’, (2015), 3 Int J of Ed and Res, 4, 1.

Hassan A, and Sabirzyanov R, ‘Optimal Shariah Governance Model in Islamic Finance Regulation’, (2015), 3 Int J of Ed and Res, 4, 1.

Hausken, K., and Gupta, D. K. ‘Determining the Ideological Orientation of Terrorist Organisations: The Effects of Government Repression and Organised Crime’. (2016). International Journal of Public Policy. 12, 1, 71.

Hausken, K., and Gupta, D. K. ‘Terrorism and Organized Crime: The Logic of an Unholy Alliance’. (2015). International Journal of Contemporary Sociology. 52, 2, 1.

Heng, Y., and Ken, M. ‘The Other War on Terror Revealed: Global Governmentality and the Financial Action Task Force's Campaign against Terrorist Financing’. (2008). Review of International Studies. 34, 3, 553.

Henrik Haahr, J. ‘Open Coordination as Advanced Liberal Government’. *Journal of European Public Policy*. 11:2 (2004), pp. 209-3.

Hoffman B, "The confluence of international and domestic trends in terrorism.’ (1997) 9 Terrorism and Political Violence 1-15.

Hogg C, Jones K, and Swift N, ‘Failure to Prevent Market Abuse: A Potential New Corporate Criminal Offense?’ (2020), 41, Bus Law Rev, 4, 121.

Holman D, and Stettner B, ‘Anti-Money Laundering Regulation of Cryptocurrency: US and Global Approaches’, (2018).

Hopkins M, and Shelton N, 'Identifying Money Laundering Risk in the United Kingdom: Observations from National Risk Assessments and a Proposed Alternative Methodology', (2019), 25, Eur J Crim Policy Res, 63.

Hopkins M, and Shelton, N. 'Identifying Money Laundering Risk in the United Kingdom: Observations from National Risk Assessments and a Proposed Alternative Methodology', (2019), 25, Eur J Crim Policy Res, 63.

Horgan, J., and Taylor, M. 'Playing the "Green Card" - Financing the Provisional IRA'. (1999). Terrorism and Political Violence. 11, 2, 1.

Howden, E., 'The Crypto-Currency Conundrum: Regulating an Uncertain Future'. (2015). Emory International Law Review. 29, 1.

Huang S, 'Cryptoassets Regulation in the UK: An Assessment of the Regulatory Effectiveness and Consistency', (2021), 29, J of Fin Reg and Compliance, 3, 336.

Huang S. 'Cryptoassets Regulation in the UK: An Assessment of the Regulatory Effectiveness and Consistency', (2021), 29, J of Fin Reg and Compl, 3, 336.

Hufnagel S, and King C, 'Anti-Money Laundering Regulation and the Art Market', (2020), 40, Legal Studies, 1, 1.

Hyoeun Y, 'The UK's Fintech Industry Support Policies and its Implications' (2017), 7, World Economy Brief, 5, 1.

Hyytia, P., and Sundqvist, E., 'Accounting for Crypto-Currencies–A Nightmare for Accountants a Qualitative Study Exploring the Issues and Challenges when Accounting for Cryptocurrencies'. (2019). http://www.diva-portal.org/smash/get/diva2:1331799/FULLTEXT01.pdf

Irwin A S, Slay J, and Choo K R, 'Money Laundering and Terrorism Financing in Virtual Environments: A Feasibility Study', (2014), 17, J of ML Control, 1, 50.

Irwin A S, Slay J, and Choo K R, 'Money Laundering and Terrorism Financing in Virtual Environments: A Feasibility Study', (2014), 17, J of ML Control, 1, 50.

Irwin, A., Choo, K., and Lui, L. 'An Analysis of Money Laundering and Terrorism Financing Typologies'. (2012). Journal of Money Laundering Control (JMLC). 15(1), 85-111

Jabotinsky H Y, 'The Regulation of Cryptocurrencies: Between a Currency and a Financial Product', (2020), 31, Fordham Intell. Prop. Media & Ent. L.J. 1, 118.

Jabotinsky H Y, ‘The Regulation of Cryptocurrencies: Between a Currency and a Financial Product’, (2020), 31, Fordham Intell. Prop. Media & Ent. L.J. 1, 118.

Jamil, A.H., Mohd Sanusi, Z., Yaacob, N.M., Mat Isa, Y. and Tarjo, T., ‘The Covid-19 impact on financial crime and regulatory compliance in Malaysia’, Journal of Financial Crime, (2021). https://doi.org/10.1108/JFC-05-2021-0107.

Jamil, A.H., Mohd Sanusi, Z., Yaacob, N.M., Mat Isa, Y. and Tarjo, T., ‘The Covid-19 impact on financial crime and regulatory compliance in Malaysia’, Journal of Financial Crime, (2021). https://doi.org/10.1108/JFC-05-2021-0107.

Jayasekara S D, ‘How effective are the current global standards in combating money laundering and terrorist financing?’ (2021), 24, J of Money Laundering Control, 2, 257.

Jayasekara S D. Administrative model of financial intelligence units: an analysis of effectiveness of the AML/CFT regime", (2022), 25, J of Money Laundering Control, 3, 511.

Jayasuriya, D. "Money laundering and terrorist financing: the role of capital market regulators", (2002). Journal of Financial Crime. 10, 30.

Jensen, R. ‘Daggers, Rifles and Dynamite: Anarchist Terrorism In Nineteenth Century Europe’. *Terrorism and Political Violence*. 16, 1 (2004), pp. 116.

Johnson D, ‘What Are the Merits of Taking a Hybrid Regulatory Approach Toward the Enforcement of Corporate Financial Crime in the United Kingdom and United States of America?’, (2022), 2, J. of White Collar and Corporate Crime, 1, 23.

Johnson, J. ‘Is the Global Financial System AML/CTF Prepared?’ *Journal of Financial Crime*. 15, 7 (2008), pp. 8.

Jonsson, M., and Cornell, S. ‘Countering Terrorist Financing: Lessons from Europe’. *Georgetown Journal of International Affairs*. 8, 1 (2007), pp. 69.

Keatinge, T., and Keen, F. ‘Social Media and (Counter) Terrorist Finance: A Fund-Raising and Disruption Tool’. *Studies in Conflict & Terrorism*. (2018), pp. 1–28. doi:10.1080/1057610x.2018.1513698

Kebbell S, ‘The Law Commission: anti-money laundering and counter-terrorism financing - reform of the suspicious activity reporting regimes’, (2018), 11, Criminal Law Review, 880.

Kochergin F, Crypto-assets: Economic nature, classification and regulation of turnover." (2022) 17 International organisations research journal 75-113.

Korejo M , Rajamanickam R and Said R, The concept of money laundering: a quest for legal definition (2021) 24 Journal of Money Laundering Control

Korteweg, R, 'Black Holes: On Terrorist Sanctuaries and Governmental Weakness' (2008) 10 *Civil Wars* 60

Koster, H, 'Towards better implementation of the European Union's anti-money laundering and countering the financing of terrorism framework' (2020), 23, J of ML Control, 2, 379.

Koster, H., 'Towards better implementation of the European Union's anti-money laundering and countering the financing of terrorism framework', (2019). Journal of Money Laundering Control.

Kumar, S, '"Terrorism" or the Illegitimacy of Politics in Colonial India' (2016) 44 *Social Scientist* 41

Kurtulis, E N, 'The "New Terrorism" and Its Critics' (2011) 34 *Studies in Conflict and Terrorism* 476

Lagerwaard P, 'Financial surveillance and the role of the Financial Intelligence Unit (FIU) in the Netherlands' (2022), J of ML Control, https://doi.org/10.1108/JMLC-09-2022-0134.

Levi, M. "Combating The Financing of Terrorism: A History and Assessment of the Control of 'Threat Finance.'" (2010), 50, The British Journal of Criminology, 4, 650. http://www.jstor.org/stable/43610773.

Levitt, M. 'Going to the Source: Why Al Qaeda's Financial Network Is Likely to Withstand the Current War on Terrorist Financing'. (2004). 27, Studies in Conflict and Terrorism, 3, 169.

Levy, I., & Yusuf, A. 'How Do Terrorist Organisations Make Money? Terrorist Funding and Innovation in the Case of al-Shabaab', (2019). Studies in Conflict & Terrorism, 1–23. doi:10.1080/1057610x.2019.1628622

Lokanan, M. E and Nasimi, N., 'The effectiveness of Anti-Money Laundering policies and procedures within the Banking Sector in Bahrain' (2019), 23, Journal of Money Laundering Control, 4, 769.

Lowe, R. J. 'Anti-money laundering – the need for intelligence', (2017), 24, J of Fin Crime, 3, 472.

M Rudner, 'Hizbullah Terrorism Finance: Fund-Raising and Money-Laundering', (2010), 33, Studies in Conflict & Terrorism, 8, 700

Marian, O. 'A conceptual framework for the regulation of cryptocurrencies.' (2015). University of Chicago Law Review. 82:53–68.

Matthias, L., ‘Who Owns Bitcoin? Private Law Facing the Blockchain’. (2019). Minnesota Journal of Law, Science & Technology. 21, 93.

Maxson S, Davis S, and Moulton, R, ‘UK Cryptoassets Taskforce publishes its final report’, (2019), 20, J of Investment Compliance, 2, 28.

Mekpor E S, ‘Anti-money laundering and combating the financing of terrorism compliance. Are FATF member states just scratching the surface?’ (2019). Journal of Money Laundering Control, 00–00. doi:10.1108/jmlc-09-2018-0057

Micheler, E., and Whaley, A. ‘Regulatory Technology: Replacing Law with Computer Code’ (2020), 21, Eur Bus Org Law Rev 349.

Murrar F, and Barakat K, ‘Role of FATF in spearheading AML and CFT’ (2021), 24, Journal of Money Laundering Control, 1, 77. https://doi.org/10.1108/JMLC-01-2020-0010

Naheem, M.A. ‘Analysis of Bahrain’s anti-money laundering (AML) and combating of terrorist financing (CTF) practices’ (2020). Journal of Money Laundering Control. https://doi.org/10.1108/JMLC-04-2018-0033 Accessed August 30, 2021.

Naz F, and others, ‘Fintech Growth during COVID-19 in MENA Region: Current Challenges and Future prospects’, (2022), Electron Commer Res, https://doi.org/10.1007/s10660-022-09583-3.

Nelson, R. M., ‘Examining Regulatory Frameworks for Digital Currencies and Blockchain’ (2019). https://crsreports.congress.gov/product/pdf/TE/TE10034

Nia, M. M. ‘From old to new terrorism: The changing nature of international security’. (2010), 18, Global Studies Journal, 1

organ, J., and Taylor, M. ‘Playing the ‘Green Card’—Financing the Provisional IRA: Part 1’. *Terrorism and Political Violence*. 11(2) (Summer 1999), p. 10.

Othman A H, and others, ‘The impact of cryptocurrencies market development on banks’ deposits variability in the GCC region’, (2020), 12, J of Fin Econ Policy, 2, 161.

Parker, T., and Sitter, N., ‘The Four Horsemen of Terrorism: It's Not Waves, It's Strains’, (2016), 28, Terrorism and Political Violence, 2, 197.

Pavlidis G, ‘International regulation of virtual assets under FATF’s new standards’ (2020), 21, J of Investment Compliance, 1, 1.

Pavlidis, G. ‘International regulation of virtual assets under FATF’s new standards’, (2020), 21, *Journal of Investment Compliance*, 1, 1.

Perri, F. S., and R. G. Brody. 'The Dark Triad: Organized Crime, Terror and Fraud' (2011), 14, Journal of Money Laundering Control, 1, 44.

Petrich, K. 'Cows, Charcoal, and Cocaine: Al-Shabaab's Criminal Activities in the Horn of Africa', (2019). Studies in Conflict & Terrorism, DOI: 10.1080/1057610X.2019.1678873

Picarelli, J. T. 'The Turbulent Nexus Of Transnational Organised Crime And Terrorism: A Theory of Malevolent International Relations', (2006), 7, Global Crime, 1, 1.

Pieth, M, 'Criminalizing the financing of terrorism,' (2006), 4, Journal of International Criminal Justice, 5, 1078

Pol R F, 'Anti-money laundering effectiveness: assessing outcomes or ticking boxes?' (2018),

21, Journal of Money Laundering Control, 2, 215.

Post J. M, McGinnis C, Moody K. 'The changing face of terrorism in the 21st century: the communications revolution and the virtual community of hatred', (2014), 32, Behav Sci Law. 3, 306.

Post, J. M. Terrorism and right-wing extremism: the changing face of terrorism and political violence in the 21st century: the virtual community of hatred. (2015), 65, Int J Group Psychother. 2, 242.

Price, E. 'Literature on the Financing of Terrorism', (2013), 7, *Perspectives on Terrorism*. 4: 112

Price, H. E. "The Strategy and Tactics of Revolutionary Terrorism." (1977), 19, *Comparative Studies in Society and History,* 1: 52.

Rabbani M R, Bashar S, and Khan S, 'Agility and Fintech is the Future of Islamic Finance: A

Study from Islamic Banks in Bahrain', (2021), 9, Int J of Sci & Tech Res, 3, 1.

Rabbani, M. R., and Khan, S., 'Agility and Fintech is the Future of Islamic Finance: A Study

from Islamic Banks in Bahrain' (2020). 9, Int. J. Sci. & Tech. Res. 3, 1

Rabbani, M. R., Khan, S., and Thalassinos, E. I., 'FinTech, Block chain and Islamic Finance: An

Extensive Literature Review, (2020). 8, Int. J. Econ. And Bus. Adm, 2, 65

Raphaeli, N. 'Financing Of Terrorism: Sources, Methods, And Channels'. (2003), 15, Terrorism and Political Violence, 4, 59.

Razzaque, A. Cummings R. T., Karolak, M., and Hamdan, A., 'The Propensity of FinTech: Input

from Bankers in the Kingdom of Bahrain', (2020), 19, J. of Info. And Know Mgmt. 1, 1

Rees, G., and Moloney, T. 'The Latest Efforts to Interrupt Terrorist Supply Lines: Schedule 7 to the Counter-Terrorism Act 2008'. (2010). Criminal Law Review, 127.

Reports

Riondet S, 'The Value of Public-Private Partnerships for Financial Intelligence', (2018), 2, J of Fin Compliance, 2, 148.

Robinson R., 'The new digital wild west: regulating the explosion of initial coin offerings'. (2018). Tennessee Law Review. 85(4):897.

Rosendorff, P. and T. Sandler, 'Too Much of a Good Thing? The Proactive Response Dilemma', (2004), 48, Journal of Conflict Resolution, 657.

Ross S, and Hannan M, 'Money laundering regulation and risk-based decision-making' (2007), 10, J of Money Laundering Control, 1, 106.

Roth, M. and Sever, M. 'Cutting Off the Hand That Feeds It: Countering Terrorist-Financing in the 21st Century'. (2010), 1 International Journal of Security and Terrorism, 1, 59.

Roth, M., and Sever, M., "The Kurdish Workers Party (PKK) as Criminal Syndicate: Funding Terrorism through Organized Crime, A Case Study," (2007) *Studies in Conflict and Terrorism* 30, p. 906.

Ryder N, 'Is It Time to Reform the Counter-Terrorism Financing Reporting Obligations? On the EU and the UK System', (2018), 19, German Law J, 5, 1170.

Ryder N, 'The Financial War on Terrorism: A Review of Counter-Terrorism Financing Strategies Since 2001' (New York: Routledge, 2015).

Ryder, N. "A false sense of security? An analysis of legislative approaches towards the prevention of terrorist finance in the United States and the United Kingdom."[2007] Journal of Business Law, p 849.

Sadowski K, 'Impact of PSD2 on The Payment Services Market –General Objectives and Evidence from Polish and UK Legal Systems', (2021), 11, Wroclaw Review of Law, Admin and Eco, 1, 1.

Salami, I. 'Terrorism Financing with Virtual Currencies: Can Regulatory Technology Solutions Combat This?', (2017), Studies in Conflict & Terrorism, 1–22.

Sauce L, 'The unintended consequences of the regulation of cryptocurrencies', (2022), 46, Cambridge Journal of Economics, 1, 57.

Schneider, F and Caruso, R. 'The (Hidden) Financial Flows of Terrorist and Transnational Crime Organisations: A Literature Review and Some Preliminary Empirical Results' (2011) https://www.econstor.eu/bitstream/10419/119378/1/diw_econsec0052.pdf accessed 29 January 2021

Schneider, F. 'The (Hidden) Financial Flows of Terrorist and Organized Crime Organisations: A Literature Review and Some Preliminary Empirical Results' (2010) *IZA Discussion Paper* http://ftp.iza.org/dp4860.pdf accessed 29 January 2021

Schwartz N, Chen K, and Markevych M, 'Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (1): Some Legal and Practical Considerations', (2021). https://www.elibrary.imf.org/view/journals/063/2021/002/article-A001-en.xml.

Sedgwick, M. 'Inspiration and the Origins of Global Waves of Terrorism,' (2007), 30, Studies in Conflict & Terrorism, 97.

Segarajasingham S, "Law Relating to Money Laundering: A Critical Analysis Focus on Sri Lankan Law', (2019), 17, Int J of Bus, Econ and Law, 4, 1.

Shaw, D. O. (2019). Beyond necessity: Hezbollah and the intersection of state-sponsored terrorism with organised crime. Critical Studies on Terrorism, 1–23. doi:10.1080/17539153.2019.1592074

Shaw, D. O. 'Beyond necessity: Hezbollah and the intersection of state-sponsored terrorism with organised crime'. (2019). Critical Studies on Terrorism, 1–23. doi:10.1080/17539153.2019.1592074

Shpayer-Makov, H. "Anarchism in British Public Opinion 1880-1914." ((1988), 31 *Victorian Studies,* 4: 487

Silke, A, "Drink, Drugs, and Rock'n'Roll: Financing Loyalist Terrorism in Northern Ireland-Part Two,' (2000), 23 *Studies in Conflict and Terrorism,* 120.

Simon, J. D. 'The Forgotten Terrorists: Lessons from the History of Terrorism'. (2008), 20, Terrorism and Political Violence, 2, 195

Söderberg G, Are Bitcoin and other crypto-assets money. (2018) 5 Economic Commentaries14

Spaendonck, R., 'To School or to Syria? The foreign fighter phenomenon from a children's rights perspective' (2016), 12, Utrecht Law Review, 2, 1-22.

Sproat, P. 'Counter-terrorist finance in the UK: a quantitative and qualitative commentary based on open-source materials' (2010) 13(4) Journal of Money Laundering Control, 315, 318.

Sproat, P. A. ‘Counter-terrorist finance in the UK’, (2010). 13, J of Money Laundering Control, 4, 315. doi:10.1108/13685201011083858.
Sung A, and others. ‘An exploratory study of the FinTech (Financial Technology) education and retraining in UK’, (2019), 11, J of Work-Applied Mgmt, 2, 187.
Sung A, Leong K, Sironi P, O’Reilly T, and McMillan A. ‘An exploratory study of the FinTech (Financial Technology) education and retraining in UK’, (2019), 11, J of Work-Applied Mgmt, 2, 187.
Teichmann, F M J. ‘Financing Terrorism through Cryptocurrencies – A Danger for Europe?’ (2018) 21 *Journal of Money Laundering Control* 513
Tofangsaz, H. ‘Rethinking Terrorist Financing; Where Does All This Lead’ (2015) 18 *Journal of Money Laundering Control* 112
Truby, J, ‘Fintech and the city: Sandbox 2.0 policy and regulatory reform proposals’, (2018) Int. Rev. of Law, Comp. & Tech.
Turner S, and Bainbridge J, ‘An Anti-Money Laundering Timeline and the Relentless Regulatory Response’, (2018), 82, The J of Crim Law, 3, 215.
Turner S., and Bainbridge J. ‘An Anti-Money Laundering Timeline and the Relentless Regulatory Response’, (2018). 82, The Journal of Criminal Law, 3, 215
Velkes G C, ‘International Anti-Money Laundering Regulation of Virtual Currencies and Assets’, (2020), 52, Int. L and Politics, 10, 87.
Velkes G G, ‘International Anti-Money Laundering Regulation of Virtual Currencies and Assets’, (2020), 52, Int Law and Politics, 3, 876.
Verhage A, ‘Great Expectations but Little Evidence: Policing Money Laundering’ (2017) 37 International Journal of Sociology and Social Policy, 477
Waszak, J D. ‘The Obstacles to Suppressing Radical Islamic Terrorist Financing’ (2004) 36 *Case Western Reserve Journal of International Law* 673
Whyte, C. ‘Cryptoterrorism: Assessing the Utility of Blockchain Technologies for Terrorist Enterprise’ (2019) *Studies in Conflict & Terrorism* 1–24
Wronka C. ‘Anti-money laundering regimes: a comparison between Germany, Switzerland and the UK with a focus on the crypto business’ (2021), Journal of Money Laundering Control, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/JMLC-06-2021-0060 Accessed March 25, 2022.

Yalcinkaya, H. ‘Turkey’s Struggle Against the Foreign Terrorist Fighters of Daesh’ (2016) 21 *Perceptions* 27

Yip C, Han N L R H and Sng B L, 'Legal and ethical issues in research' (2016) 60 Indian J Anaesth 684.

Zetzsche D A, and others, ‘Regulating A Revolution: From Regulatory Sandboxes To Smart Regulation’, (2017), 23, Fordham Journal of Corporate and Financial Law, 1, 31

Zetzsche, D A and Others, ‘From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance’, (2017), New York University Journal of Law and Business, European Banking Institute Working Paper Series 2017 - No. 6

Allen J G, and UK Finance, ‘Same Activity, Same Risk, Same Regulation’, (2021). https://www.ukfinance.org.uk/system/files/Same%20activity%2C%20same%20risk%2C%20same%20regulation%20-%20FINAL.pdf Accessed March 25, 2022.

Alsebaie F, ‘GCC: Promoting Blockchain Technology Adoption in the Financial Services Sector: Insights from Bahrain’s Experience’ (2020), https://www.iga.gov.bh/Media/Pdf-Section/Share/GCC-Promoting-Blockchain-Technology-Adoption-in-the-Financial-Services-Sector.pdf Accessed November 25, 2022.

Anderson, D. ‘4th Report on the Operation of the Terrorist Asset-Freezing Etc Act 2010’. (2015). Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/412084/TAFA_2014__4th_report_.pdf Accessed on January 29, 2021.

Anderson, D. ‘Fourth report on the operation of the Terrorist-Asset Freezing Etc. Act 2010’ (2014). 11.

Anderson, D. ‘Second report on the operation of the Terrorist-Asset Freezing Etc. Act 2010’ (2012). 11.

Andres, P., Arroyo, D., Correia, R., and Rezola, A., ‘Regulatory and Market Challenges of Initial Coin Offerings’. (2019). https://ecgi.global/sites/default/files/working_papers/documents/final2andresarroyocorreiarezola_1.pdf

Bahrain FID, “Annual report 2016”, Financial Intelligence Directorate, (2016).

Bains P, and others, ‘Regulating the Crypto Ecosystem: The Case of Unbacked Cryptoassets,’ (2022), IMF Fintech Note 2022/007, International Monetary Fund, Washington, DC.

Bank of England, 'Central Bank Digital Currency: Opportunities, Challenges and Design. (2020). https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf?la=en&hash=DFAD18646A77C00772AF1C5B18E63E71F68E4593

BEDB, 'Bahrain FinTech Ecosystem Report 2018, (2019). https://164b166b-ce2b-409c-80d0-881210c4ed36.filesusr.com/ugd/304023_6c6990419b084d8aa7999f50bc223517.pdf Accessed August 30, 2021.

Borlini, L., and Montanaro, F., 'The Evolution of the EU Law Against Criminal Finance: The Hardening of FATF Standards within the EU. (2017). Georgetown Journal of International Law.

Braddick K., Bailer A., and Ramsden D., 'Cryptoassets Taskforce: Final Report'. (2018). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf Accessed March 25, 2022.

Braddick K., Bailer A., and Ramsden D., 'Cryptoassets Taskforce: Final Report'. (2018). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf Accessed March 25, 2022.

Braddick, K., Bailey, A., and Ramsden, D., 'Cryptoassets Task Force: Final Report'. (2018). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/crypto_assets_taskforce_final_report_final_web.pdf

Browning S, 'Cryptocurrencies: Bitcoin and other exchange tokens', Briefing Paper No. 8780 (2020), https://researchbriefings.files.parliament.uk/documents/CBP-8780/CBP-8780.pdf Accessed March 25, 2022.

Bullmann, D., Klemm, J., and Pinna, A., 'In search for stability in crypto-assets: are stable coins the solution?' (2018). https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf

Bureau of Counterterrorism. 'Country Reports on Terrorism 2019' (2020). Available at https://www.state.gov/wp-content/uploads/2020/06/Country-Reports-on-Terrorism-2019-2.pdf Accessed on January 29, 2021.

Cabinet Office. 'Recovering the Proceeds of Crime—A Performance and Innovation Unit Report'. (2000). 118-120.

CBB Rule Book, 'Financial Crime Module, Vol 1: Conventional Banks', (2021). https://www.cbb.gov.bh/wp-content/uploads/2021/05/Consultation_Vol-1_FC_E-KYC.pdf Accessed August 30, 2021.

CBB Rulebook, ‘Crypto-Asset Module: Central Bank of Bahrain Rule Book, Vol 6: Capital Markets’ (2019). https://cbben.thomsonreuters.com/sites/default/files/net_file_store/Vol_6-CRA-Feb_2019.pdf Accessed August 30, 2021.
CBB Rulebook, ‘Crypto-Asset Module: Central Bank of Bahrain Rule Book, Vol 6: Capital Markets’ (2019). https://cbben.thomsonreuters.com/sites/default/files/net_file_store/Vol_6-CRA-Feb_2019.pdf Accessed August 30, 2021.
CBB RuleBook, ‘Financial Crime Module, Vol 2: Islamic Banks’ (2021). https://www.cbb.gov.bh/wp-content/uploads/2021/05/Consultation_Vol-2_FC_E-KYC.pdf Accessed August 25, 2021.
CBB RuleBook, ‘Financial Crime Module, Vol 2: Islamic Banks’ (2021). https://www.cbb.gov.bh/wp-content/uploads/2021/05/Consultation_Vol-2_FC_E-KYC.pdf Accessed August 25, 2021.
CCAF, ‘FinTech Regulation in the Middle East and North Africa,’ (2021). https://www.jbs.cam.ac.uk/wp-content/uploads/2022/02/ccaf-2022-02-fintech-regulation-in-mena.pdf Accessed Nov 30, 2022.

CCAF, World Bank and World Economic Forum, ‘The Global Covid-19 FinTech Market Rapid Assessment Report,’ University of Cambridge, World Bank Group and the World Economic Forum (2020), https://www.jbs.cam.ac.uk/wp-content/uploads/2021/03/2020-ccaf-global-covid-fintech-market-rapid-assessment-study-v2.pdf Accessed Nov 30, 2022.

Chiu I H, ‘Regulating Crypto-Finance: A Policy Blueprint’, ECGI Working Paper Series in Law, (2021), https://ecgi.global/sites/default/files/working_papers/documents/chiufinal.pdf Accessed March 25, 2022.

Clancy, T. ‘Theory of an Emerging-State Actor: The Islamic State of Iraq and Syria (ISIS) Case’. (2018). Systems. 6, 2, 16.

Coelho R, Fishman J, and Ocampo D G, ‘Supervising Cryptoassets for Anti-Money Laundering, FSI Insights on Policy Implementation’, (2021), https://www.bis.org/fsi/publ/insights31.pdf Accessed March 25, 2022.

Committee on Payments and Market Infrastructures, ‘Payment Aspects of Financial Inclusion’ (2016). https://documents1.worldbank.org/curated/en/806481470154477031/pdf/107382-WP-REPLLACEMENT-PUBLIC-PAFI-Report-final-in-A4.pdf Accessed August 25, 2021.

Committee on Payments and Market Infrastructures, 'Payment Aspects of Financial Inclusion' (2016). https://documents1.worldbank.org/curated/en/806481470154477031/pdf/107382-WP-REPLLACEMENT-PUBLIC-PAFI-Report-final-in-A4.pdf Accessed August 25, 2021.

Cooper, K. A. 'A critical examination of the anti-money laundering legislative framework for the prevention of terrorist finance with particular reference to the regulation of alternative remittance systems in the UK'. (2014). Available at http://etheses.whiterose.ac.uk/6906/1/Karen%20Cooper%20%20student%20id%20200509079%20School%20of%20law%20%20PhD%202014.pdf Accessed on January 29, 2021.

Cutts T, 'Crypto-Property: Response to Public Consultation by the UK Jurisdiction Taskforce of the LawTech Delivery Panel' (June 19, 2019). LSE Law - Policy Briefing Paper No. 36, June 2019, Available at http://dx.doi.org/10.2139/ssrn.3406736 Accessed March 25, 2022.

D W Arner, J N Barberis and R P Buckley, 'The Evolution of Fintech: A New Post-Crisis Paradigm?', (2015), https://core.ac.uk/download/pdf/38088713.pdf

Deloitte, 'Fintech:-On the brink of further disruption,' (2020), https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/financial-services/deloitte-nl-fsi-fintech-report-1.pdf Accessed Nov 30, 2022.

Department for International Trade, 'UK FinTech State of the Nation,' (2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/801277/UK-fintech-state-of-the-nation.pdf Accessed Dec 12, 2022.

Dion-Schwatz, C., Manheim, D., and Johnston, P. B. 'Terrorist Use of Cryptocurrencies: Technical and Organisational Barriers and Future Threats'. (2019). https://www.rand.org/content/dam/rand/pubs/research_reports/RR3000/RR3026/RAND_RR3026.pdf Accessed on January 29, 2021.

European Central Bank "Crypto-assets: Implications for financial stability, monetary policy, and payments and market infrastructures", Occasional Paper Series No. 223, (May 2019). https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf

European Central Bank, "Virtual currency schemes – a further analysis", (February 2015). https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf

European Central Bank, "Virtual currency schemes", (October 2012). https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

European Commission, 'Report from The Commission To The European Parliament And The Council' (2019). https://ec.europa.eu/info/sites/info/files/supranational_risk_assessment_of_the_money_laundering_and_terrorist_financing_risks_affecting_the_union.pdf
European Commission, 'Report from The Commission to The European Parliament and The Council' (2017). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0340
EY, 'UK FinTech: Moving mountains and moving mainstream,' (2020), https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/emeia-financial-services/ey-uk-fintech-2020-report.pdf Accessed Nov 29, 2022.
FATF 'Guidance on Risk-Based Supervision, FATF, Paris', (2021), www.fatf-gafi.org/publications/documents/Guidance-RBA-Supervision.html Accessed March 25, 2022.
FATF 'Virtual Assets and Virtual Asset Service Providers: Guidance for a Risk-based Approach.' (2019). https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html
FATF Annual Report, 'Financial Action Task Force-Annual Report 2019-2020, FATF/OECD, Paris'. (2020). https://www.fatf-gafi.org/media/fatf/documents/brochuresannualreports/FATF-annual-report-2019-2020.pdf
FATF Report, 'Virtual Currencies: Key Definitions and Potential AML/CFT Risks' (2014). https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf
FATF, 'Annual Report 2020-2021', (2021). https://www.fatf-gafi.org/media/fatf/documents/brochuresannualreports/Annual-Report-2020-2021.pdf Accessed March 25, 2022.
FATF, 'Anti-Money Laundering and Counter-terrorist Financing Measures: United Kingdom-Mutual Evaluation Report'. (2018). https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-Kingdom-2018.pdf
FATF, 'Anti-money laundering and counter-terrorist financing measures–United Kingdom, Fourth Round Mutual Evaluation Report, FATF', Paris (2018) http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-united-kingdom-2018.html Accessed March 25, 2022.

FATF, 'Anti-money laundering and counter-terrorist financing measures – United Kingdom 1st Regular Follow-up Report, FATF, Paris' (2022) http://www.fatf-gafi.org/publications/mutualevaluations/documents/fur-united-kingdom-2022.html Accessed Nov 25, 2022.

FATF, 'Anti-money laundering and counter-terrorist financing measures– United Kingdom, Fourth Round Mutual Evaluation Report, FATF,' (2018), Paris http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-united-kingdom-2018.htm Accessed Nov 20, 2022.

FATF, 'COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses' (2020). https://www.fatf-gafi.org/media/fatf/documents/COVID-19-AML-CFT.pdf Accessed August 30, 2021.

FATF, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' (2019). <www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html> Accessed August 20, 2021.

FATF, 'Guidance on Risk-Based Supervision, FATF, Paris,' (2021), www.fatf-gafi.org/publications/documents/Guidance-RBA-Supervision.html Accessed March 25, 2022.

FATF, 'Methodology for Assessing Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems, updated October 2021,' FATF, Paris, (2013-2021), http://www.fatf-gafi.org/publications/mutualevaluations/documents/fatf-methodology.html Accessed Dec 5, 2022.

FATF, 'Methodology for Assessing Technical Compliance with The FATF Recommendations And The Effectiveness Of AML/CFT Systems' (2020). https://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf Accessed August 30, 2021.

FATF, 'Money Laundering using New Payment Methods, (2010)'. Available at < https://www.fatfgafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf >Accessed on January 29, 2021

FATF, 'Opportunities and Challenges of New Technologies for AML/CFT,' FATF, Paris, France (2021), https://www.fatf-gafi.org/publications/fatfrecommendations/documents/opportunities-challenges-new-technologies-aml-cft.htm Accessed Dec 23, 2022.

FATF, 'Second 12-month Review Virtual Assets and VASPs,' FATF, Paris, France, (2021) <www.fatf-gafi.org/publications/fatfrecommendations/documents/second-12-month-review-virtual-assets-vasps.htm> Accessed Dec 1, 2022.

FATF, 'The Role of Hawala and Other Similar Service Providers in Money Laundering and Terrorist Financing', FATF/OECD (2013), p. 9.

FATF, "Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)", FATF/ OECD, Paris. (2015). Available at < http://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organisation-ISIL.pdf.>Accessed on January 29, 2021

FATF, FATF Focus on Virtual Assets. (2020). https://www.fatf-gafi.org/publications/virtualassets/documents/virtual-assets.html?hf=10&b=0&s=desc(fatf_releasedate)

FATF.GAFI, 'Financial Action Task Force: The United Kingdom of Great Britain and North Ireland', (2007), https://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20UK%20FULL.pdf> Accessed March 25, 2022.

FATF' Anti-money laundering and counter-terrorist financing measures: United Kingdom-Mutual Evaluation Report. (2018). https://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-united-kingdom-2018.html

FATF–Egmont Group, 'Concealment of Beneficial Ownership' (2018), Paris, France. <www.fatf-gafi.org/publications/methodandtrends/documents/concealment-beneficial-ownership.html> Accessed August 21, 2021.

FATF-MENAFATF, 'Anti-Money Laundering and Counter-Terrorist Financing Measure-Bahrain. Fourth Round Mutual Evaluation Report, FATF, Paris. (2018). http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-bahrain-2018.html

FATF-MENAFATF, 'Anti-Money Laundering and Counter-Terrorist Financing Measures for Kingdom of Bahrain: Mutual Evaluation Report' (2018).

FCA 'Guidance on Cryptoassets Feedback and Final Guidance to CP 19/3'. (July, 2019). https://www.fca.org.uk/publication/policy/ps19-22.pdf

FCA, 'Business Plan 2021/22', https://www.fca.org.uk/publication/business-plans/business-plan-2021-22.pdf Accessed March 25, 2022.

FCA, ‘Consumers warning about the risk of Initial Coin Offerings (ICOs)’, (2017), https://www.fca.org.uk/news/statements/initial-coin-offerings Accessed March 25, 2022.
FCA, ‘Discussion paper on Distributed Ledger Technology’ Discussion Paper DP 17/3, (2017). https://www.fca.org.uk/publication/discussion/dp17-03.pdf Accessed March 25, 2022.
FCA, ‘Financial Crime Guide: A firm’s guide to countering financial crime risks (FCG)’, (March, 2022). https://www.handbook.fca.org.uk/handbook/FCG.pdf Accessed March 25, 2022.
FCA, ‘Guidance on Cryptoassets’ (January, 2019). https://europeanchamberofdigitalcommerce.com/wp-content/uploads/2019/06/Guidance-on-Crypto-assets-Consultation-Paper.pdf
FCA, ‘Guidance on Cryptoassets: Feedback and Final Guidance to CP 19/3’ (2019). Policy Statement PS 19/22. https://www.fca.org.uk/publication/policy/ps19-22.pdf Accessed March 25, 2022.
FCA, ‘Payment Services and Electronic Money–Our Approach’, (2018). https://www.fca.org.uk/publication/finalised-guidance/fca-approach-payment-services-electronic-money-july-2018-track-changes.pdf Accessed March 25, 2022.
FCA, ‘Prohibiting the sale to retail clients of investment products that reference cryptoassets’, Policy Statement PS20/10, (2020). https://www.fca.org.uk/publication/policy/ps20-10.pdf Accessed March 25, 2022.
FCA, ‘Research Note: Cryptoasset Consumer Research 2021’, https://www.fca.org.uk/publications/research/research-note-cryptoasset-consumer-research-2021 Accessed March 25, 2022.
Feikert-Ahalt C, ‘Regulatory Approaches to Cryptoassets in Selected Jurisdictions,’ (2019), https://tile.loc.gov/storage-services/service/ll/llglrd/2019668148/2019668148.pdf Accessed Dec 17, 2022.
Financial Services Authority. ‘Final Notice: Habib Bank AG Zurich’, (2012). Retrieved http://www.fsa.gov.uk/static/pubs/final/habib-bank.pdf. Accessed March 25, 2022.
FSA, ‘Anti-Money Laundering Supervision by the Legal and Accountancy Professional Body Supervisors: Progress and Themes from Our 2020/21 Supervisory Assessments’. (2021). https://www.fca.org.uk/publication/opbas/supervisory-assessments-progress-themes-2020-21.pdf Accessed March 25, 2022.

FSB, ‘Crypto-asset markets: Potential channels for future financial stability implications’. (2018). https://www.fsb.org/wp-content/uploads/P101018.pdf
FSB, ‘Crypto-Asset Markets: Potential Channels for Future Market Stability Implications,’ Basel, (2018), https://www.fsb.org/wp-content/uploads/P101018.pdf Accessed Dec 17, 2022.
Gambling Commission, ‘The Money Laundering and Terrorist Financing Risks within the British Gambling Industry’, (Dec 2020), https://assets.ctfassets.net/j16ev64qyf6l/1hA9tcIqe0F0AETdwaQM1U/4440bed7d59035a78cefca96a9326a66/Gambling_Commission_Risk_Assessment_2020_Final_version.pdf Accessed March 25, 2022.
Government Office for Science, ‘FinTech Futures: The UK as a World Leader in Financial Technologies’, (2015), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/413095/gs-15-3-fintech-futures.pdf Accessed March 25, 2022.
Gunson, C., and Altymulkamedov, B., ‘Crypto Asset Exchanges in the Middle East: Kingdom of Bahrain and the Abu Dhabi Global Market (ADGM)’. (2019). http://amereller.com/wp-content/uploads/2019/06/190617_Bahrain-and-ADGM-Crypto-Exchange-Regulation.pdf
Hagan S, ‘Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT)-Report on the Review of the Effectiveness of the Program,’ (2011). https://www.imf.org/external/np/pp/eng/2011/051111.pdf Accessed Dec 11, 2022.
Harneys, ‘European Union: Adoption of the Fifth Anti-Money Laundering Directive’. (2018). https://www.harneys.com/media/1485/european-union-adoption-of-the-fifth-anti-money-laundering-directive.pdf
Helm T, Low A, and Townson J, ‘UK FinTech-State of the Nation’, 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/801277/UK-fintech-state-of-the-nation.pdf Accessed March 25, 2022.
His Majesty King Hamad bin Isa Al Khalifa, “Bahrain Economic Vision 2030,” Government of Bahrain, (2019), <https://www.bahrain.bh/wps/wcm/connect/38f53f2f-9ad6-423d-9c96-2dbf17810c94/Vision%2B2030%2BEnglish%2B%28low%2Bresolution%29.pdf?MOD=AJPERES. > Accessed Dec 1, 2022.

HM Government and UK Finance,' Economic Crime Plan 2019-22', Jul 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/816215/2019-22_Economic_Crime_Plan.pdf Accessed March 25, 2022.
HM Government, 'A New Approach to Financial Regulation: Consultation on Reforming the Consumer Credit Regime' (HM Treasury 2010). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/81289/consult_consumer_credit211210.pdf Accessed March 25, 2022.
HM Government. 'CONTEST, The United Kingdom's Strategy for Countering Terrorism'. (2018). Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf Accessed on January 29, 2021.
HM Government. Report of the Commission to Consider Legal Procedures to Deal with Terrorist Activities in Northern Ireland. (London, 1972).
HM Parliament. 'Post-legislative Scrutiny of the Counter-Terrorism Act 2008'. (2014). Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/291925/Cm_8834_Print_Ready.pdf Accessed on January 29, 2021.
HM Treasury and EY, 'UK FinTech: On the Cutting Edge: An Evaluation of the International FinTech Sector', (2016). https://euagenda.eu/upload/publications/untitled-107589-ea.pdf Accessed Dec 7, 2022.
HM Treasury, 'Amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 Statutory Instrument 2022', (Jul 2021), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1004603/210720_SI_Consultation_Document_final.pdf.
HM Treasury, 'Anti-Money Laundering and Counter-Terrorism Financing: Supervision Report 2019-2020', Nov 2021. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1034539/HMT_Supervision_Report_19-20.pdf Accessed March 25, 2022.
HM Treasury, 'Consultation on the Fifth Money Laundering Directive: Response To The Consultation' (Jan 2020),

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/860491/5MLD_Consultation_Response.pdf Accessed March 25, 2022.
HM Treasury, 'National risk assessment of money laundering and terrorist financing 2020' (2020),https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/945411/NRA_2020_v1.2_FOR_PUBLICATION.pdf > Accessed Dec 1, 2022.
HM Treasury, 'National Risk Assessment of Money Laundering and Terrorist Financing 2020', (Dec 2020),
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/945411/NRA_2020_v1.2_FOR_PUBLICATION.pdf Accessed March 25, 2022.
HM Treasury, 'Transposition of the Fifth Money Laundering Directive: Consultation', (2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/795670/20190415_Consultation_ontheTransposition_of_5MLD_web.pdf Accessed March 25, 2022.
HM Treasury, 'UK Regulatory Approach to Cryptoassets and Stablecoins: Consultation and Call for Evidence' (2021).
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950206/HM_Treasury_Cryptoasset_and_Stablecoin_consultation.pdf Accessed March 25, 2022.
HMRC, 'Corporate Report: HMRC Anti-Money Laundering Supervision Annual Assessment', (Mar 2021). https://www.gov.uk/government/publications/hmrc-anti-money-laundering-supervision-performance-assessment/hmrc-anti-money-laundering-supervision-annual-assessment Accessed March 25, 2022.
HMRC, 'Tacking Tac Evasion: Government Guidance for the Corporate Offenses of Failure to Prevention the Criminal Facilitation of Tax Evasion', (Sep 2017)
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/672231/Tackling-tax-evasion-corporate-offences.pdf Accessed March 25, 2022.
Home Office. 'Counter Terrorist Finance Strategy'. (June 5, 2013).
Home Office. 'Legislation Against Terrorism – A Consultation Paper'. (1998). para 6.14. Available at
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/265689/4178.pdf Accessed on January 29, 2021.

Houben, R., and Snyers A., 'Cryptoassets: Key Developments, Regulatory Concerns and Responses'. (2020). https://www.blockchainwg.eu/wp-content/uploads/2020/05/IPOL_STU2020648779_EN.pdf

Houben, R., and Snyers, A., 'Cryptocurrencies and Blockchain: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion'. (2018). https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf

House of Commons Treasury Committee, 'Economic Crime-Eleventh Report of Session 2021-22', (Jan 2022). https://committees.parliament.uk/publications/8691/documents/88242/default/ Accessed March 25, 2022.

House of Commons, 'Cryptoassets-Twenty-Second Report of Session 2017-19'. https://publications.parliament.uk/pa/cm201719/cmselect/cmtreasy/1845/1845.pdf

House of Commons, 'Government and Financial Conduct Authority Responses to the Committee's Twenty-Second Report: Crypto-assets'. (2019). https://publications.parliament.uk/pa/cm201719/cmselect/cmtreasy/1845/1845.pdf

Humaidan K, 'Bahrain Fintech Ecosystem Report 2022'. https://30402333-6bc3-4539-9672-6f0d4f7f6ead.usrfiles.com/ugd/304023_bb24749371464f7986c1b0e08dad5899.pdf > Accessed November 25, 2022.

Humaidan K, and Al Sharaf Y, 'Bahrain FinTech Ecosystem Report 2022', (2022). https://theblockchaintest.com/uploads/resources/Bahrain%20FinTech%20bay%20-%20FinTech%20Ecosystem%20Report%20-%202022%20Feb.pdf.

Humud, C. E., Pirog, R., & Rosen, L. 'Islamic State Financing and U.S. Policy Approaches'. Congressional Research Service (CRS). (2015). Available at https://www.fas.org/sgp/crs/terror/R43980.pdf Accessed on January 29, 2021.

IMF Country Report. 'Kingdom of Bahrain: Detailed Assessment on Anti-Money Laundering and Combating the Financing of Terrorism'. (2005). Available at https://www.imf.org/external/pubs/ft/scr/2007/cr07134.pdf Accessed on January 29, 2021.

IMF, 'Kingdom of Bahrain: Detailed Assessment on Anti-Money Laundering and Combating the Financing of Terrorism', (2007), https://www.imf.org/external/pubs/ft/scr/2007/cr07134.pdf > Accessed Dec 29, 2022.

IMF, 'Kingdom of Bahrain: Financial System Stability Assessment,' (2006). https://www.imf.org/external/pubs/ft/scr/2006/cr0691.pdf

Impact Assessment, 'Transportation of the Fifth Anti-Money Laundering Directive', (Oct 2019), https://www.legislation.gov.uk/ukia/2019/172/pdfs/ukia_20190172_en.pdf Accessed March 25, 2022.

International Monetary Fund (IMF). 'Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT)'. IMF Program Document, Topical Trust Fund. (2009). Available at https://www.imf.org/external/np/otm/2009/anti-money.pdf Accessed on January 29, 2021.

Jenik I, and Duff S, 'How to Build a Regulatory Sandbox: A Practical Guide for Policy Makers' (2020). https://www.cgap.org/sites/default/files/publications/2020_09_Technical_Guide_How_To_Build Regulatory_Sandbox.pdf Accessed August 25, 2021.

Jenkins, B. M. *The New Age of Terror*. Rand Corporation. (2006). Available at https://www.rand.org/content/dam/rand/pubs/reprints/2006/RAND_RP1215.pdf Accessed on January 29, 2021.

Kalifa R, 'Kalifa Review of UK FinTech', (2021), https://www.skadden.com/-media/Files/Publications/2021/03/The-Kalifa-Review/KalifaReviewofUKFintech.pdf > Accessed Dec 1, 2022.

Keating T and Others, 'No Rest for the Wicked: Driving Change in the UK's Post-FATF Evaluation-AML Regime', (2019), https://static.rusi.org/20190219_fatf_uk_evaluation_web.pdf> Accessed Dec 5, 2022.

Keatinge, T. *The Role of Finance in Defeating Al-Shabaab*. Whitehall Report, 2-14. (2014). Available at https://rusi.org/sites/default/files/201412_whr_2-14_keatinge_web_0.pdf Accessed on January 29, 2021.

Keatinge, T., and Keen, F. 'Social Media and Terrorist Financing: What Are the Vulnerabilities and How Could Public and Private Sectors Collaborate Better?' (2019). Available at https://rusi.org/sites/default/files/20190802_grntt_paper_10.pdf Accessed on January 29, 2021.

Keatinge, T., Carlisle, D., and Keen, F. 'Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating Responses'. (2018). Available at https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf Accessed on January 29, 2021.

Kirschenbaum, J., and Veron, N., 'A Better European Union Architecture to Fight Money Laundering. 9. Policy Contribution. (2018). https://www.bruegel.org/wp-content/uploads/2018/10/PC-19_2018-241018_.pdf

KPMG, 'Beyond Basel IV: Incorporating Cryptoassets into the Basel Framework. (2019). https://assets.kpmg/content/dam/kpmg/ca/pdf/2020/03/basel-iv-crypto-en.pdf

KPMG, 'FinTech Focus: UK (2020) ', https://assets.kpmg/content/dam/kpmg/uk/pdf/2020/07/fintech-pulse-report-2020.pdf > Accessed November 30, 2022.

KPMG, 'FinTech: Transforming-Financial Services in the UK', (2019), <https://www.innovatefinance.com/wp-content/uploads/2019/09/kpmg-fintech-transforming-financial-services-in-the-uk.pdf >Accessed Nov 30, 2022.

KPMG, "Anti-Money Laundering Sanctions Update" (2020). https://assets.kpmg/content/dam/kpmg/my/pdf/kpmg-newsletter-anti-money-laundering-6.pdf Accessed August 28, 2021.

Law Commission, 'Anti-Money Laundering: The SAR Regime', (2019). <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2019/06/6.5569_LC_Anti-Money-Laundering_Report_FINAL_WEB_120619.pdf > Accessed Dec 17, 2022.

Law Commission, 'Anti-Money Laundering: the SARs Regime Consultation Paper' Consultation Paper No 236 (20 July 2018). https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2018/07/Anti-Money-Laundering-the-SARS-Regime-Consultation-paper.pdf Accessed March 25, 2022.

Mackintosh, K., and Duplat, P. 'Study of the Impact of Donor Counter-Terrorism Measures on Principled Humanitarian Action', United Nations Office for the Coordination of Humanitarian Affairs, 2013. Available at < https://www.nrc.no/globalassets/pdf/reports/study-of-the-impact-of-donor- counterterrorism-measures-on-principled-humanitarian-action.pdf >Accessed on January 29, 2021

Maguire A, 'Cryptoassets-Obtaining English Freezing and Proprietary Injunctions in Relation to Cyberfraud', (2020). https://littletonchambers.com/wp-content/uploads/2020/10/Cryptoassets-AMG-Oct-2020.pdf Accessed March 25, 2022.

Maxwell N J, 'Expanding the Capability of Financial Information-Sharing Partnerships', (2019), https://www.future-

fis.com/uploads/3/7/9/4/3794525/pr%C3%A9cis_of_ffis_paperexpanding_the_role_of_fisps_-_march_2019.pdf Accessed March 25, 2022.

MENAFATF, 'Anti-Money Laundering and Counter Terrorist Financing Measures: Kingdom of Bahrain Mutual Evaluation Report'. (2018).

MENAFATF, 'Coronavirus Pandemic (COVID-19) and its Impact on AML/CFT Systems in the Middle East and North Africa Region' (2020). http://www.menafatf.org/information-center/menafatf-publications/coronavirus-pandemic-covid-19-and-its-impact-amlcft-systems Accessed August 30, 2021.

MENAFATF, 'Mutual Evaluation Report of the Kingdom of Bahrain on Anti-Money Laundering and Combating Financing of Terrorism' (2006). http://www.menafatf.org/information-center/menafatf-publications/mutual-evaluation-report-kingdom-bahrain-anti-money Accessed August 30, 2021.

MENAFATF, 'Mutual Evaluation Report, 4th Follow-Up Report for Bahrain: Anti-Money Laundering and Combating the Financing of Terrorism' (2012). http://www.menafatf.org/information-center/menafatf-publications/fourth-follow-report-bahrain Accessed August 30, 2021.

MENAFATF, 'Social Media and terrorism Financing', (2019). Available at <http://menafatf.org/sites/default/files/FINAL-TM-SF-en.pdf >Accessed on January 29, 2021

Milken Institute, 'Developing Bahrain and the UAE into FinTech Hubs'. (2019). https://milkeninstitute.org/sites/default/files/2019-10/Developing%20Bahrain%20and%20the%20UAE%20into%20FinTech%20Hubs%20-%20A%20Timeline%20of%20Activity_FINAL-102119.pdf

Mueller J, and Piwowar, M. S. 'The rise of Fintech in the middle east: An analysis of the emergence of Bahrain and the United Arab Emirates', (2019), https://milkeninstitute.org/sites/default/files/reports-pdf/FinTech%20in%20the%20Middle%20East-FINAL-121119_0.pdf > Accessed November 30, 2022.

Muller C, Suglia J and Liu B, 'Evolving Investment Management Regulation: Light at the End of the Tunnel' (2013). https://assets.kpmg/content/dam/kpmg/pdf/2013/06/EIMR-Light-at-the-end-of-the-tunnel-2013-KPMG.pdf Accessed August 30, 2021.

NCA, ‘Requesting a defence from the NCA under POCA and TACT UK Financial Intelligence Unit’ (2018), <https://service.betterregulation.com/sites/default/files/upload/2018-05/Requesting%20A%20Defence%20Under%20POCA%20TACT%20-%20v4%200.pdf > Accessed Dec 15, 2022.

NCA, ‘SARs Regime Good Practice: Frequently Asked Questions-Suspicious Activity Reports’, (2020), https://www.nationalcrimeagency.gov.uk/who-we-are/publications/462-sars-faq-july-2020/file Accessed Dec 15, 2022.

NCA, ‘UK Financial Intelligence Unit Suspicious Activity Reports (SARs) Annual Report, 2020’ (2020), https://www.nationalcrimeagency.gov.uk/who-we-are/publications/480-sars-annual-report-2020/file Accessed March 25, 2022.

NCA, ‘UK Financial Intelligence Unit: Suspicious Activity Reports-Annual Report 2020’, (2020). <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/480-sars-annual-report-2020/file > Accessed Dec 15, 2022.

OPBAS, ‘Office for Professional Body Anti-Money Laundering Supervision (OPBAS): Sourcebook for Professional body anti-money laundering supervision’, (2018), https://www.fca.org.uk/publication/opbas/opbas-sourcebook.pdf Accessed March 25, 2022.

others ‘Legal and Regulatory Considerations for Digital Assets’ (2020). https://www.jbs.cam.ac.uk/wp-content/uploads/2020/10/2020-ccaf-legal-regulatory-considerations-report.pdf Accessed March 25, 2022.

Owens L, ‘National strategic assessment of serious and organised crime 2018,’ (2018). https://www.nationalcrimeagency.gov.uk/who-we-are/publications/173-national-strategic-assessment-of-serious-and-organised-crime-2018/file Accessed Nov 20, 2022.

Peters, G. W., Panayi, E., and Chapelle, A., ‘Trends in cryptocurrencies and block chain technologies: a monetary theory and regulation perspective’ (2015). EY Global Financial Services Institute. 3, 1.

Pol, R. F., ‘Anti-money laundering: The world's least effective policy experiment? Together, we can fix it,’ (2020). Policy Design and Practice. 3, 76.

Prasad, E., ‘Central Banking in a Digital Age: Stock-Taking and Preliminary Thoughts. (2018). https://www.brookings.edu/wp-content/uploads/2018/04/es_20180416_digitalcurrencies.pdf

PWC, ‘In Depth: A Look at Current Financial Reporting Issues (2019). https://www.pwc.com/gx/en/audit-services/ifrs/publications/ifrs-16/cryptographic-assets-related-transactions-accounting-considerations-ifrs-pwc-in-depth.pdf

Saad K, ‘Bahrain FinTech Bay Manifesto 2020’. (2018). https://www.bahrainfintechbay.com/_files/ugd/304023_edcec280389e43a1ad0593c76b559fd6.pdf > Accessed November 25, 2022.

Sahay, R and Others, ‘The Promise of FinTech: Financial Inclusion in the Post Covid-19 Era’. No 20/09. (Washington, IMF Library, 2020).

Sprenger P, and Balsiger F, ‘Anti-Money Laundering in Times of Cryptocurrencies: Cryptocurrencies—Game Changers in Many Ways’ (2018). https://assets.kpmg/content/dam/kpmg/ch/pdf/anti-money-laundering-in-times-of-cryptocurrency.pdf Accessed August 25, 2021.

Stroligo K, Hsu C-H, and Kouts T, ‘Financial Intelligence Units Working with Law Enforcement Authorities and Prosecutors’, (2018), https://star.worldbank.org/sites/default/files/fius-report-04-sk1.pdf > Accessed Dec 3, 2022.

The Central Bank of Bahrain and Financial Institutions Law. https://www.cbb.gov.bh/wp-content/uploads/2018/12/THE_CENTRAL_BANK_OF_BAHRAIN_AND_FINANCIAL_INSTITUTIONS_LAW_ENGLISH.pdf Accessed August 30, 2021.

The Law Library of Congress. ‘Regulation of Cryptocurrency Around the World’. (2018). https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf

The Law Library of Congress. ‘Regulatory Approaches to Cryptoassets in Selected Jurisdictions’. (2019). https://www.loc.gov/law/help/crypto-assets/crypto-asset-regulation.pdf

The Report, ‘Capital Markets Overview: Bahrain Bourse-An Oasis of Investment Opportunities (2020).https://bahrainbourse.com/resources/files/Thought%20Leadership/OBG_05BH20_Capital%20Markets.pdf > Accessed Dec 12, 2022.

Tritt L, ‘Legislative Approaches to Trust Arbitration in the United States: Arbitration of Internal Trust Disputes: Issues in National and International Law’ (Oxford University Press, 2016, Forthcoming), University of Florida Levin College of Law Research Paper No. 16-48. Available at SSRN: http://dx.doi.org/10.2139/ssrn.2703989 Accessed August 25, 2021.

Turki, M and others, ‘The Regulatory Technology “RegTech”, and Money Laundering Prevention in Islamic and Conventional Banking Industry’ (2020), 6, Heliyon, 1.

UK Jurisdiction Taskforce, 'Legal Statement on Cryptoassets and Smart Contracts', (Nov 2019). https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf Accessed March 25, 2022.

UKFIU, 'Suspicious Activity Report (SAR) Glossary Codes and Reporting Routes', (2022), https://www.nationalcrimeagency.gov.uk/who-we-are/publications/597-sar-glossary-codes-and-reporting-routes-june-2022/file Accessed Dec 5, 2022.

UN Office on Drugs and Crime, 'Preventing Terrorist Acts: A Criminal Justice Strategy Integrating Rule of Law Standards in Implementation of United Nations Anti-Terrorism Instruments' (2006). https://www.unodc.org/pdf/terrorism/TATs/en/3IRoLen.pdf Accessed August 25, 2021

UNCAC, 'Report on the Meeting of the Ended Intergovernmental Working Group on Asset Recovery Held in Vienna on 29th and 30th May, 2019 (2019). https://www.unodc.org/documents/treaties/UNCAC/WorkingGroups/workinggroup2/2019-May-29-30/V1905966e.pdf Accessed August 30, 2021

United States Department of State, "Investment climate statement –Bahrain", Bureau of Economic and Business Affairs, (2015). <www.state.gov/e/eb/rls/othr/ics/2015/241473.html> Accessed August 30, 2021

Warrick, Thomas, and Joze Pelayo. Improving Counterterrorism and Law Enforcement Cooperation between the United States and the Arab Gulf States. Report. Atlantic Council, 2020. 56-65. Accessed August 20, 2021. http://www.jstor.org/stable/resrep26651.8

Zimmerman, P., 'Blockchain Structure and Cryptocurrency Prices. Staff Working Paper No. 855'. (2020). https://www.bankofengland.co.uk/-/media/boe/files/working-paper/2020/blockchain-structure-and-cryptocurrency-prices.pdf

Conference proceedings

De Figueirdo, R. and Weingast, B. 'Vicious Cycles: Endogenous Political Extremism and Political Violence'. (2001). Institute of Governmental Studies Working Paper, 2001-9.

Farrugia F, Ellul J, and Azzopardi G, 'Detection of Illicit Accounts over the Ethereum Blockchain. (2020), 1, Expert Systems with Applications' 150. https://doi.org/10.1016/j.eswa.2020.113318.

UNSGSA FinTech Working Group and CCAF, 'Early Lessons on Regulatory Innovations to Enable Inclusive FinTech: Innovation Offices, Regulatory Sandboxes, and RegTech. Office of the UNSGSA and CCAF', (New York, NY and Cambridge, UK, 2019).
Yordan, Carlos L., 'Enacting Counter Terrorism Financing Laws in the UAE and Bahrain: The Fusion of Global Pressures, Regional Dynamics, and Local Interests' (2008). Mediterranean Programme, European University Institute Workshop No. 6, Florence

Theses

Aljawder, A A., 'Uniform Anti Money Laundering Policy and Laundering Process Eradication', Brunel University PhD Thesis. (2018).
https://bura.brunel.ac.uk/bitstream/2438/18208/1/FulltextThesis.pdf Accessed August 30, 2021.
Almutawa, A. The Legitimacy of Counterterrorism Financing Measures in Bahrain with Reference to the United Kingdom. (PhD thesis, University of Leeds, 2019).
Alzubairi, F. 'Kuwait and Bahrain's Anti-Terrorism Laws in Comparative and International Perspective'. (2011). Available at
https://tspace.library.utoronto.ca/bitstream/1807/30158/6/Alzubairi_Fatemah_201107_Master_thesis.pdf Accessed on January 29, 2021.
Burton, M. "The Challenges of ISIS and the Modern Nation-State" (2016). Honors Theses. 126.
https://digitalworks.union.edu/theses/126
F. S. Sahin. 'Case Studies in Terrorism-Drug Connection: The Kurdistan Workers' Party, the Liberation Tigers of Tamil Elam, and the Shining Path'. Unpublished Master's Thesis. University of North Texas, Denton, 2001.
Modara M, 'The Influence of Government-Private Sector Collaboration On Innovation in A Developing Knowledge Economy: The Case of Bahrain' (2019) University of Bangkok PhD Thesis. http://dspace.bu.ac.th/bitstream/123456789/4122/1/marjan_moda.pdf Accessed August 27, 2021.

Webpages

Bambrough, B. 'As Bitcoin's Total Value Nears $1 Trillion, These Crypto Prices Are Leaving Bitcoin In The Dust' (Feb 2021). Available at

https://www.forbes.com/sites/billybambrough/2021/02/18/as-bitcoin-total-value-nears-1-trillion-these-crypto-prices-are-leaving-it-in-the-dust/?sh=62cf5d974689 Accessed on January 29, 2021.
BIS, 'Payment, clearing and settlement systems in the Kingdom of Bahrain' (2017), https://www.bis.org/cpmi/publ/d156.pdf Accessed November 25, 2022.
BoE, 'Joint Statement from UK Financial Regulatory Authorities on Sanctions and the Cryptoasset Sector – 11 March 2022'. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1060448/Statement_from_UK_authorities_on_Cryptoassets_-_March_2022.pdf Accessed March 25, 2022.
Bowler T, 'Countering Tax Avoidance in the UK: Which Way Forward?' (Feb 2009), https://ifs.org.uk/comms/dp7.pdf Accessed March 25, 2022.
Browne, R., 'Bitcoin Hits New All-time High Above $23,000, Extending its Wild 2020 Rally'. (December 2020). Accessed December 20, 2020 https://www.cnbc.com/2020/12/17/bitcoin-btc-price-hits-new-all-time-high-above-23000.html
Castillo, M., '$6Billion United Nations Agency Launches Bitcoin, Etherium Crypto Fund'. (2019). https://www.forbes.com/sites/michaeldelcastillo/2019/10/08/6-billion-united-nations-agency-launches-bitcoin-ethereum-crypto-fund/#3d33f9f7493b
CBB Rulebook, 'Enhanced Customer Due Diligence: Politically Exposed Persons ('PEPs'), Vol 6-Capital Markets,' (2022), https://cbben.thomsonreuters.com/rulebook/aml-15-enhanced-customer-due-diligence-politically-exposed-persons-peps> Accessed Dec 12, 2022.
Clautice, T., "Nation State Involvement in Cryptocurrency and the Impact to Economic Sanctions" (2019). Economic Crime Forensics Capstones. 43. https://digitalcommons.lasalle.edu/ecf_capstones/43
CPA Canada, 'Audit Considerations Related to Cryptocurrency Assets and Transactions'. (2018). http://klp.com.sg/files/Canada-CPA_audit-considerations_-related-to-cryptocurrency.pdf
Dabrowski, M., and Janikowski, L., 'Virtual Currencies and their Potential Impact on Financial Markets and Monetary Policy'. (2018). https://case-research.eu/files/?id_plik=5708
Davies, C. 'ISIS Suspect Jack Letts' Parents Found Guilty of Funding Terrorism'. (2019). Available at https://www.theguardian.com/uk-news/2019/jun/21/jack-letts-isis-suspect-parents-found-guilty-of-funding-terrorism-oxford-syria Accessed on January 29, 2021.

Deakin, D. R., 'Study Declares 95% of Reported Bitcoin Trading is Fake.' (2019). https://www.notebookcheck.net/Study-declares-95-of-reported-bitcoin-trading-is-fake.414981.0.html

Directives, 'Directive (EU) 2018/843 Of The European Parliament and of The Council'. (2018). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843

Durrant, S., Understanding the Nexus between Cryptocurrencies and Transnational Crime Operations. (2018). https://academicworks.cuny.edu/cgi/viewcontent.cgi?article=1070&context=jj_etds

Edwards, V. 'Indiana Mother Married to ISIS Extremist Who Moved Her Young Family to Syria is Sentenced to Six and a Half Years in Prison for Providing $30,000'. (2020). Available at https://www.dailymail.co.uk/news/article-8931709/Indiana-woman-sentenced-6-1-2-years-providing-30-000-assets-ISIS.html Accessed on January 29, 2021.

FATF (2012), 'High-Level Principles for the relationship between the FATF and the FATF-style regional bodies, updated February 2019', FATF, Paris, France (2019). Available at < www.fatf-gafi.org/publications/fatfgeneral/documents/high-levelprinciplesfortherelationshipbetweenthefatfandthefatf-styleregionalbodies.html >Accessed on January 29, 2021

FATF 'Best Practices on Beneficial Ownership for Legal Persons, FATF', Paris, (2019). Available at < www.fatf- gafi.org/publications/documents/beneficial-ownership-legal-persons.html >Accessed on January 29, 2021

FATF 'Global Money Laundering &Terrorist Financing Threat Assessment'. (2010). Available at <https://www.fatf-gafi.org/media/fatf/documents/reports/Global%20Threat%20assessment.pdf>Accessed on January 29, 2021

FATF, 'Best Practices on Beneficial Ownership for Legal Persons, FATF, Paris', (2019). Available at < www.fatf-gafi.org/publications/documents/beneficial-ownership-legal-persons.html >Accessed on January 29, 2021

FATF, 'FATF Guidance, Transparency and Beneficial Ownership' (2014). Available at < http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-transparency-beneficial-ownership.pdf

FATF, 'FATF Report to the G20, FATF, France,' (2020), Available at < www.fatf-gafi.org/publications/virtualassets/documents/report-g20-so-called-stablecoins-june-2020.html >Accessed on January 29, 2021

FATF, 'Financing of the terrorist organisation Islamic State in Iraq and the Levant (ISIL), FATF', (2015). Available at < www.fatf-gafi.org/topics/methodsandtrends/documents/financing-of-terrorist-organisation-isil.html >Accessed on January 29, 2021

FATF, 'Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites And Internet Payment Systems (2008)'. Available at < https://www.fatf-gafi.org/media/fatf/documents/reports/ML%20TF%20Vulnerabilities%20of%20Commercial%20Websites%20and%20Internet%20Payment%20Systems.pdf >Accessed on January 29, 2021

FID, 'The Annual Report of the Financial Intelligence Directorate,' (2022), https://www.bahrainfiu.gov.bh/mcms-store/magazine/en/Annual_Report/2021/index.html#1

FSA, 'Anti-Money Laundering Supervision by the Legal and Accountancy Professional Body Supervisors: Progress and Themes from Our 2020/21 Supervisory Assessments.' (2021). https://www.fca.org.uk/publication/opbas/supervisory-assessments-progress-themes-2020-21.pdf Accessed Nov 25, 2022.

FSA, "Anti-Money Laundering, Counter Financing of Terrorism, and Counter-Proliferation Financing" Current Status and Challenges' (2022), https://www.fsa.go.jp/en/news/2022/20221007/20221007.pdf Accessed Dec 29, 2022.

Herridge, C. 'ISIS Accused of Selling Fake PPEs Online to Finance Terrorism'. (2020). Available at https://www.cbsnews.com/news/isis-accused-of-selling-fake-ppe-online-to-finance-terrorism/ Accessed on January 29, 2021.

Hill, M. 'Bahrain Ultimate Beneficial Owner ("UBO") Rules Take Effect'. (2020). Available at https://www.charlesrussellspeechlys.com/en/news-and-insights/insights/corporate/2020/bahrain-ultimate-beneficial-owner-ubo-rules-take-effect/ Accessed on January 29, 2021.

Kirby, E. J. 'The City Getting Rich From Fake News'. (2016). Available at https://www.bbc.com/news/magazine-38168281 Accessed on January 29, 2021

Langat R, and Alhashemi M, 'Crypto markets: The Crypto-Asset Exchange ecosystem in Bahrain', (2022), <https://www.mondaq.com/fin-tech/1229550/crypto-markets-the-crypto-asset-exchange-ecosystem-in-bahrain > Accessed Dec 15, 2022.

Mogielnicki, R. ‘Bahrain and Abu Dhabi Compete to be Gulf’s Cryptocurrency Hub. The Arab Gulf States Institute in Washington’, (2019), <https://agsiw.org/bahrain-and-abu-dhabi-compete-to-be-gulfs-cryptocurrency-hub > Accessed Dec 20, 2022.

Murphy A, ‘The Investigator-Centred Approach to Financial Crime: Doing What Matters’, (2020), https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-investigator-centered-approach-to-financial-crime-doing-what-matters Accessed March 25, 2022.

Nagajaran, S., ‘Bitcoin’s, Market Cap Could Hit $1 trillion in 2021 as its growing Reserve Currency Status Drives Adoption Higher. (December 2020). Accessed December 20, 2020 https://africa.businessinsider.com/markets/bitcoins-market-cap-could-hit-dollar1-trillion-in-2021-as-its-growing-reserve/xhyxwgv

Nelson D, ‘Sanctioned Crypto Wallet Linked to North Korean Hackers Keeps Laundering’, (2022), <https://www.coindesk.com/tech/2022/04/15/sanctioned-crypto-wallet-linked-to-north-korean-hackers-keeps-on-laundering/ > Accessed Dec 25, 2022.

Reback S, ‘Binance's Bahrain License Upgraded for More Crypto Services’, (2022), <https://www.coindesk.com/business/2022/05/26/binances-bahrain-license-upgraded-for-more-crypto-services/ > Accessed Dec 12, 2022.

Salama, V. “As Territory Shrinks, ISIS Looks for New Money Sources,” (Seattle Times, October 19, 2016). Available at < https://www.seattletimes.com/nation-world/as-territory-shrinks-is-group-looks-for-new-money-sources/ >Accessed on January 29, 2021

Smith, A., and Vladimir, B., ‘Fake News: How a Partying Macedonian Teen Earns Thousands Publishing Lies’ (2016), Available at <https://www.nbcnews.com/news/world/fake-news-how-partying- macedonian-teen-earns-thousands-publishing-lies-n692451 >Accessed on January 29, 2021

Youssef N, ‘Digital Customer On-Boarding, e-KYC and Digital Signatures in The Arab Region, (2020)’. https://www.amf.org.ae/sites/default/files/Files/Digital%20Identy%20Booklet.pdf Accessed August 25, 2021

Others

Ehrentraud, J., and others. ‘FinTech and Payments: Regulating Digital Payments Services and e-Money’ (2021). https://www.bis.org/fsi/publ/insights33.pdf Accessed August 30, 2021.

Gelemerova, L, ‘On the frontline against money-laundering: the regulatory minefield’, (2009) 52 Crime Law Soc Change, 33–55.

IMF, “Economic diversification in oil-exporting Arab countries”, in Annual Meeting of Arab Ministers of Finance, Manama, Bahrain (2016). <www.imf.org/external/np/pp/eng/2016/042916.pdf> Accessed August 30, 2021.

Implementation Review Group, ‘Review of Implementation of the United Nations Convention Against Corruption’ (2019). https://www.unodc.org/documents/treaties/UNCAC/WorkingGroups/ImplementationReviewGroup/17-18December2019/V1910900e.pdf Accessed August 25, 2021.

Appendices

Appendix 1: Description of the FATF Standards

Standard	Description
Assessing risk and applying risk-based approach	The FATT provides a National Risk Assessment approach that guides countries for determining exposures to ML/TF risks. With over 12 criteria, the RBA offers a stringent criteria covering all operations that can be applied to cryptoassets.
National cooperation and coordination	The policies designed for national-level institutions, including ministries and departments are integral in ensuring domestic coordination and cooperation, which is necessary for the domestic use of cryptoassets.
Money Laundering offense	Money laundering offenses under cryptoassets guidelines include the concealment, arrangements and acquisition of cryptoassets for illegal purposes.
Confiscation and provisional measures	The country has measures to confiscate any property that is viewed as being used for illegal purposes, including money used in illegal cryptoassets operations.
Terrorist financing offence	The country has a robust terror financing legislation, whereby any conduct that is deemed to be used in terror financing is investigated thoroughly.
Targeted financial sanctions, terrorism and terrorist financing	Comprised of 7 criteria, the standard mirrors the provisions under UNSCR 1452, whereby freezing of assets is performed without delay
Targeted financial sanctions- Proliferation	The standard is based on 5 criteria, which primarily relate to the freezing of assets that are related to proliferation of cryptoassets, including assets that are directly/ indirectly owner or co-owned by the suspected individuals.
Non-profit organisations	Under the most recent review, 80% of the 380,000 institutions which lie under this category were reviewed. A public register is established for all these institutions.
Financial institution secrecy law	None of the financial secrecy laws can be employed to protect parties involved in the cryptoassets

Customer due diligence	Clear obligations and actions when the data related to customers is viewed as insufficient or incorrect.
Record keeping	Keeping of records of all transactions and retaining the data for the designated period
Politically exposed persons	Politically exposed persons are treated as targets for financial malfeasance, due to their position and power in policy making
Correspondent banking	Correspondent banking institutions in third-party countries have to follow specific guidelines in order to avoid certain exposures to cyber assets threat
Money or value transfer services	Supervision of activities whereby money or valuable items are transferred, with sufficient sanctions for entities that contravene the guidelines
New technologies	The emergence of new technologies under Crypto markets present novel risks and exposures
Wire transfers	With over 18 criteria, the stand focuses on the prohibition of certain risky wire transfers, as well as extensive oversight on every transaction
Reliance on third parties	Third party transactions present certain challenges with identification of the parties, hence the need for increased vigilance
Internal controls and foreign branches and subsidiaries	Internal control measures designed to reduce the exposure due to poor operational management within the institutions, specifically with risks associated with cryptoassets
Higher risk countries	Transactions involving parties from higher-risk countries are taken through a more stringent oversight process. This is in response to the 4AMLD guidelines under MLRs
Reporting of suspicious transactions	Prompt handling and reporting of suspicious transactions in order to determine whether the is a need to take additional measures
Tipping-off and confidentiality	Sharing of information about potential risks between financial institutions has to be done, in spite of the presence of confidentiality clauses

DNFBPs[5]: Customer due diligence	Designated Non-Financial Business and Professions have to comply with the requirements for customer due diligence, since they can be used as the aperture for introduction of cryptoassets
DNFBPs: Other measures	These institutions have to take other measures that are not normally imposed, since they are not part of the financial sector, including screening the entities involved in their value chains
Transparency & BO[6] of legal persons	Transparency concerns arise when individuals with beneficial ownership can utilise their position to mask crypto asset transactions. This is especially relevant for legal persons, such as cryptoassets
Transparency & BO of legal arrangements	Legal arrangements involving cryptoassets offer parties to the transactions unique advantages and responsibilities that can be exploited, especially if they involve foreign entities
Regulation and supervision of financial institutions	Financial institutions are at the centre cryptoassets markets.
Powers of Supervision	The power of supervisory staff in the regulatory institutions, including the power to make decisions when supervising the cryptoassets sector
Regulation and supervision of DNFBPs	The regulation of DNFBPs, such as casinos is integral in ensuring that the financial sector is not adversely impacted by the introduction of cryptoassets to the country through other sectors.
Financial intelligence units	Financial intelligence units provide an additional source of information about cryptoassets, especially through the intelligence from National Crime Agency and Serious Organised Crime Agency.
Responsibilities of law enforcement and investigative authorities	The involvement of the police and other agencies involved in law enforcement is key in investigating crimes related to cryptoassets, such as physical theft

[5] Designated Non-Financial Business and Professions
[6] Beneficial ownership

Powers of law enforcement and investigative authorities	The law enforcement agencies must have the power to investigate crimes associated with cryptoassets, through training and provision of information on how to identify wrongdoing.
Cash couriers	Cash couriers, including those entering or leaving the country, or those travelling domestically, have to declare the purpose of the funds. Similarly, control over the quantities ensures that hard cash is not transported for use in crypto asset transactions later.
Statistics	Statistics under Suspicious Activity Reporting are necessary in order to enable the country to determine the most prominent exposures at any time
Guidance and feedback	Competent and responsible institutions have established reliable mechanisms for reporting their activities to all stakeholders involved in cryptoassets handling
Sanctions	The sanctions established by the country are sufficient and dissuasive enough to prevent individuals from engaging in the use of cryptoassets for illegal activities
International instruments	Signatory to international conventions such as the Vienna Convention[7], the Palermo Convention[8], the Terror Finance Convention[9] and the Merida Convention[10], specifically to control the use of cryptoassets for illegal activities
Mutual legal assistance	Legal assistance is available, especially when it comes to helping other countries to enforce certain laws, including International Cooperation Act of 2003 and External Requests and Orders of 2005.

[7] Also referred to as the Law of Treaties (VCLT) is an international agreement signed in 1969 but came into effect in 1980, regulating treaties between states. Known as the "treaty on treaties", it establishes comprehensive rules, procedures, and guidelines for how treaties are defined, drafted, amended, interpreted, and operate.

[8] The Palermo Convention, signed in 2000, is also referred to as the United Nations Convention against Transnational Organised Crime

[9] The Terror Financing Convention, signed in 1999, but came into effect in 2002, has 132 signatories, and criminalises acts associated with the financing of acts related to terrorism. The convention promotes the cooperation between the judicial and law enforcement agencies (police) in the prevention, investigation and punishment of the financing of terrorist activities.

[10] Also referred to as the United Nations Convention against Corruption, the Merida Convention is a legally binding international anti-corruption multilateral treaty, with 140 signatories, which became effective in 2005.

Mutual legal assistance, freezing and confiscation	Take expeditious measures in order to identify, freeze, sieve and confiscate property suspected to be used in illegal cryptoassets deals in collaboration with other countries
Extradition	Prompt extradition of individuals suspected to have broken crypto asset regulations in other countries, in order to ensure that all culprits are punished.
Other forms of international cooperation	A multiplicity of international cooperation, specifically designed to seal the loopholes that criminals involved in illegal activities involving cryptoassets can use

Appendix 2: Definition of the Typologies for Legislative Approaches

1. Actors	
Participation	Participation involves the criminalisation of participation in the organisation, thereby implying that individuals who are directly and indirectly (offenses that if committed would constitute a crime) involved in the institutions are liable under the law. For participation offenses, the individuals are required to have known about the offense, or proof of recklessness leading to lack of awareness about the offense.
Bribery and Corruption	Bribery and corruption offenses are targeted by legislation that seeks to stop widespread corruption, by targeting those who give, as well as those who receive the bribes. The legislative approach is designed to curtail the use of position by persons with power, to influence key decisions. The legislation eliminates high level corruption which is pervasive, and can lead to loss of confidence in the governance and judicial frameworks.
Sentence enhancement	Sentence enhancement is utilised in increasing the severity of the punitive measures for those involved in certain offenses. The legislative approaches involve identification of precipitating or special circumstances that warrant additional punishment.
2. Activities	
Enterprise crime offenses	Enterprise crimes focus on placing sanctions based on the activities of an organisation, instead of targeting individual persons. The measures promote individual liability, since in most cases, members of an organisation are often aware (or supposed to be aware) of the activities. The legislative approach is best suited for white collar client, and helps target the clientelistic links within such organisations. However, these legislative approaches are faced with a number of complexities. These laws provide law enforcement agencies with powers to investigate certain crimes, including the use of search warrants, interception of telecommunications and undercover investigations.

Law enforcement powers	
Coercive Investigation	Coercive investigative powers empower ad hoc institutions to investigate certain criminal activities that are not fully covered under the traditional LEAs. By abrogating certain privileges, individuals are given the powers to contravene certain laws, such as those against self-incrimination, with provisions for making agreements in order to get key testimonies.
3. Objectives	
Organisational proscription	Proscription is used to designate specific organisations as illegal, based on their characteristics or the activities they are involved in. The declarations are integral in laying down the foundation for preventing particular crimes, especially if the organisation is involved in planning, facilitation, support, or engagement in particular activities. The legal approaches are founded on the premise that organisations meeting such criteria will eventually get involved in criminal activities. Proscription is often linked to participation offenses. Under proscription, there is no need for intention to commit the crime, since liability is assessed dependent on the presence of a threat, thus making it possible for prevention of the specific crimes. In order to achieve the goals of proscription, the law has taken measures to define the particular issues prohibited under the law in a coherent manner, in order to demonstrate the contexts within which TF occurs.
Conspiracies	However, the laws increase the potential for prosecuting people for offenses not committed, as well as focusing on offenses
4. Structures	
Unlawful association	Legislative approaches leading to laws that outlaw certain associations are integral in preventing direct and indirect associations for the purpose of disrupting certain actions. Although similar to conspiracy laws, these laws prohibit the association with certain individuals, and establish blanket liability for individuals who associate with those illegal entities (legal and natural persons).
5. Impacts	

	Legislative approaches that focus on impacts seek to impose punishments or sanctions based on the impact of the act or potential act on society. The approach is best suited for victimless crimes, or crimes whose effects vary from one situation to another.
Economic harm	In Bahrain, this approach focuses on unexplained wealth as a way of bridging the gaps investigatory activities, especially for persons involved in certain activities as such as money laundering or terror finance. The legislative approach also seeks to prevent the persons from engaging in similar criminal activities, by taking away the means through which financed the activities through freezing.
Physical harm	The legislative approaches focus on tackling organisations based on the physical impacts of their actions, especially when similar substantive offenses exist. This include measures to punish the facilitation the activities of criminal groups. The legislative approaches feature provisions for joint commission, especially when targeting the more powerful members of the organisation, especially those who participated covertly. These measures are taken due to the fact that the physical harm from the actions can only be achieved through the participation of all members of the organisation. CTF in Bahrain entails considerations of the physical harm, specifically due to the outcomes of the attack, but fails to account the physical harm befalling individuals that were denied their services and entitlements due to the misuse of the financial system for the intended purposes. Similarly, the legal frameworks do not focus on the opportunity costs from the loss of reputation in the country…
Psychological impact	Psychological impacts involve the loss of reputation and intimidation that are imposed by criminal organisations on its victims. It is thus necessary to recognise this dimension of the harm. These legislative approaches focus on designing laws against intimidation of witnesses, or interference with investigative processes, which leads to subversion of justice.

Appendix 3: Summary of Contents of the CBB Rule Books Vol 1 to 7

CBB Rule Book Vol 1	**Introduction**	Users' Guide
	High Level Standards	Licensing Requirements
		Principles of Business
		High-level Controls
		Auditors and Accounting Standards
		General Requirements
	Business Standards	Business and Market Conduct
		Capital Adequacy
		CA Table of Contents
		Part 1: Definition of Capital
		Part 2: Credit Risk
		Part 3: Other Risks
		Credit Risk Management
		Operational Risk Management
		Financial Crime
		Prudential Consolidation and Deduction Requirements [was deleted in January 2015]
		Training and Competency
		Internal Capital Adequacy Assessment Process
		Stress Testing
		Domestic Systemically Important Banks

		Reputational Risk Management
		Liquidity Risk Management
		Digital Financial Advice
	Reporting Requirements	CBB Reporting Requirements
		Public Disclosure Requirements
	Enforcement & Redress	Compensation
		Enforcement
CBB Rulebook Vol 2	**Introduction**	Users' Guide
	High Level Standards	Licensing Requirements
		Principles of Business
		High-Level Controls
		Auditors and Accounting Standards
		General Requirements
		Shari ‘a Governance
	Business Standards	Capital Adequacy
		CA Table of Contents
		Part 1: Definition of Capital
		Part 2: Credit Risk
		Part 3: Other Risks
		Business and Market Conduct
		Risk Management
		Credit Risk Management

		Operational Risk Management
		Liquidity Risk Management
		Financial Crime
		Prudential Consolidation and Deduction [Deleted in January 2015]
		Training and Competency
		Internal Capital Adequacy Assessment Process
		Stress Testing
		Domestic Systemically Important Banks
		Reputational Risk Management
		Digital Financial Advice
	Reporting Requirements	CBB Reporting
		Public Disclosure
	Enforcement & Redress	Enforcement
		Compensation
CBB Rulebook Vol 3	**Introduction**	Users' Guide
	High Level Standards	Authorisation
		Principles of Business
		High Level Controls
		Auditors and Actuaries
		General Requirements
	Business Standards	Capital Adequacy
		Business and Market Conduct

		Client Money
		Risk Management
		Financial Crime
		Training and Competency
		Insurance Aggregators
	Reporting Requirements	CBB Reporting
		Public Disclosure
	Enforcement & Redress	Enforcement
		Compensation
	Sector Guides	Captive Insurance
		Insurance Intermediaries and Managers
		Takaful / Retakaful
CBB rulebook Vol 4	**Introduction**	Users' Guide
	High level Standards	Authorisation
		Principles of Business
		High Level Controls
		Auditors and Accounting Standards
		General Requirements
	Business Standards	Capital Adequacy
		Business and Market Conduct
		Client Assets
		Risk Management

		Financial Crime
		Training and Competency
		Digital Financial Advice
	Reporting Requirements	CBB Reporting
		Public Disclosure
	Enforcement & Redress	Enforcement
		Compensation
	Sector Guides	Category 1 licensees
		Category 2 licensees
		Category 3 licensees
		Islamic Investment Firms
CBB Rulebook Vol 5	**Introduction**	Users' Guide
	High Level Standards	Principles of Business
		Auditors and Accounting Standards
	Business Standards	Financial Crime
	Enforcement & Redress	Enforcement
CBB Rulebook Vol 6	**Introduction**	Users' Guide
		Executive summary
	Institutions	Markets and Exchanges
		Clearing, Settlement and Depository
		Market Intermediaries and Representatives
		Crypto-Asset

	Collective Investment Undertakings	[Replaced by Volume 7 in April 2012]
	Market Standards	Offering of Securities
		Take-overs, Mergers and Acquisitions
		Prohibition of Market Abuse and Manipulation
		Market Surveillance, Investigation & Enforcement
		Anti-Money Laundering & Combating Financial Crime
	Ongoing Obligations	Listing Requirements
		Disclosure Requirements
	High Level Standards	High-Level Controls (Corporate Governance)
	Dispute Resolution and Investor Protection	Dispute Resolution, Arbitration and Disciplinary Proceedings
	International Co-operation	International Co-operation & Exchange of Information
CBB Rulebook Vol 7	Introduction	User guide
	High Level Standards	Authorisation / Registration Requirements
		Relevant Persons
		Corporate Governance
		Liquidation / De-registration Requirements
	Classification of Undertakings	Bahrain Domiciled Retail CIUs
		Bahrain Domiciled Expert CIUs

		Bahrain Domiciled Exempt CIUs
		Bahrain Domiciled Real Estate Investment Trusts (B-REITs)
		Overseas Domiciled CIUs
		Shari'a Compliant CIUs
		Private Investment Undertakings
	Reporting Requirements	CBB Reporting
	Enforcement & Redress	Enforcement

Appendix 4: Minimum Capital Requirements for CPO licensees

Category	Specific Digital assets provided	Obligations of authorised licensees
1(BHD 25,000)	• Receiving and transmitting orders • Providing investment advice concerning accepted cryptoassets	• Not allowed to hold client's assets or money • Refrain from charging fees or commissions from parties other than their clientele • Not allowed to operate a crypto-asset exchange
2 (BHD 100,000)	• Trade-in accepted crypto asset as an agent • Management of digital asset portfolios • Custody of cryptoassets • Providing investment advise	• Not allowed to deal as a principal, from their account, but can act as an agent.
3 (BHD 200,000)	• Trade-in accepted crypto asset as an agent • Trade-in accepted crypto asset as a principal • Management of digital asset portfolios • Custody of cryptoassets • Providing investment advise	• Allowed to hold/ control digital assets belonging to clients and deal as a principal • However, cannot operate a crypto-asset exchange
4 (BHD 300,000)	• Operating a licenced crypto-asset exchange • Custody of cryptoassets	• Restricted from executing orders from clients against proprietary capital or engaging in matched principal trading.

Appendix 5: Roles of Institutions under UK's AML Regime

Primary Objective	Activities	Key Institution(s)
1. Understanding the threat and performance metrics	Collective threat assessment	NAC, NECC, UK Finance, LSAG, AASG, HMT, Home Office
	Creating fully operational performance systems to determine what works	Home Office, UK Finance, NECC, JFT
	Perform NRAs	HMT, Home Office
	Resolving evidence gaps through long-term research strategies	HMT, Home Office, Ministry of Justice
2. Better information sharing	Review barriers to effectiveness	HMT, Home Office, NECC, UK Finance, LSAG, AASG
	Promote information sharing among institutions	HMT, Home Office
	Implementing the JMLIT model	HMT, NECC
	Improvement effectiveness of JMLIT model	UKFIU, OPBAS, LSAG, AASG, NECC
	Promote information sharing on Fraud	Home Office
3. Procedures, Powers and Tools	Implement action plan for recovering of assets	Home Office, LEA
	Propose legislative changes to primary and secondary legislation	Home Office
	Transposition of 5MLD	HMT
	Implement recommendations on Disclosure Review	CPS, AGO, NPCC
	Introduction of tactical targeting orders	HMT, UKFIU, Home Office

	Creating framework for repatriation of the funds	Home Office, UK Finance
	Clarify powers of sanctions supervisors	HMT, LSAG, AASG
	Review of how criminals abuse the UK Market	HMT, FCA
	Determine how to block from UK Market	HMT
4. Enhanced Capabilities	Enhancement of the role of NECC in line with the JMLIT model	NECC
	Enhance capabilities for AML/CTF	NECC, UK Finance, Cabinet Office
	Develop action plans for PPP against economic crimes	HMT, UK Finance, Home Office, NECC
	Create resources model for economic crime reforms	Home Office, UK finance, Cabinet Office, NCA, HMT
	Launch economic crime courts	HM Courts and Tribunal Services, Ministry of Justice
	Develop ways for using payment systems to tackling economic crimes	FCA, PSR, HMT, UK Finance, BoE
	Enhance LEA response to Fraud	Home Office, City of London Police, NECC
	Enhance support for victims of economic crimes	Home Office
	Seal vulnerabilities used by Fraudsters	JFT
	Develop professional counter fraud systems	Cabinet Office
	Deliver the digitised design for SARs	SARs Transformation Program, NRA, Home Office, HMT

	Enhance utility of SARs for prevention of economic crimes	SARs Transformation Program, UKFIU, Home Office
	Ensure SARs are confidential	Home Office, UKFIU, HMT
5. Risk-based supervision and management of risks	Review MLRs and OPBAS regulations	HMT
	Enhance engagement and supervision of FCA	FCA
	Enhance HMRC supervision	HMT, OPBAS, HMRC
	Enhance consistency of AML/CTF supervision	OPBAS for accountancy and legal institutions
	Position FCA as supervisor for AML/CTF regime for cryptoassets	FCA
	Support innovations for regulatory compliance	FCA, HMT, Home Office, UK Finance
	Enhancing holistic response to economic crimes at institutional level	UK Finance
	Promote digital CDD	HMT, JMLSG, HMRC, LSAG
	Education and awareness creation of threats from economic crimes	UK Finance, NECC, LSAG, AASG, Home Office
6. Ensuring transparent ownership of businesses	Reformation of company's house	BEIS
	Requirements for reports for discrepancies in beneficial ownership information	HMT
	Enhance transparency of overseas ownership	BEIS
7. International Strategy	Enhance the understanding of the characteristics of international threat	UKFIU, NECC

	Cooperation for achievement of international standards	Home Office, UK Finance, HMT, FCDO, Government Digital Services
	Enhance foreign capabilities	FCA, Home Office, HMRC, HMT, OPBAS, NECC, UKFIU, Cabinet Office
	Enhance ability for investigation and prosecution of foreign crimes	NCA, CPS, FCDO
	Promoting integrity in international business activities	FCDO
8. Governance and PPP	Review the governance of economic crimes	HMT, Home Office
	Create stronger PPPs	HMT, Home Office, UK Finance, LSAG, AASG
	Enhance participation of civil society	HMT, Home Office