NEW TECHNOLOGY FOR OLD CRIMES? THE ROLE OF CRYPTOCURRENCIES IN CIRCUMVENTING THE GLOBAL ANTI-MONEY LAUNDERING REGIME AND FACILITATING TRANSNATIONAL CRIME

by

Ijeamaka Elizabeth Anika

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF

THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF LAWS

in

The Faculty of Graduate and Postdoctoral Studies

THE UNIVERSITY OF BRITISH COLUMBIA

(Vancouver)

May 2019

The following individuals certify that they have read, and recommend to the Faculty of Graduate and Postdoctoral Studies for acceptance, the dissertation entitled:

New Technology for Old Crimes? The Role of Cryptocurrencies in Circumventing the Global Anti-Money Laundering Regime and Facilitating Transnational Crime

submitted by Ijeamaka Elizabeth Anika in partial fulfillment of the requirements for

the degree of Master of Laws

in Law

Examining Committee:

Benjamin Perrin, Law
Supervisor

Graham Reynolds, Law
Supervisory Committee Member

Abstract

The phenomenon of transnational crimes such as money laundering, drug trafficking, and terrorist financing remains a persistent problem for the international community and for individual states. Though existing efforts to combat transnational crimes are by no means perfect, the recent iteration of financial technology – cryptocurrencies – presents a potential alternative means for circumventing the regulatory measures that inhibit transnational crimes. Most features of traditional banking facilities are absent in cryptocurrencies: transactions therein are considered to be relatively anonymous, cryptocurrencies are also decentralized, and their use lacks any formal oversight. Thus, cryptocurrencies could be considered a further complication to the already challenging problem faced by regulatory and enforcement agencies in striving to combat transnational crimes.

To date, the degree to which cryptocurrencies remain susceptible to exploitation for criminal purposes is still the subject of much debate. Therefore, this thesis will contribute to this ongoing conversation by examining the extent to which the use of cryptocurrencies facilitates transnational crimes and in turn circumvent the existing global anti-money laundering (AML) regime. Using a New Legal Realism theoretical lens, this thesis interrogates how the complex international AML framework could be interpreted, in the first instance, to apply to cryptocurrency-facilitated money laundering. This thesis also provides an overview of cryptocurrencies using Bitcoin as a case study. Given the emerging nature of cryptocurrencies, Bitcoin, as the first fully developed and widely used cryptocurrency network, is used to highlight the operating systems of cryptocurrencies.

Furthermore, this work draws from the criminological discipline to explain the attractiveness of cryptocurrencies for money laundering to facilitate transnational crime. Relying on a number of criminological theories, this thesis demonstrates the importance of regulating cryptocurrencies

while the problem of its illicit use is still at a nascent stage. In this case cryptocurrencies, in the absence of cohesive regulation, could become attractive to criminals seeking alternative avenues to launder the proceeds of their crimes. Thus, this thesis contributes original insights to the discussion of new techniques for facilitating transnational crimes by demonstrating through interpretation, how cryptocurrencies could be brought within the application of the existing AML regime as it is.

Lay Summary

Cryptocurrencies, such as Bitcoin, continue to gain mainstream public awareness. They are increasingly viewed as an alternative non-denominated ‘currency’ operating according to their own rules. At the same time, cryptocurrencies are notable for the instances where it has been used to facilitate criminal activity beyond domestic borders: money laundering, drug trafficking, terrorist financing, to name a few. Existing regulatory mechanisms for transnational crimes do not explicitly contemplate the use of cryptocurrencies for perpetrating transnational crimes including money laundering. Therefore, this thesis will examine the extent to which cryptocurrencies are able to facilitate transnational crimes and circumvent the existing global anti-money laundering regime. Following this, this work also demonstrates how cryptocurrencies could be brought within the existing AML regime.

Preface

This thesis is the original, unpublished, independent work of Ijeamaka Elizabeth Anika.

Table of Contents

List of Abbreviations

AML	Anti-Money Laundering
BTC	Bitcoin
CDD	Customer Due Diligence
CFT	The Convention on Financing of Terrorism
DATA	Digital Asset Transfer Authority
FATF	Financial Action Task Force
FinTech	Financial Technology
FINTRAC	Financial Transactions and Reports Analysis Centre of Canada
FIU	Financial Intelligence Units
IGCI	Interpol Global Complex for Innovation
IMF	International Monetary Fund
Interpol	The International Police Organization
KYC	Know Your Customer
MLA	Mutual Legal Assistance
NLR	New Legal Realism
OECD	Organization for Economic Co-operation and Development
TOR	The Onion Router
UNCAC	United Nations Convention Against Corruption
UNCTOC	United Nations Convention on Transnational Organized Crime
UNODC	United Nations Office on Drug and Crime
UNSC	United Nations Security Council

Acknowledgements

I am deeply indebted to Benjamin Perrin and Graham Reynolds, whose advice, comments, and support during the past year have been invaluable to the completion of this thesis and the LLM in general. I am also grateful for the generous financial support provided by Peter A. Allard School of Law Graduate Scholarship, UBC International Tuition Award, the University of Nigeria Nsukka, and Tenece Professional Services. I am also grateful to the faculty and staff of the Peter A. Allard School of Law, especially Graduate Program Advisor, Joanne Chung, and Associate Dean Karin Mickelson. Your incisive counsel means a lot to me. My gratitude also goes to Professor Obiora Okafor, who is always ready with advice and support.

During my time here in Vancouver, I have met so many wonderful people. I am particularly grateful to Anuli Uzozie, and her family, who have become family. To the staff of Raven, Osprey, and Chee in a Tree, thank you for going beyond the call of duty to support us. My thanks also go to Dominika Wiesner and Molly Joeck, my ever supportive friends and fellow Allard Graduate students.

Thank you to my family and friends for their boundless support, both financially and emotionally. In particular, my parents and siblings (the Nnaji and Anika families), whose love and laughter has sustained me. To Mrs. Carol Anika, you remain evergreen in my mind and I have missed you through highs and lows of this journey. Special gratitude to my brother, 'Uncle Chuma': thank you for inspiring this work, for your presence here in Vancouver, and your endless support. To my delightfully fearless Dilinna, who continues to inspire me to be bold and gives me many reasons to smile every single day. You are my best girl and I love you.

Most of all, to Nnamdi Anika: thank you for your unwavering belief in my abilities and for your incredible support in this adventure. I love you more each day.

And finally, to God Almighty, I thank You for the strength You give to me each day to keep going. Through Your abundant Grace, You continuously show me that Your hand is upon me and I am forever grateful.

Dedication

For Nnamdi and for Dilinna.

Chapter 1: Introduction

"In Just Two Decades, Technology Has Become A Cornerstone of Criminality".[1]
– Yury Fedotov, Executive Director, United Nations Office of Drug and Crime

"[...] the link between virtual currencies/crypto-assets and other predicate crimes appears to be growing." [2]
– Financial Action Task Force Report to G20 Finance Ministers and Central Bank Governors

1.1 Research Overview

The use of cryptocurrencies, such as Bitcoin, for financial transactions is steadily gaining momentum in the virtual and real world. To date, the extent to which cryptocurrencies remain susceptible to exploitation for criminal purposes is still the subject of much debate. Within the context of criminality, specific concerns have been raised regarding cryptocurrencies including its use in laundering the proceeds of transnational crimes by exploiting the 'anonymity' feature associated with cryptocurrency use.

Cryptocurrencies have also been said to benefit society in a number of ways, such as in minimizing the costs incurred in conducting transactions, especially with overseas transfer of funds are minimized. Its structure is such that the use of middlemen such as brokers, agents, legal representatives, certain complications and costs associated with traditional banking services are avoided.[3] Cryptocurrencies also create more access to facilities for banking and financial transactions for a huge populace who do not have access to traditional banking methods or prefer

1 Yury Fedotov, "In Just Two Decades, Technology Has Become a Cornerstone of Criminality (23 October 2017), online (blog): *The Huffington Post* <http://www.unodc.org/unodc/en/frontpage/2017/October/in-just-two-decades--technology-has-become-a-cornerstone-of-criminality.html>

2 FATF, FATF Report to G20 Finance Ministers and Central Bank Governors (Paris: FATF, July 2018) online: *FATF* <www.fatf-gafi.org/publications/fatfgeneral/documents/report-g20-fm-cbg-july-2018.html>.

3 The Commonwealth, *Commonwealth Working Group on Virtual Currencies: Working Group Report* (London: Commonwealth, 2015); Nicholas Godlove, "Regulatory Overview of Virtual Currency" (2014) 10 *Oklahoma Journal of Law and Technology* 1 at 13. William J. Luther and Lawrence H. White, "Can Bitcoin Become a Major Currency?" (5 June 2014), GMU Working Paper in Economics No. 14-17, online: SSRN <https://ssrn.com/abstract=2446604>.

not to use them. This is because all that is required to access the Bitcoin network is access to the Internet.[4]

For its benefits and emerging concerns over its potential drawbacks in creating an alternative financial transacting system, crypto-currencies have become the subject of significant public and regulatory interest.[5] They are increasingly viewed as an alternative non-denominated 'currency' operating under their own technological parameters.[6] However, unlike traditional currencies (e.g. the Canadian Dollar or the British Pound) that operate within a legislative framework both internationally and at the domestic level, cryptocurrency regulation is presently not explicitly contemplated within international legislative mechanisms. [7] As a result, the concern over the attractiveness of cryptocurrencies in facilitating money laundering and transnational crimes continues to grow amid already identified instances of its illicit use. It suffices to say at this point that though regulation of cryptocurrencies is important, what is required is thoughtful regulation which facilitates its legitimate use and curbs cryptocurrency use for illicit purposes.

---

4 The World Bank's Global Financial Development Report on Financial Inclusion indicates that about half of the world's adult population (about 2.5 billion) do not have an account at a formal banking institution – by choice or due to barriers such as distance from domicile cost of maintaining an account. See World Bank, Global Financial Development Report 2014, (Washington: World Bank, 2014) at 1. The benefits of cryptocurrencies are discussed more comprehensively in chapter 4 of this work.

5 The European Union Agency for Law Enforcement Cooperation (Europol), Press Release, "Money Laundering with Digital Currencies: Working Group Established" (9 September2016), online <https://www.europol.europa.eu/newsroom/news/money-laundering-digital-currencies-working-group-established09Sep2016>. Steven Russollilo, "Bitcoin Goes to the Big Four: PwC Accepts First Digital-Currency Payment" (30 November 2017), The Wall Street Journal, online <https://www.wsj.com/articles/pricewaterhousecoopers-accepts-fee-in-bitcoin-1512036992>. Julia Kollewe "Bitcoin: UK and EU Plan Crackdown Amid Crime and Tax Evasion Fears" (4 December 2017), The Guardian, Online <https://www.theguardian.com/technology/2017/dec/04/bitcoin-uk-eu-plan-cryptocurrency-price-traders-anonymity>.

6 Gertrude Chavez-Dreyfuss, "Bitcoin hits another record high in march towards $20,000" (December 12 2017) Reuters, online <https://www.reuters.com/article/uk-markets-bitcoin/bitcoin-hits-another-record-high-in-march-towards-20000-idUSKBN1E60PE>. Paolo Tasca, "Digital Currencies: Principles, Trends, Opportunities, and Risks" (7 September 2015) Social Sciences Research Network (SSRN), online <https://ssrn.com/abstract=2657598>.

7 For instance, are cryptocurrencies to be considered 'money' or 'commodities' or even 'negotiable instruments' with laws applicable to the use of these items applying to them?

1.2 Context of the Problem

Money laundering is a financial crime that transcends national borders. It is the method by which criminals disguise the illegal origins of their wealth and protect their asset bases, so as to avoid the suspicion of law enforcement agencies and mask any trail of incriminating evidence. When conduct such as illicit drug trafficking or trafficking in persons occurs,[8] an initial (predicate) crime transpires. Subsequently, its proceeds would need to be masked (laundered) in order for perpetrators to utilize the wealth in society. It has also been found that terrorism is facilitated by money laundering in order to finance terrorist activities.[9]

Traditionally, money laundering was accomplished primarily through conventional banking institutions. However, efforts to combat transnational crime and money laundering of its proceeds increasingly displace these habitual methods. Banking and financial institutions are now required to report suspicious or large financial activity and conduct independent enquiries of new and existing customers to validate their identities and source of funds.[10] This leaves money launderers seeking alternative (less regulated) means for concealing the source or proceeds of transnational crime. At the same time, cryptocurrency networks remain unregulated either on their own or embedded (explicitly) within other subject areas. This 'regulatory gap' makes cryptocurrencies, in their present unregulated state, potentially very appealing for those who wish to engage in money laundering and related criminal activities, human rights violations, and other forms of exploitation.[11]

---

8 Examples of transnational crimes.

9 International Monetary Fund, "The IMF and the Fight Against Money Laundering and the Financing of Terrorism" (30 October 2017), The International Monetary Fund, online <<http://www.imf.org/external/np/exr/facts/aml.htm>

10 International instruments such as the United Nations Convention on Transnational Organized Crime and the Financial Actions Task Force Recommendations contain such provisions and are discussed further later in this chapter.

11 The term 'regulatory gap' refers to the absence of government regulation on a given activity. The International Union for the Conservation of Nature and Natural Resources Research Paper describes the regulatory gap as: "substantive and/or geographical gaps in the international legal framework, i.e. issues which are currently unregulated or insufficiently regulated at a global, regional or sub- regional level." See Kristina M. Gjerde *et al*, *Regulatory and Governance Gaps in the International Regime for the Conservation and Sustainable Use of Marine Biodiversity in Areas beyond National Jurisdiction* (Gland: IUCN, 2008) at 1, online: < https://portals.iucn.org/library/sites/library/files/documents/EPLP-MS-1.pdf>. The term appropriately describes the regulatory status of cryptocurrencies in the context of transnational crimes.

There is a growing concern that existing forms of criminal activity are now facilitated by advances in technology: communications, transportation, and financial transactions intended to facilitate globalization.[12] These advances add to the ease with which crime can be committed. With the recent iteration of technological development in the form of cryptocurrencies, a potential alternative means for circumventing regulatory measures that inhibit transnational crimes has also arrived. In the context of Anti-Money Laundering (AML) instruments, money laundering using conventional banking mechanisms which involved real human presence, place, or physical operation which can be monitored.[13] Though existing efforts to combat money laundering of this sort is by no means perfect, regulatory and enforcement officials are often able to identify and combat its occurrence. However, with the emergence of cryptocurrencies, especially as instantiations of its use for illicit purposes are revealed,[14] a thorny problem is emerging for law enforcement and regulatory agencies. This is especially so, given that most features of traditional banking facilities are absent in cryptocurrencies: it involves non-face to face virtual banking, is decentralized, and lacks any formal oversight.

For instance, obtaining evidence that cryptocurrencies have been used in the facilitation of money laundering and transnational crimes comes with a new set of challenges given that users are able to conduct transactions with relative anonymity.[15] In their research, Irwin *et al* conduct an empirical inquiry on cryptocurrencies and identify ease of use as a key factor that attracts criminals seeking new avenues for terrorism financing to cryptocurrencies.[16] To build on their findings, I

---

12 Maryke Silalahi Nuth, "Taking Advantage of New Technologies: For and Against Crime", (2008) 24:5 Computer L & Security Rev 437. Benjamin Perrin, "Social Media Crime in Canada: Annotated Criminal Code" (Ottawa: Canadian Bar Association Law for the Future Fund, 2017).
This is discussed further in chapter 2.

13 Margaret Beare, "Responding to Transnational Organized Crime: Follow the Money" in Felia Allum & Stan Gilmour, eds., Routledge Handbook of Transnational Organized Crime (Abingdon: Routledge, 2011) 274

14 The instances of Silk Road and Liberty Reserved are mentioned later in this work.

15 The anonymity of cryptocurrencies is discussed further later in chapter 4 of this thesis.

16 Angela S.M. Irwin, Jill Slay, Ki-Kwang Raymond Choo, and Lui Liu, "Are the financial transactions conducted inside virtual environments truly anonymous? An experimental research from an Australian perspective," (2013) 16:1 J Money Laundering Control 6.

adopt a criminological lens in considering what additional reasons might explain why cryptocurrencies would be attractive to those seeking to launder the source or proceeds of crime.

At the initial stage of its development, suggestions that cryptocurrencies such as Bitcoin could potentially be used for money laundering and in facilitating other transnational crimes were met with dismissal by regulatory authorities.[17] The United Kingdom Policy Risk Assessment policy paper on money laundering and terrorist financing published in 2015 took the position that 'new payment methods' (which includes cryptocurrencies) presented a 'low risk' for use in money laundering.[18] As the use of cryptocurrencies grows, the initial dismissal of its impact and relevance for money laundering is giving way to heightening awareness of its significance in this regard. [19] A study by the University of Cambridge Centre for Alternative Finance found that the estimated number of cryptocurrencies users has increased from 0.3 million in 2013 to 5.8 million in early 2017.[20] Given the growth in its usage, it becomes pertinent to understand what cryptocurrencies are, and consider whether and how to bring them within the confines of an appropriate regulatory mechanism. Domestic authorities and international institutions are now rethinking their position on cryptocurrencies given their continued growth in use and popularity.[21] The 2017 iteration of the UK risk assessment policy paper now considers the risks of money laundering using 'digital currencies' to be 'emerging'.[22]

---

17 See for instance, United Kingdom Home Office, "UK National Risk Assessment of Money Laundering and Terrorist Financing: Policy Paper" (October 2015) GOV>UK, online: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf>. This report described the risk of crime using cryptocurrencies such as bitcoin as low.

18 Id. In the year in which this report was published, London was reportedly considered "global money laundering centre for the drug trade. See James Hanning & David Connet, "London is now the global money-laundering centre for the drug trade, says crime expert" July 4, 2015 Independent, online: <https://www.independent.co.uk/news/uk/crime/london-is-now-the-global-money-laundering-centre-for-the-drug-trade-says-crime-expert-10366262.html>.

19 Julia Kollewe, Bitcoin, *supra* note 5.

20 Garrick Hileman and Michel Rauchs, "Global Cryptocurrency Benchmarking Study", Cambridge Judge Business School [Cambridge Centre for Alternative Finance], University of Cambridge, online <https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf >.

21 See *supra* note 4.

22 United Kingdom Home Office, "UK National Risk Assessment of Money Laundering and Terrorist Financing" *supra* note 17.

The terms 'digital currency' and others associated with cryptocurrencies will be analysed in chapter 4 of this thesis.

International regulatory and enforcement agencies considering the problem of cryptocurrencies have thus far focused on capacity building for law enforcement officials and increasing awareness in the law enforcement sector.[23] For instance, the international enforcement agency, Interpol has announced that it is creating its own digital currency as a means of understanding the use of cryptocurrency in commission of transnational crime.[24] In doing so, their aim is to build a knowledge base on cryptocurrency operations and equip police authorities with the capacity to identify and apprehend criminals who use cryptocurrencies to facilitate their operations.[25]

An example of bitcoin facilitating criminal enterprise is the online marketplace, Silk Road, which was being used to facilitate money laundering by drug and human traffickers.[26] With bitcoin as the only form of payment accepted, Silk Road and its users were able to maintain anonymity of transactions. This illicit marketplace was discovered through a collaborative effort involving the US with various departments and international law enforcement agencies. The varied response by international and domestic institutions concerning the emerging use of cryptocurrencies, especially for criminal purposes, demonstrates that the question is no longer whether cryptocurrencies are being used to facilitate money laundering and other transnational crimes, but to what extent and how the law should respond.

1.3 Significance of Topic

Technology has become pervasive in society. Most aspects of human interaction today are facilitated by one form of technological advancement or another. Within this broad context, financial technology (FinTech) seeks to make financial services more accessible to the public.

---

23 Interpol, Europol and some national agencies have organised conferences where ideas can be shared and collaborative efforts developed. Europol Press Release, *supra* note 5. Other domestic regulatory agencies have also made statements in recognition of the increasing growth of cryptocurrencies. Chanyaporn Chanjaroen, Andrea Tan & Haslinda Amin, "Singapore Won't Regulate Cryptocurrencies, Central Bank Chief Says" (24 October 2017) Bloomberg (blog), online: <https://www.bloomberg.com/news/articles/2017-10-24/singapore-won-t-regulate-cryptocurrencies-remains-alert-to-risk>.

24 Interpol, Press Release, "Project to Prevent Criminal Use of Blockchain Technology Launched by International Consortium" (24 May 2017) Interpol online: <https://www.interpol.int/News-and-media/News/2017/N2017-069>.

25 Id.

26 United States v Ross William Ulbricht, Superseding Indictment, In the United States District Court for the District of Maryland, October 1, 2013, online: < https://www.ice.gov/doclib/news/releases/2013/131002baltimore.pdf>.

Legislative institutions at the domestic and international levels are coming to terms with this development and considering ways of adapting existing laws or enacting new ones to cover arising issues.[27] Therefore, it is important to consider how the growth and existence of cryptocurrencies affect different spheres of society.

For instance, financial institutions are likely to have concerns over the impact of this growth in utilization of cryptocurrencies for their traditional banking methods. Financial regulators would also need ensure that transactions and trading using this mechanism follows financial regulatory tools and that they are not a means for circumventing financial compliance instruments.

Furthermore, government administration relies on public revenue and concerns in this regard are also raised by the use of cryptocurrencies. [28] The existence of cryptocurrencies outside institutional regulation means that governments are unable to generate income (through taxation) from their usage and would seek ways to create a framework for their cryptocurrency taxation.[29] Taxation would be especially important to developing countries seeking to strengthen their government's administrative capacity through revenue generation.

Finally, and this is the issue with which this work with contend, is the use of cryptocurrencies in facilitating crime especially those of a transnational nature. In focusing on this last problem, this work will examine the hypothesis that cryptocurrencies circumvent international anti-money laundering regimes that are designed to combat transnational crime. Within this parameter, the use of cryptocurrencies to facilitate the laundering of illicit profits, and consequently other forms of transnational organized crime will be examined.

---

27 An example of this consideration could be found here. Benjamin Perrin, Social Media Crime, *supra* note 12.

28 Europol Press Release, *supra* note 5. Steven Russollilo, *supra* note 5. Julia Kollewe, *supra* note 5.

29 This would draw on rationale attributed to the development of the Tobin Tax. For James Tobin, part of the rationale for the taxation of such financial/currency transaction lies in the reduction of the socially harmful effects of finance while retaining its benefits (James Tobin, "A Proposal for International Monetary Reform" (1978) 4:3-4 Eastern Economic J 153). Other advocates of the Tobin Tax view it as a good way of raising revenue for economic and social developments. Ian Young, "Banks and Tax" in Sajid M. Chaudhry & Andrew W. Mullineux, eds., Taxing Banks Fairly (Cheltnam: Edward Elgar Publishing Limited, 2014) 90 at 99.

1.4 Key Concepts

This thesis is at the intersection of the relationship between transnational crime, money laundering and cryptocurrencies. Before setting out the research questions, these key concepts will each be briefly defined.

1.4.1 Transnational Crime

This work will be limited to the category of crimes commonly referred to as transnational crime. Understood as treaty crimes of international concern,[30] they include trafficking in persons,[31] arms trafficking,[32] migrant smuggling,[33] dealing in conflict natural resources such as diamonds (referred to as 'predicate offences in the UNCTOC),[34] and terrorism ('postdicate' in its relationship to money laundering).[35] Though these crimes originated as criminological concepts to explain criminal conduct defined differently in different states, they have been recognised as forms of crime under international treaties such as the UNCTOC.[36] The crimes in this group are identified

30 Treaty crimes of international concern, often involving money laundering, are distinguished from core international crimes. The latter, genocide, aggression, serious violations of the laws and customs of armed conflict and crimes against humanity, have a basis in customary international law and in terms of Articles 5 to 9 of the Rome Statute of the International Criminal Court, UN Doc. A/CONF. 183/9 they fall under the jurisdiction of the International Criminal Court (ICC). See M. Cherif Bassiouni, "The Source and Content of International Criminal Law: A Theoretical Framework", in M. Cherif Bassiouni ed., International Criminal Law Vol. I: Crimes 2nd (New York: Transnational Publishers, 1999), 4.

31 Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention Against Transnational Organized Crime 15 November 2000, 2237 UNTS at 319 (entered into force on 28 January 2004)

32 Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition, supplementing the United Nations Convention against Transnational Organized Crime 31 May 2001, 2326 at UNTS 208 (entered into force 3 July 2005)

33 Protocol against the Smuggling of Migrants by Land, Sea and Air, supplementing the United Nations Convention against Transnational Organized Crime 15 November 2000, 2241 UNTS at 480 (entered into force on 28 January 2004)

34 United Nations Convention Against Transnational Organized Crime and its Protocols thereto, 15 November 2000, 2225 UNTS 209 (entered into force 29 September 2003) [UNCTOC].

35 International Convention for the Suppression of the Financing of Terrorism 9 December 1999, 2178 UNTS at 197 (entered into force 10 April 2002). My use of the term 'postdicate' is inspired by Thomas R.T. Naylor's usage in his piece "The International Anti-Money Laundering Regime: A Bankrupt Policy Desperate for a New Raison D'être" in Georgios Antonopoulos, Marc Groenhuijsen, Jackie Harvey, Tijs Kooijmans, Almir Maljevic & Klaus Von Lampe (eds.) Usual and Unusual Organising Criminals in Europe and Beyond: Profitable Crimes, from Underworld to Upperworld (Antwerp: Maklu, 2011) 131 at 136. My use of this term is to explain how the financing of terrorist activities commonly occurs following (post) the laundering process.

36 Bruce Zagaris, "Transnational Organized Crime" in Bruce Zagaris, (ed.), *International White Collar Crime: Cases and Materials* (Cambridge: Cambridge University Press, 2010) 168.

by their ability to transcend domestic borders, transgress laws in multiple states, and have an international impact.[37] .

1.4.2 Money Laundering

Money laundering involves the "conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her action."[38] It also encompasses the "the concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime."[39] Transnational crimes which involve money laundering will be the substantive crimes appraised in my thesis.

1.4.3 Cryptocurrency

Cryptocurrency is a mathematics-based, decentralized virtual currency protected by cryptography principles[40] with the ability to settle and reconcile global transactions at a lower cost using blockchain technology.[41] Cryptocurrencies are not tied to any government or backed by any bank (middle-man) and its popularity stems from a neo-libertarian ideology where individuals believe

---

37 UNCTOC, *supra* note 34.

38 See UNCTOC article 6, *supra* note 34. This broad UNCTOC definition of money laundering is preferred amongst AML definitions of money laundering. It is adopted in ensuing AML instruments such as United Nations Convention Against Corruption, 31 October 2003, 2225 UNTS 209 (entered into force 29 September 2003 [UNCAC] and FATF, International Standards on Combatting Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations (Paris: FATF, 2012) [FATF Recommendations]. In earlier AML treaties such as United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, drug trafficking is specified as the only predicate crime for money laundering. see United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (20 December 1988), 1582 UNTS 95; in force 11 November 1990 [Vienna Convention].

39 UNCTOC, *supra* note 34.

40 Financial Action Tax Force (FATF) Report, "Virtual Currencies – Key Definitions and Potential AML/CFT Risks" (June 2014), FATF, online: <http://www.fatf-gafi.org/topics/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html>.

41 Zach Church, "Blockchain Explained: An MIT Expert on Why Distributed Ledgers and Cryptocurrencies Have the Potential to Affect Every Industry" (25 May 2017), MIT Sloan School of Management, online < http://mitsloan.mit.edu/newsroom/articles/blockchain-explained/>. The block chain technology replaces the centralized banking system as the trusted third party that serves to underwrite financial transactions using cryptocurrency.

they should be free to conduct their business in private without (or with limited) regulatory interference from government.[42] Examples of cryptocurrencies include Bitcoin,[43] Litecoin,[44] Monero,[45] Zcash,[46] and Ethereum.[47] Bitcoin represents the first fully implemented cryptocurrency protocol and is considered the top cryptocurrency by market capitalization.[48] Bitcoin has two meanings. *Bitcoin* (uppercase) is the global payment protocol or network through which a person can send and receive money denominated in a digital currency known as *bitcoin* (lowercase) abbreviated to BTC.[49] New forms of cryptocurrencies are constantly being developed as potentially more effective and private alternatives. Although the use of cryptocurrency is marginal in comparison with fiat currency transactions, it is estimated that the cryptocurrency market today is worth over 7 billion dollars, with bitcoin-ATMs being deployed in cities in Canada, Germany, and the US.[50]The ledger of cryptocurrency network transactions is often publicly available and transactions contained therein are only identified by a string of letters and numbers not linked to

---

42 Peter Vallentyne and Bas van der Vossen, "Libertarianism" in Edward N. Zalta (ed.), *The Stanford Encyclopedia of Philosophy* (Fall 2014 Edition), online: <https://plato.stanford.edu/archives/fall2014/entries/libertarianism/> While transactions are not completely anonymous, they are pseudonymous, thereby ensuring the privacy of its users in a manner not obtainable with traditional banking institutions. Colin Faife, "Live Free or Mine: How Libertarians Fell in Love with Bitcoin" (10 October 2016) Coindesk (blog), online: <https://www.coindesk.com/live-free-or-mine-how-libertarians-fell-in-love-with-bitcoin/>

43 Bitcoin.org

44 Litecoin.com

45 Monero.org

46 https://z.cash

47 Ethereum.org

48 CoinMarketCap, "Top 100 Cryptocurrencies by Market Capitalization" online: <https://coinmarketcap.com>, last visited March 11 2019.

49 See Lam Pak Nian & David Lee Kuo Chen, "Introduction to Bitcoin" in David Lee Kuo Chuen (ed),.), *Handbook of Digital Currencies: Bitcoin, Innovation, Financial Instruments, and Big Data* (London: Academic Press, 2015) at 14. By this analogy, Dollars is the denomination and legal tender established by various countries using that description, but transactions are conducted using dollars. In a bit to improve on the legitimacy of bitcoin and a reflection of its growth, some exchanges have proposed the currency code XBT for bitcoin which is compatible with ISO 4217.

50 Primavera De Filippi, "Bitcoin: A Regulatory Nightmare to a Libertarian Dream" (2014) 3:2 Internet Policy Review online: <https://policyreview.info/node/286/pdf>. The world's first bitcoin ATM, operated by Bitcoiniacs, is located inside Waves Coffee House at Howe and Smithe streets in downtown Vancouver and went live on October 29, 2013. Bitcoins can be purchased there as well as at other bitcoin-ATM deployed in any other location. CBC News, "World's first bitcoin ATM opens in Vancouver" October 29, 2013, online: < https://www.cbc.ca/news/technology/world-s-first-bitcoin-atm-opens-in-vancouver-1.2286877> last accessed August 3, 2018.

any individual.[51] For this reason, empirical research into cryptocurrencies such as bitcoin has observed that users are able to conclude pseudo-anonymous financial transactions.[52]

1.5 Research Questions

The research questions for this thesis are as follows:

1) How does money laundering facilitate transnational crime?
2) What are the strengths and weaknesses of the global anti-money laundering regime?
3) Are cryptocurrencies able to circumvent the global anti-money laundering regime and to what extent is this possible?

1.6 Methodology and Theoretical Framework

This research will be primarily doctrinal in nature, involving documentary analysis of key international conventions that deal with money laundering.[53] The issues under consideration reflect the cross-border nature of transnational crime and cryptocurrencies. The nature of transnational crimes also exemplifies how difficult it would be for a single country to effectively regulate the issue under its domestic laws. This difficulty in turn points to the need for an international (in the first instance) framework for regulating cryptocurrencies.

---

51 For Bitcoin, Litecoin, and Ethereum for instance, transactions are publicly available on the ledger (Blockchain) while Monero and Zcash are examples of cryptocurrencies whose ledgers are also publicly available but take steps to obfuscate the transaction records on the ledger. See Frank Etto, “Know Your Coins: Public vs. Private Cryptocurrencies” September 22, 2017 Nasdaq online: <https://www.nasdaq.com/article/know-your-coins-public-vs-private-cryptocurrencies-cm849588>.

52 Perri Reynolds & Angela S.M. Irwin, "Tracking digital footprints: anonymity within the bitcoin system" (2017) 20:2 J Money Laundering Control 172

53 International Convention Against the Taking of Hostages, New York, 17 December 1979, 1316 UNTS 205; Vienna Convention, *supra* note 38 (20 December 1988), 1582 UNTS 95; in force 11 November 1990; UNCTOC, *supra* note 34. Terrorist Financing Convention, *supra* note 35; UNODC, Legislative Guides for the Implementation of the United Nations Convention Against Transnational Organized Crime and the Protocols Thereto (New York: United Nations, 2004).

For my theoretical framework and methodology, I draw on the emerging field of New Legal Realism (NLR), with a strong emphasis on Gregory Shaffer's work.[54] For Shaffer, cultural and economic globalization means that the type of problems conceived by stakeholders are no longer domestic (concerning individuals within the borders of a single state) or purely between states. As a result, there is an increasing array of international organizations that deal specifically with transnational problems that arise from social interactions amongst individuals on a global scale.[55] This development in turn now require an international perspective to tackle them.

Key to my research is the contemplation of the 'borderless' nature of cryptocurrencies and its facilitation of a transnational crime phenomenon. As such, Shaffer alerts us that what is required is the contemplation of transnational legal norms such as those emanating from the transnational crime treaties identified for evaluation in this work.[56] A common thread between cryptocurrencies and transnational crimes is that they operate in a transnational manner and therefore outside the exclusive control of any given nation. Drawing on NLR, individual nations cannot address cryptocurrency use in money laundering and transnational crimes (also cross-border in nature) in isolation but must dialogue with other states and relevant international institutions with a mandate for anti-money laundering. This approach would result in solutions which do not involve states infringing the sovereignty of other states (by seeking to implement policies that encroach on the jurisdiction of other states) can be obtained.

The chosen theoretical lens provides a justification for interrogating the complex international AML framework, in the first instance from an international dimension. Focusing on the international dimension is pragmatic in accordance with the NLR approach as it seeks cohesive regulation that considers the diverse interests of states, allows cryptocurrencies to be used

---

54 Gregory Shaffer, "The New Legal Realist Approach to International Law" (2015) 28:2 Leiden J Intl L (Symposium on New Legal Realism) 189, online: <https://ssrn.com/abstract=2605198>.

55 Id at 9.

56 Id. See also Gregory Shaffer, "New Legal Realism in International Law" in Heinz Klug, Elizabeth Mertz, & Sally Engle Merry (eds.) Studying Law Globally: New Legal Realist Perspectives Vol. II (Cambridge: Cambridge University Press, 2015).

legitimately, and at the same time strives for restrictions that would prevent exploitation for illicit purposes.

From a practical perspective, this approach ensures that solutions proposed are cooperative and cohesive, avoiding gaps in regulation that could be exploited by criminally-minded actors.

The aim is also to examine the adequacy of existing international regulations to protect against transnational crime in light of technological advances that support alternative means of financial transactions using cryptocurrencies. In doing so, this work will be part of the greater body of research that seeks to highlight the influence of technology on criminal conduct.[57]

This work is interdisciplinary. As the law does not tell us why crimes are committed and why individuals are likely to gravitate towards one avenue of criminal conduct over the other, it is necessary to look to other disciplines in considering the risk of cryptocurrencies being used for money laundering to facilitate transnational crime. Specifically, this work will draw on criminological theories that explain how efforts to combat money laundering and transnational crime lead to the displacement of criminal opportunity. Such theories could also explain how such displacement could result in gravitation towards presently unregulated openings to achieve criminal purpose.

In this case cryptocurrencies, in the absence of cohesive regulation, could become attractive to criminals seeking alternative avenues to launder the proceeds of their crimes. The criminological theory of situational crime, for instance, suggests that when people believe that crime prevention mechanisms are in place, they are likely to be deterred from pursuing their criminal purpose using a particular avenue.[58] This logic is based on the concept of rational choice – that every criminal

---

57 Ronald V. Clarke, "Technology, Criminology, and Crime Science" (2004) 10, European Journal on Criminal Policy and Research 55.

58 Ronald V. Clarke, "Situational Crime Prevention: Theory and Practice (1980) 20:2 Brit J Crim. 136. Ronald V. Clarke, Situational Crime Prevention: Its Theoretical Basis and Practical Scope (1983) 4 Crime and Justice 225. Nicholas Gilmour, "Preventing money laundering: a test of situational crime prevention theory" (2016) 19:4 J Money Laundering Control 376; Nicholas Gilmour, "Understanding the practices behind money laundering: A rational choice interpretation" (2015) 44 Intl JL Crime & Practice 1. Ronald V. Clarke, *id*.

will assess the situation of a potential crime, weigh their potential gains from the crime against what they stand to lose, and then act accordingly.[59] Scholars such as Nicholas Gilmour[60] and Ronald Clarke[61] suggest that using this approach, appropriate measures could be devised for prevention of money laundering. Clarke adds that this theory of situational crime prevention could also be adapted to take account of technological developments that create further avenues for crime. Therefore, this theory is appropriate for this thesis as it deals with money laundering where the criminal actors, in a bid to launder the proceeds of their crimes, could turn from traditional banking institutions to cryptocurrencies given that AML efforts at present, primarily target said banking institutions.

1.7 Scope of Research

The scope of this thesis has been defined according to four parameters. First, the instruments examined are limited to international treaties and other relevant documents that make up the international AML regime. Various inter-governmental meetings usually under the auspices of the United Nations have emphasized the need for states to work together on issues of a transnational nature. The UNCTOC for instance, recalls in its preamble the importance of international cooperation of states on the relevant matters. Therefore, this work will focus primarily on treaties that oblige states to proscribe certain conduct and assist other states in their efforts to suppress the crimes of international concern included in the treaties.[62] These conventions are referred to as 'suppression conventions' because they have transnational elements that require states working together to 'suppress' them. This thesis also considers other relevant instruments or strategies from

59 Derek B. Cornish and Ronald V Clarke, Understanding Crime Displacement: An Application of Rational Choice Theory (1987) 25 Criminology 933

60 Nicholas Gilmour, "Preventing money laundering" *supra* note 58; Nicholas Gilmour, "Understanding the practices behind money laundering" *supra* note 58.

61 Ronald V. Clarke, ''Technology, Criminology and Crime Science'' *supra* note 57.

62 Neil Boister, "Human Rights Protections in the Suppression Conventions" (2002) 2:2 Human Rights L Rev, 199 at 199-200.

international agencies such as Interpol,[63] IMF, and the World Bank, all of which are part of the target audience for this work.

Secondly, this work focuses on money laundering, an essential component of transnational crime. In doing so, it draws on the growth of international anti-money laundering (AML) policies and instruments that see the fight against money laundering as an effective way to tackle transnational organized crime (TOC).[64] While speculation remains on whether reducing money laundering has a similar effect on predicate crimes, it is accepted that globally, the amount of money laundered is exorbitant and continues to increase.[65] It is also acknowledged that money laundering supports organized criminals, drug trafficking, trafficking in person, terrorist financing, firearms and human smuggling, to name a few predicate and postdicate crimes.[66] Though the forms of transnational crime are numerous, I have limited the crimes I will examine in this thesis to drug trafficking and terrorist financing as instances of predicate and postdicate transnational crimes. Drug trafficking represents the first transnational organized crime linked to money laundering and it continues to generate the most illicit revenue today. [67] Terrorist financing, on the other hand, is interesting as a transnational crime which relies on money laundering for a different purpose and presents a different side of transnational crimes, one which is not aimed at generating illicit wealth for use in the legitimate financial system. Rather, terrorist financing is aimed at laundering legitimate or illegitimate funds in order to further terrorist activities, a problem which remained at the core of modern domestic and international security.

Finally, this thesis focuses on Bitcoin as a case study of cryptocurrencies. As the first fully developed and widely used cryptocurrency network (estimated to control about 47% of the

63 Efforts so far have been on capacity building for law enforcement officials and increasing awareness, for instance the development of the Interpol Global Complex for Innovation under which it is collaborating with other agencies and developing its own cryptocurrency to study how the mechanism is used in the commission of crime (Interpol Global Complex for Innovation online: <https://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation)>

64 Margaret Beare, "Responding to Transnational Organized Crime: Follow the Money" *supra* note 13.

65 Id at 266

66 Id, 266.

67 UNODC, Travaux Préparatoires of the Negotiations for the Elaboration of the United Nations Convention Against Transnational Organized Crime and the Protocols Thereto United Nations Office on Drugs and Crime. (New York: United Nations, 2006) at *xi*.

cryptocurrency market as of 2018),[68] Bitcoin is used to illustrate the key features of cryptocurrencies in the context of the issues established above.[69] Using Bitcoin as a case study is appropriate given the emerging nature of cryptocurrencies.[70] The similarities in the important features amongst different forms of cryptocurrency such as their lack of regulation, reliance on blockchain technology, and their operation outside any traditional banking mechanism will enable the results achieved using bitcoin to be applied generally to the others.

This research will be of value to a variety of stakeholders including human rights agencies; international and regional law enforcement and policing agencies such as Interpol and Europol; international and regional institutions such as UNODC, World Bank, IMF, European Central Bank, and their domestic counterparts. It will also be important for domestic governments as a whole, whose interests in cryptocurrencies vary from acceptance, observation, and rejection. For human rights organisations for instance, their concern is to ensure that the work they have done so far in preventing and prosecuting human rights violations does not suffer setbacks through the use of cryptocurrencies.[71]

While the literature on this subject is steadily emerging, it does not present a comprehensive picture of the problem in terms of regulation, monitoring, and enforcement. The scope of this thesis is limited to the contemplation of the international framework for AML and how this applies to cryptocurrencies. While I do not evaluate the efforts from a domestic or regional perspective, there are numerous endeavors in this regard which are identified in subsequent chapters where it is relevant to do so. Building on the existing literature, this thesis will provide a comprehensive evaluation of a selection of international instruments that apply to this problem. In doing so, the aim is to identify gaps or loopholes that could enable perpetrators to circumvent the existing international AML instruments by using cryptocurrencies.

---

68 Billy Bambrough, "Binance CEO Predicts A Bitcoin and Crypto 'Bull Run'" Forbes November 12, 2018, online: < https://www.forbes.com/sites/billybambrough/2018/11/12/binance-ceo-predicts-a-bitcoin-and-crypto-bull-run/#67e6a0a63921>.

69 Garrick Hileman and Michel Rauchs, *supra* note 20 at 20.

70 Jeffery S. Beaudry & Lynne Miller, Research Literacy: A Primer for Understanding and Using Research (New York: Guilford Publications, 2016).

71 Yury Fedotov, supra note 1.

1.8 Thesis Overview

The structure of the thesis tracks the three research questions presented above. Chapter 2 examines and defines transnational crime generally and for the purpose of this work. It will examine transnational crime and its link to the issue of money laundering. In doing so, this chapter will answer the first research question: how does money laundering facilitate transnational crimes such as illicit drug trade, human trafficking, migrant smuggling, terrorist financing, and dealing in conflict natural resources?

Chapter 3 describes and evaluates the extant international anti-money laundering regime with a view to identifying provisions that could be interpreted to apply to cryptocurrency-facilitated money laundering. This chapter seeks to answer the second research question: what are the strengths and weaknesses of the existing international anti-money laundering regime? Next, Chapter 4 of this thesis provides an overview of cryptocurrencies using bitcoin as a case study. This will involve an analysis of what cryptocurrencies are and how they are used. Chapter 4 will also evaluate why cryptocurrencies such as bitcoin should be a cause for concern in the realm of money laundering.

In Chapter 5, I evaluate whether cryptocurrencies can be brought within the existing international AML regime. This chapter will also address the importance of regulating cryptocurrencies from a transnational perspective. Together with Chapter 4, this chapter will answer the third research question: are cryptocurrencies able to circumvent the global anti-money laundering regime and to what extent is this possible? In the concluding chapter of this thesis, I highlight the major findings of my research. I also identify some preliminary recommendations that would bring cryptocurrencies within the existing international anti-money laundering regime; explain the limitations encountered in the course of the research; and set out possible areas for future research.

Chapter 2: Transnational Crimes: Money Laundering and Underlying Crimes

The phenomenon of transnational crimes is becoming increasingly pervasive in our global society, aided by various factors, in particular globalization and advances in Internet technology. Transnational crimes affect modern political, legal, and social spheres.

The import of transnational crime in modern times is exemplified by the 9/11/2001 coordinated terrorist attacks on the World Trade Centre and Pentagon buildings in the United States. In analyzing this incident, Currie and Rikhof observe that the attack involved mostly nationals of Saudi Arabia with ties to a terrorist organization in Afghanistan, in itself constituting transnational crime.[72] The attacks were made possible using laundered funds.[73] These strikes took place in the United States with victims from different countries and who had varying ties to the country where the attacks occurred. The varying nationalities of both victims and perpetrators has jurisdictional implications for the different states that were affected either through the physical location of the attacks, the place or places where planning took place, the nationality of the victims and perpetrators, or the source of funds for the attacks. The trial of alleged perpetrators in the United States, the United Kingdom, and in France.[74] Some alleged perpetrators were taken to detention sites in different states (with and without the knowledge of such states), interrogated, and themselves sometimes subjected to harm of some kind, most especially torture.[75] This raises international law issues of respect for territorial sovereignty of states and extraordinary rendition of alleged offenders, amongst other issues.

This chapter sets out the problem of transnational crime, and the elements that influence or facilitate it. In evaluating transnational crime, we see how different developments in society (the catalysts) create opportunities for transnational crime's continued proliferation. These include

72 Robert Currie & Dr Joseph Rikhof, International and Transnational Criminal Law, 2nd ed. (Toronto: Irwin Law, 2013) at 325. See also International Convention for the Suppression of the Financing of Terrorism 1999.
73 Id.
74 Id.
75 Id.

globalization, technology, corruption, and persisting problems that are peculiar to certain third world countries.

This chapter also seeks to understand how money laundering, though established as a transnational crime in itself, facilitates other forms of cross-border or transnational crime. Furthermore, this chapter sets the scene for future discussion within this work on a new enabling element for money laundering i.e. cryptocurrencies, and its role in facilitating other transnational crimes. Finally, this chapter will highlight how money laundering facilitates specific forms of transnational crime with the objective of understanding how cryptocurrencies impacts this process.

2.1 Transnational Crime: Definition or Defining Features?

Transnational crime is a concept with origins in criminology. Within the discipline of criminology, scholars were traditionally concerned with the phenomenon of crime in a local construct. With advances in cross-country interaction amongst individuals, so also did the parameters of crime. As a result, it became increasingly necessary to contemplate the occurrence of criminal activity within a national context and beyond.[76] The limits of domestic authorities with regards to combatting criminal conduct that concerned the jurisdiction of another state – and infringing their territorial sovereignty – pointed to the need for international cooperation in tackling transnational crimes.

In adopting a definition for transnational crime, the United Nations Convention on Transnational Organized Crime (UNCTOC) offers the following definition of transnational crime, stating in article 3(2) that crime becomes transnational when

> […] it is committed in more than one state; it is committed in one state but a substantial part of its preparation, planning, direction or control takes place in another state; it is committed in one state but involves an organised criminal group that

76 David O. Friedrichs, "Transnational Crime and Global Criminology: Definitional, Typological, and Contextual Conundrums." (2007) 34:2 Social Justice 4. Philip Reichel and Jay Albanese, eds., Handbook of Transnational Crime & Justice (Thousand Oaks: Sage Publishing, 2005)

> engages in criminal activities in more than one state; or it is committed in one state but has substantial effects in another state.[77]

The statement of purpose (article 1) of the UNCTOC declares the objective of the Convention to be the promotion of cooperation amongst state parties in the context of organized crimes which have an international dimension.[78]

This objective ties in with findings emanating from the criminology discipline referred to above. Crime of this kind in particular is no longer confined to domestic borders. Factors such as globalization and technological developments for instance facilitate cross-border movement of people, information, trades and services for legitimate and illegitimate purposes. Affirming the justification for the UNCTOC, then UN Secretary General, Kofi Anan referred to the necessity of adopting a transnational law enforcement response where "crime crosses borders."[79] He also noted that where criminal actors seek to exploit the opportunities provided by globalization for their purposes, this must be recognized and addressed with instruments that go beyond individual national mechanisms.[80]

The need for international cooperation also recognizes the jurisdictional sovereignty of states. In the investigation or prosecution of a crime, a country seeking to tackle all aspects of a criminal transaction that exceed its domestic jurisdiction cannot interfere with the sovereignty of another state without its consent and/or involvement.

---

77 The United Nations Convention on Transnational Organized Crime, adopted by General Assembly resolution 55/25 of 15 November 2000) is the primary instrument in the fight against transnational organized crime, at article 3(2), accessed December 4, 2017, <https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf>.

78 Id.

79 Id at iii.

80 Id. Addressing the functionality of a transnational perspective to cross-border crime, Kofi Anan comments that:

"[I]f crime crosses borders, so must law enforcement […] If the enemies of progress and human rights seek to exploit the openness and opportunities of globalization for their purposes, then we must exploit those very same factors to defend human rights and defeat the forces of crime, corruption and trafficking in human beings

2.2 Transnational Crime in Literature

Literature on the concept of transnational crime can be found in both the law and criminology disciplines. From a criminological perspective, Gerhart Mueller views transnational crime as a criminological principle devised by the UN Crime Prevention and Criminal Justice Branch to enable the identification of a particular phenomenon where crime transcends domestic borders to contravene the laws of multiple countries.[81] Van Duyne also observes that transnational crime constitutes "the passing of illegal goods and/or services over national borders and/or rendering criminal support to criminal activities or related persons in more than one country.[82]"

The Encyclopedia on Transnational Crime adds the following to the concept of transnational crime: "those crimes that are committed across national borders or have effect in other nations.[83] The Encyclopedia also explains that legislative provisions on transnational crime can be framed either under domestic or international law.[84] In the case of a domestic law framing, what makes the law transnational is whether it is couched to have effect beyond the jurisdiction of the drafting country. This definition places emphasis on the implications of state sovereignty for transnational law.[85]

For Cyrille Fijnaut, the term transnational crime is wide in scope and encompasses the realms of organized, corporate, professional and political crime.[86] He also argues that though 'transnational'

---

81 Gerhart Mueller, "Transnational crime: Definitions and Concepts" in Philip Williams and Dmitri Vlassis, eds., *Combating Transnational Crime: Concepts, Activities, and Responses* (Abingdon: Frank Cass, 2001) 13.

82 Quoted in Felia Allum & Stan Gilmour, "Introduction" in Felia Allum & Stan Gilmour (eds.) *supra* note 13 at 7.

83 William C. Plouffe Jr., "Transnational Crime: Defined" in Margaret E. Beare (ed.) (2012*) Encyclopedia of Transnational Crime & Justice* (Thousand Oaks: SAGE Publications Ltd, 2012).

84 Id.

85 Given that domestic law is intended for confines of an individual country's jurisdiction, any attempt to extend its reach beyond this parameter to create rights, or duties, or punishment, or some other effect in another country implicates the sovereignty of such other country or countries which all states are bound to respect pursuant to international law.

86 Cyrille Fijnaut, "Transnational Crime and the role of the United Nations" (2000) 8 European Journal of Criminal Law and Criminal Justice 119, at 120. Also stressing the transnational nature of the crimes here, Neil Boister points to a Privy Council ruling in explaining that the harmful effects of the crimes in this group abroad mean that they seldom ever domestic in nature. For Boister, transnational crime connotes criminal activity whose actual or potential effects are transboundary in nature and involve either domestic or international law or both. He adds that by extension, transnational criminal law binds transnational crime with transnational law which (in reference to Philip Jessup's work) is defined as "all laws which regulates actions and events that transcend national frontiers." See Neil Boister, "Transnational Criminal Law?" (2003) 14:5 EJIL 953-976 at 954 citing Somchai Liangsiriprasert v United States Government [1990] 2 All ER 866, the Privy Council, hearing an appeal Hong Kong held per Lord Griffiths: "Hong Kong's jurisdiction could be extended to conspiracies carried out entirely abroad […]

connotes the crossing of domestic borders, much of transnational crime is purely domestic in nature, noting for instance that in the case of illicit transnational trafficking in drugs, production is domestic and involves control of domestic economies.[87]

Based on the literature canvassed above, the common features that must be present before criminal activity could be considered transnational include the involvement of a series of offenders whose actions facilitate the completion of the end crimes and a transboundary effect of the criminal transaction.[88] For instance, money laundering involves the obscuring (conversion or concealment) of proceeds of other criminal activities which often entails conduct such as fraud, breach of financial rules on disclosure of origin of funds, know your customer requirements, and corruption, to accomplish the end result.[89]

2.3 Transnational Crime: The Catalysts

Certain factors (catalysts) in the past and at present facilitate the perpetration of transnational crime. They include development, poverty, inequality, economic dependency, discrimination, and a breakdown in social norms that govern society.[90] For the purpose of this thesis, these catalysts have been grouped into the following thematic areas: corruption (inequality, breakdown in norms), technology (development), globalization (development), sovereignty (economic dependency), and the third world dimension (poverty, inequality, economic dependency).

Unfortunately in this century crime has ceased to be largely of local origin and effect. Crime is now established on an international scale and the common law must face this new reality" (at 878).

87 Id. The risks involved in transporting drugs across borders attract the high rewards to those willing to take such risks and illustrates this crucial aspect of the illicit activity. The development of legislation to combat drug trafficking can be traced to the efforts by the US authorities to crack down on importation of illicit drugs within their territory, making this transnational aspect essential. The emphasis by Cyrille Fijnaut on the local aspects of drug trafficking in this illustration fails to recognize an important aspect of drug trafficking: transportation of the finished product from one country to another for distribution and consequent generation of huge profits for the traffickers from countries that yield high revenues.

88 Andre Bossard, Transnational Crime and Criminal Law (Chicago: University of Chicago, Office of International Criminal Justice, 1990).

89 Introduction to part III on transnational crime page 107-108

90 See Louise Shelley, "The Globalization of Crime," in Mangai Natarajan (ed.) International Criminal Justice (New York: Cambridge University Press, 2011) at 3.

2.3.1 Transnational Crime and Corruption

Corruption in its simplest form involves the abuse of a position of trust. It is not always criminal but it is always unethical. Corruption occurs in all spheres and levels of society and in all countries to varying degrees despite the conjecture that it is a developing country (or third world) phenomenon. It is considered "central to the rise and the perpetuation of crime, terrorism, and other social ills."[91] Louise Shelley definitively calls corruption an "incubator for the growth of organized crime."[92]

Estimates about the cost of corruption differ but the consensus is that corruption is an enormous problem for society.[93] The Preamble to the United Nations Convention Against Corruption (UNCAC) states that corruption has the ability to affect the stability and security of societies, decimate its ethical values and justice, and endanger sustainable development and the rule of law.[94]

Corruption is linked to, and facilitated in one way or another by, forms of crime including organized crime such as money laundering. Corruption also facilitates illicit activities at a transnational level thereby requiring international cooperation to tackle. Such international cooperation is evident in the work carried out by a range of international and regional organizations.[95]

Although corruption itself is not defined in the UNCAC, corrupt activities are described therein: bribery of public officials (undue advantage given to or on behalf of a public official for that official to act or refrain from acting in accordance with his official duties);[96] bribery of foreign

---

91 Louise Shelley (ed.), Dirty Entanglements: Corruption, Crime, and Terrorism (Cambridge: Cambridge University Press, 2014) at 65.

92 Id.

93 Id.

94 UNCAC, *supra* note 38. The UNCAC currently has 140 signatories and 186 ratifications.

95 UNODC, World Bank/IMF, the African Union, the Council of Europe, the Customs Cooperation Council (also known as the World Customs Organization), the European Union, the League of Arab States, the Organisation for Economic Cooperation and Development (OECD), and the Organization of American States to name a few.

96 Article 15 UNCAC defines this as "the promise, offering or giving, to a public official, directly or indirectly, of an undue advantage, for the official himself or herself or another person or entity, in order that the official act or refrain from acting in the exercise of his or her official duties; (b) The solicitation or acceptance by a public official, directly or indirectly, of an undue

public officials and officials of public international organizations;[97] embezzlement, misappropriation or other diversion of property by a public official;[98] trading in influence;[99] abuse of functions;[100] illicit enrichment;[101] bribery in the private sector;[102] embezzlement in the private sector;[103] and laundering the proceeds of crime.[104] In urging criminalization of these specific activities as corruption offences, the UNCAC fails to consider the fact that in societies where corruption is prevalent, those tasked with adopting the necessary legislative and other measures that may be necessary to criminalize these actions may be involved in the corrupt practices described.

Corruption facilitates transnational crime. Corruption is the phenomenon that enables perpetrators to bribe public or private officials (governments or financial institutions) in order to launder the large amounts of illicit funds obtained as a result of their crimes. The Financial Action Task Force Report: *Laundering the Proceeds of Corruption* states that the fight against corruption is inextricably linked with that against money laundering given that stolen assets for instance require placement, layering, and integration phases of money laundering to be integrated into the financial system.[105]

Literature on corruption demonstrates that at its core, corruption is the obtaining of private gain through improper means. Scholars have attempted to define corruption in such a manner that

---

advantage, for the official himself or herself or another person or entity, in order that the official act or refrain from acting in the exercise of his or her official duties."

97 UNCAC, article 16: "(1) […]the promise, offering or giving to a foreign public official or an official of a public international organization, directly or indirectly, of an undue advantage, for the official himself or herself or another person or entity, in order that the official act or refrain from acting in the exercise of his or her official duties, in order to obtain or retain business or other undue advantage in relation to the conduct of international business," (2) " the solicitation or acceptance by a foreign public official or an official of a public international organization, directly or indirectly, of an undue advantage, for the official himself or herself or another person or entity, in order that the official act or refrain from acting in the exercise of his or her official duties." See UNCAC, *supra* note 38.

98 UNCAC, article 17

99 UNCAC, article 18

100 UNCAC, article 19: […] when committed intentionally, the abuse of functions or position, that is, the performance of or failure to perform an act, in violation of laws, by a public official in the discharge of his or her functions, for the purpose of obtaining an undue advantage for himself or herself or for another person or entity."

101 UNCAC, article 20: […], when committed intentionally, illicit enrichment, that is, a significant increase in the assets of a public official that he or she cannot reasonably explain in relation to his or her lawful income."

102 UNCAC, article 21

103 UNCAC, article 22

104 UNCAC, article 23

105 FATF, FATF Report: Laundering the Proceeds of Corruption (Paris: FATF, 2011).

encompasses its various facets while at the same time placing emphasis on certain attributes. For instance, Joseph S. Nye observes that corruption is a behavioural deviation from one's formal public duties for private gratification.[106] The emphasis here is on the actions of a public official. Klarven places similar emphasis on the activities of public officials: "a civil servant using its office as an income-maximizing unit."[107] Transparency International (TI), on the other hand defines corruption as "the misuse of entrusted power for private gain."[108] Carl J. Friedrich explains that corruption occurs when a power holder takes actions in favour of any person(s) who provide an unauthorised reward.[109] The World Bank definition states that corruption is the "abuse of public office for private gain." While the Asia Development Bank (ADB) defines it as "the abuse of public or private office for personal gain."[110] Louise Shelley adds that in most developing and post-communist countries, there is an absence of clear boundaries between the public and private sectors. In addition, corruption has at some point also been linked to the work of international agencies such as the UN "oil for food" program.[111]

However, I consider corruption to be a phenomenon that affects both the public and private sector, in developed and developing countries, and perpetrated by state and non-state actors alike. Thus, this work aligns with the definition offered by TI and the ADB encompassing the occurrence of

---

106 Joseph S. Nye, 'Corruption and Political Development: A Cost-Benefit Analysis' (1967) 61 American Political Science Review, 419.

107 Jacob V Klaveren, 'The Concept of Corruption' in AJ Heidenheimer, M Johnston and VT LeVine (eds.), Political Corruption: A Handbook (Transaction Publishers 1989) 25–6.

108 Transparency International (TI) (2008). Frequently Asked Questions About Corruption. Retrieved June 30, 2018, from <www.transparency.org/news_room/faq/corruption_faq#faqcorr1>

109 Carl J. Friedrich, 'Political Pathology' (1966) 37(1) The Political Quarterly 70 at 74.

110 Raymond Baker, John Christensen, and Nicholas Shaxson, "Catching Up with Corruption," The American Interest (September/October 2008) online: <http://www.the-american-interest.com/article-bd.cfm?piece=466. Asian Development Bank, Anticorruption: Our Framework and Strategies, 1998, online: <http://www.adb.org/documents/anticorruption-policy>.

111 Louise Shelley ed., Dirty Entanglements, *supra* note 91 at 66. The UN Security Council initiative, the Oil-for-Food program, started in 1996 to allow Iraq sell oil to pay for food and other necessities for its inhabitants who were suffering under UN sanctions post-Gulf War I. The UN Oil for Food Program was plagued by corruption allegations that some of the profits it generated were diverted to the Iraqi government and some UN officials according to the UN Independent Inquiry Committee. See Paul A. Volcker Richard J. Goldstone, & Pieth, Manipulation of the Oil-For-Food Programme by the Iraqi Regime Oil Transactions and Illicit Payments Humanitarian Goods Transactions and Illicit Payments The Escrow Bank and the Inspection Companies Other UN-Related Issues (Independent Inquiry Committee into the United Nations Oil-For-Food Programme, October 27, 2005) www.iic-offp.org (website not found) but document obtained online: <https://www.files.ethz.ch/isn/13894/ManipulationReport.pdf>.

corruption in both the public and private sector wherein financial institutions and other intermediaries facilitate the obscuring of ill-gotten funds.[112]

2.3.2 Transnational Crimes and Globalization

While globalization may not have created the phenomenon of transnational crime, globalization is linked to its advancement. This linkage plays a part in its current manifestation by widening and changing the actors involved, creating a larger market for illicit activities, and increasing the speed and facilities that enable its proliferation.[113] Louise Shelley for instance, notes that the increase in opportunities brought about by globalization equally creates opportunities for criminals to engage in international expansion of their activities owing to ease of communication and movement of people and goods.[114] For Jay Albanese, the effect of globalization is that the world is effectively shrinking. As a result of such shrinkage, Jay Albanese observes that a shift is occurring from local and domestic enterprises to international schemes that links rapidly connect, the demand for and supply of illicit goods and services across borders.[115]

Globalization refers to the increasing interconnectedness of nations borne out of trade liberalization at the end of the cold war.[116] As part of such liberalization, goods and services flow across state borders together with capital, manufacturing of goods is outsourced to different nations increasing the need for quick movement of goods, and tourism has expanded. Air travel is estimated to have grown at approximately 5% per year over the last 30 years especially with the

---

112 In the following chapters of this thesis (particularly chapters 4 and 5) I highlight the implications of corruption facilitating money laundering using cryptocurrencies.

113 Ibid. Id.

The term 'globalization' describes as "the integration and interaction of people, companies, and government from different nations; it is a process driven by international trade and investment, and facilitated by information technology." See Globalization.org online: < http://www.globalization.org/ What_is_Globalization.html>.

114 Id.

115 Jay Albanese, "Transnational Organized Crime," in Mangai Natarajan (ed.) International Criminal Justice (New York: Cambridge University Press, 2010) 231 at 235.

116 UNODC, The Globalization of Crime: A Transnational Organized Crime Threat Assessment (Vienna: UNODC, 2010) at 29.

introduction of jumbo jets and airline deregulation.[117] In addition to this, it is also estimated that more than 29 million flights transported nearly 2.2 billion passengers in 2007.[118]

Economic disparities amongst nations is heightened as a result of globalization which contributes to the disproportionality between developed and developing societies. International competition has led to the decline in small-scale agriculture. This decline has driven farmers to farm valuable crops and with the rise of the drug trade. Farming of opium, for instance, becomes more attractive to farmers in a bid to support their families. The financial disparities, heightened through globalization, also drive emigration to affluent countries where entry requirements are stringent, and criminals are able to exploit the search for 'greener pastures' through trafficking in persons, smuggling of migrants, and provision of cheap labour.[119]

Consequently, transnational crime groups exploit the opportunities that come with globalization to expand their activities to previously unexploited regions of the world where the legislative framework is corrupt, law enforcement lax, extradition is mostly prohibited, and bank secrecy is robust. In such regions, crime groups are able to obtain profits from illicit activities and integrate them into the legitimate business sector. As a result, illicit globalization can hide easily among the licit; control of crime remains state-based while the operations of criminals move beyond single-state reach.[120]

2.3.3 Transnational Crime and Sovereignty

Closely related to corruption is the effect of transnational crime on state sovereignty. In the context of transnational crimes, the capability of domestic governments to determine what persons or goods and services cross their national borders is an attribute of their sovereignty and enables them

117 Id at 30.
118 Id.
119 Other forms of crime that have 'benefited' from globalization include trafficking arms, endangered species, art, and antiquities; illegal dumping of hazardous waste; and counterfeiting and credit card frauds. See Louise Shelley, "The Globalization of Crime," *supra* note 90 at 3.
120 Id.

to govern effectively. Where their capacity is to do so is lax, crime is able to permeate national frontiers with impunity thereby posing a threat to the sovereignty of the state.

States are traditionally separated by territorial limits. They are also defined by differences in legal systems and levels of economic development. On the other hand, transnational criminal groups have no respect for borders in the process of carrying out their illicit transactions. When such groups consider the differences in jurisdictions, this is done to consider which legal systems are weak and consequently have more favourable markets for their illicit trade, or for storing the proceeds of their crimes.[121] By transcending domestic borders, states efforts are frustrated by the inability to address criminal activity which occurs within their borders. Regardless of the fact that some of the criminal activity occurs within a state's territory, where a crucial element of the crime is beyond territorial reach (such as the alleged offender or the laundered funds), it presents challenges to the individual state seeking to prosecute the criminal activity.

In 1996 when President Bill Clinton of the United States presented the revised National Security Strategy to the US Congress, for the first time he stated that transnational organized crime had become a concern for sovereignty and security in that nation.[122] The sentiment that transnational crime was emerging as a disruption to sovereignty, security, and governance was echoed by different governments in the lead up to the development of a convention on transnational organized crime.[123]

As legitimate non-state activities gained traction, transnational organizations and illicit activities grew alongside them. William Clifford observes that the growth of illicit activities along transnational lines is the natural result of societal changes (such as though globalization) as well

---

121 Jay Albanese, "Transnational Organized Crime," *supra* note 115 at 231. Robert Currie & Dr Joseph Rikhof, *supra* note 72.

122 Fernando Reinares & Carlos Resa. "Transnational organized crime as an increasing threat to the national security of democratic regimes: assessing political impacts and evaluating state responses." NATO (1999) online: <http://www.nato.int/acad/fellow/97-99/reinares.pdf>. citing USG (United States Government) Enlargement and engagement: national security strategy of the United States. (Washington: Government Printing Office, 1996).

123 Id, at 1.

as evolving technology.[124] The crime itself, he argues, stays the same but the number of individuals, and opportunities increase as a result of "urbanization, technological sophistication, and a new worldwide interdependence of our communities."[125]

Despite challenges to the principle of state sovereignty, all states remain formally equal under international law regardless of the fragility of their condition or resources.[126] This demands mutual respect for sovereigns whereby the laws or decrees of one state should not impinge on the sovereignty of another. In response the UNCTOC for instance, emphasizes the purpose of the convention: "promote cooperation to prevent and combat transnational organized crime more effectively.[127] In doing so, states are seeking to close this gap between their ability to combat crime and the transnational activities of criminal actors.

2.3.4 Transnational Crime and Developments in Technology

A linked contributor to the effect of globalization on transnational crime is the continuous advances in technology. Telecommunications and Internet technology create access to information, goods and services. As a result of globalization, such access extends across the globe.[128]

Theories of transnational crime suggest that such crimes are spurred by the desire to make money and the laws of supply and demand for the goods or service in question.[129] Transnational crimes

---

124 William Clifford, "New dimensions in criminality: National and Transnational" (1975) 8:2 Australian and New Zealand Journal of Criminology 67 at 69. Societal changes brought about by influences such as globalization and technology are discussed below in this chapter.

125 *Id.* This statement is unpacked further later in this chapter.

126 This principle of state sovereignty connotes "(a) a jurisdiction, prima facie exclusive, over a territory and the permanent population living there; (b) a duty of non-intervention in the area of exclusive jurisdiction of other states; and (c) the ultimate dependence upon consent of obligations arising whether from customary law or from treaties." See James Crawford, Brownlie's Principles of Public International Law (8th ed.) (Oxford: Oxford University Press, 2012) at 12 and 447.

127 The preamble to the UNCTOC also notes that "Strongly convinced that the United Nations Convention against Transnational Organized Crime will constitute an effective tool and the necessary legal framework for international cooperation in combating, inter alia, such criminal activities as money-laundering, corruption, illicit trafficking in endangered species of wild flora and fauna, offences against cultural heritage and the growing links between transnational organized crime and terrorist crimes, […]."

128 Forms of communication here includes the Internet, email services, use of mobile phone, and other communication devices, etc.

129 Neil Boister, "Further reflections on the concept of transnational criminal law" (2015) 6:1 Transnational Legal Theory, 9.

also involve some form of organizational arrangement amongst the parties involved in the illicit acts through misuse of legitimate forms of business and industry organization.[130] The modern iteration of the theory of transnational crime must also now include its facilitation through technology. The fast-pace of technological developments is such that, law and enforcement mechanisms are constantly left to trail behind. Andre Bossard makes a similar observation when he indicates that transnational crimes take advantage of "all forms of progress, especially international transport […] telecommunications and computers."[131]

Technology has enabled banking and financial institutions to offer rapid money transfer services to customers. Money can move swiftly through several bank accounts in several countries within a very short time. On the other hand, such transactions can take law enforcement officials and banking regulators more than a year to unravel even with the cooperation of law enforcement and banks in the different countries. The reason for this lengthy duration is in part due to the amount of time it takes to detect suspicious transaction together with the time taken to make the necessary link between suspicious transaction and the criminal actors.

More recently, technology advances can be observed with the rise financial technology (FinTech) and blockchain for the financial industry. Amongst other things, financial technology facilitates covert banking transactions and provides unsophisticated criminals with sophisticated tools for achieving their purposes.[132] This new dimension in the factors that facilitate transnational crimes forms the core of chapter 4 of this work and will be discussed there in detail.

2.3.5 Transnational Crime and the Third World Dimension

The distinct relationship between transnational crimes and developing countries is considered here in the context of drug trafficking. Drug trafficking is the most recognized contemporary form of

---

William Clifford, "New dimensions in criminality" *supra* note 124 at 69. Robert Currie & Dr Joseph Rikhof, *supra* note 72 at 325.

130 Jay Albanese, "Transnational Organized Crime," *supra* note 115 at 235.

131 Andre Bossard, Transnational Crime and Criminal Law, *supra* note 88 at 141.

132 Id.

transnational criminal activity.[133] Due to its prevalence, it was initially recognized as the only predicate transnational crime to money laundering in international conventions.[134] Its impact is felt in security and development, and where it is prevalent in fragile societies, the effects are debilitating.[135] Drug traffickers are known to rely on violence to assert and maintain their control over their products and to protect their markets. Consequently, governments determined to tackle its occurrence are compelled to spend a large amount of state resources to combat it, with the consequence that funds earmarked for sustainable development are diverted. For developing countries with limited resources, this further limits the state capacity for societal development. In Mexico, the fight amongst drug traffickers for control over trafficking routes and conflict with the government resulted in violence and instability. An estimated 27,000 homicides were reported over a nine-month period in 2011.[136]

Transnational crimes also flourish in developing countries where governance systems are often fragile. Where governance is weak, transnational crime enterprises operate unfettered generate funds at a magnitude that is arguably more than that generated legitimately in some societies. The crime groups in some instances ensure government reliance on their funds to prevent a complete failure of the state. In doing so, they keep the country's government 'enslaved' to their purpose thereby destabilizing rule of law, infrastructure and social developments, and proper functioning of government.[137] As a result, transaction costs for the transnational crime groups are kept to a minimum and profits increase.[138]

---

133 United Nations Economic and Social Council Commission on Crime Prevention and Criminal Justice, "World Crime Trends and Emerging Issues and Responses in the Field of Crime Prevention and Criminal Justice" Twenty-sixth Session Vienna, 22-26 May 2017, at 14; online: <https://www.unodc.org/documents/data-and-analysis/statistics/crime/ccpj/World_crime_trends_emerging_issues_E.pdf> accessed November 10, 2018.

134 Vienna Convention, *supra* note 38.

135 Id.

136 Jason M. Breslow, "The Staggering Death Toll of Mexico's Drug War," FRONTLINE, July 27, 2015, <https://www.pbs.org/wgbh/frontline/article/the-staggering-death-toll-of-mexicos-drug-war/>.

137UNODC, Drug Money: The Illicit Proceeds of Opiates Trafficked on the Balkan Route (Vienna: United Nations Office on Drugs and Crime, 2015) online <http://www.unodc.org/documents/data-and-analysis/Studies/IFF_report_2015_final_web.pdf>.

138 Id.

In the private sector of some developing economies especially drug producing ones, the revenues generated from illicit trades are sometimes so enormous that they can compete with legitimate businesses for human capital where it offers a better income.[139] On the other hand, much of this revenue is laundered and pocketed by the transnational crime organizations.[140] For instance, a United Nations Office on Drug and Crime (UNODC) Report estimates that the cultivation of opiates contributed one-eighth of Afghanistan's GDP in 2014.[141] This revenue is laundered and deposited in foreign banks, while the poppy farmers receive less than one per cent of the generated profits from the produced and trafficked drugs.[142]

Africa is playing an increasing role in the drug trafficking market: in production, as a transit point, and in terms of consumption.[143] Nigeria, Mali, Ghana, and Senegal are fast becoming transit points for cocaine trafficking between South American and Europe.[144] The South American drug trafficking organizations provide cocaine as payment to the Nigerian crime groups who eventually began purchasing for themselves and evolved from smugglers to wholesalers. The prevalence of such substances further destabilizes the fragile states on the continent, as well as threatening public health with increasing consumption of drugs.[145]

2.4 Money Laundering

The international legislative instruments examined in this work all contain definitions of money laundering in a way that reveals the evolution of transnational crimes over the years. The United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substance (Vienna Convention) definition of money laundering has trafficking in drugs as its only predicate

---

139 id.
140 Id.
141 Id at 19.
142 Id.
143 See Aïssata Maïga and Elizabeth Tompkins, "West Africa's New Drug of Choice: The Rise of Methamphetamine" (Stockholm: Institute for Security and Development Policy, June 12, 2014), 1–2. The Nigerian traffickers have gone even further to engage in synthetic drug production, especially methamphetamine due to weak chemical and pharmaceutical controls, and easily export through porous transit routes in West Africa as a result of laxity in enforcing rule of law. See also United Nations Office on Drugs and Crime, Transnational Organized Crime in West Africa: A Threat Assessment (Vienna: UNODC, 2013), 10–11, http://www.unodc.org/documents/data-and-analysis/tocta/West_Af- rica_TOCTA_2013_EN.pdf.
144 Id.
145 Id.

offence.[146] At the time of the convention, trafficking in drugs had experienced accelerated growth, placing it at the forefront of international concern over transnational crimes. Subsequently in the UNCTOC, money laundering applies to the "widest range of predicate offences" reflecting international recognition of other equally important offences linked to money laundering[147]

The UNCTOC in article 6 defines money laundering as the "conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her action." The International Monetary Fund (IMF) explains it simply as the process whereby the illegal source of profits is disguised to obscure the link between an original criminal activity (the predicate offence) and its financial proceeds.[148] The Financial Actions Task Force (FATF) defines money laundering as "the processing of criminal proceeds to disguise their illegal origin" and "legitimize" the ill-gotten gains of crime."[149] These show that every step in the laundering process (described below) and every person facilitating the completion of that process is caught within the definitions above. Beyond these definitions, scholars explain money laundering as the conversion of cash into a financial instrument or asset that can be used without revealing the illegal source of the funds.[150]

2.4.1 Money Laundering: Placement, Layering, and Integration

There are three stages in the laundering of the proceeds of crime in order to obscure their link to predicate crimes: placement (wash), layering (spin), and integration (dry).[151] These stages do not necessarily occur consecutively. With changes in methods of money laundering and the rise in

146 Vienna Convention, *supra* note 38.

147 UNCTOC, *supra* note 34, article 2 (2).

148 International Monetary Fund, Factsheet: The IMF and the Fight Against Money Laundering, *supra* note 9.

149 FATF, "What is Money Laundering? Basic Facts About Money Laundering", online: <http://www.fatf-gafi.org/MLaundering_en.htm>.

150 Marco Arnone & Leonardo Borlini, "International anti-money laundering programs: Empirical assessment and issues in criminal regulation" (2010) 13:3 Journal of Money Laundering Control 226 at 236. Bruce Zagaris also describes a three-stage cycle of placement, layering, and integration of illicit funds. See Bruce Zagaris, "Money Laundering and Counterterrorism Financial Enforcement" in Bruce Zagaris, *supra* note 36 at 67.

151 Bill Kte'pi, "Money Laundering: Methods" in Margaret E. Beare (ed.) *Encyclopedia of Transnational Crime supra* note 83 at 262-264.

financial technology, the stages are not intended to represent a closed list for the money laundering process. For instance, legitimately generated funds can be transferred from a bank account in one country to an account in another country without detection by either banking officials or law enforcement authorities.

Placement (the wash cycle) involves depositing the illegally derived funds (often in the form of cash) into financial institutions. By this process (known as smurfing), large sums of cash are broken down into smaller, less conspicuous quantities and deposited over time into a single account or multiple bank accounts.[152] Placement may also involve drafting an employee of a banking institution to create an illegitimate opening for depositing the funds, thereby providing an air of legitimacy. The aim in both instances is to evade banking secrecy laws designed to combat money laundering such as the detailed AML requirements on banking institutions in the FATF Recommendations.[153]

Layering involves creating financial transactions that mask the source of the funds and inhibit the ability of authorities to trace the origin of the funds (spin cycle). The proceeds of crime are given a clean appearance often by mixing them with legitimate funds. Layering could be achieved through casinos because it is predominantly a cash-based industry. For instance, casino chips could be purchased using illicit funds, the chips could then be converted back to cash, thereby giving the illicit funds a legitimate appearance. [154] Layering is also achieved through the buying and selling

---

152 Through international conventions or agreements, it has become the norm that cash transactions over US$10,000 require reporting by financial institutions. In this regard, smurfing is employed where by deposit of amounts of just under the said reporting limits are made in multiple banks over a period of time, using multiple depositors. See David C. Hicks, "Money Laundering: Vulnerable Commodities and Services" in Margaret E. Beare (ed.) *Encyclopedia of Transnational Crime*, *supra* note 83.

153 The FATF Recommendations require reporting of transactions above a certain limit deemed suspicious and carrying out due diligence often referred to as Know Your Customer (KYC) whereby the customer's details and details of the transaction is verified. More details of KYC and reporting obligations are provided in the next chapter.

154 The B.C. government in 2017 hired Peter German to conduct an independent investigation on how widespread money laundering is at casinos in the Lower mainland following a report by MNP LLP found in one instance that approximately $13.5 million in $20 denomination were accepted by Richmond's River Rock casino in July 2015. See Peter M. German, An Independent Review of Money Laundering in Lower Mainland Casinos Conducted for the Attorney General of British Colombia (2018), online: <https://news.gov.bc.ca/files/German_Gaming_Final_Report.pdf>. Recently in British Columbia, the Attorney General points out that gaps in the AML legislation provisions in BC whereby cash purchases of high-end vehicles inadvertently being used to launder the proceeds of crime and introduce illicit funds into society because such transactions do not require reporting. See Justin McElroy, "B.C. to ask Ottawa for more tools to fight money laundering" CBC News Mar 26, 2018 online: <http://www.cbc.ca/news/canada/british-columbia/bc-ottawa-eby-trip-march-2018-1.4593444>.

of assets (property, luxury goods) to obscure the source of the funds especially where the monitoring of such purchases is lax.[155] Intermediaries such as lawyers are also used during this stage to create purchase securities in bearer form using a lawyer's trust account.[156]

Given the level of complexity that the launderers employ to obscure the source and/or origin of the funds, the use of FinTech in financial transactions is attractive to launderers for concealing the proceeds of crime.[157] It follows that Internet-based financial transactions using cryptocurrencies represent a distinctive peak in the advances in Internet-based financial transactions. Anti-money laundering (AML) institutions continuously strive to close loopholes that enable money laundering through traditional banking platforms. In light of this, cryptocurrencies could grow in attraction to launderers where it serves the purpose of providing anonymity for launderers and obfuscating links their predicate illicit activities.[158]

The integration stage of money laundering is the final step in obscuring the link to predicate crimes required to assimilate the funds back into the legal economy. The rationale for integration is that "the economic realities associated with the opportunity cost of money means that a portion of the criminally derived money will need to be invested in other endeavors, regardless of whether they are legal or illegal."[159] The common method employed in reintegrating proceeds of crime into legitimate society (known as the buy-back technique)[160] is illustrated as follows: Mr. X has illicit funds obtained from drug trafficking. He uses the funds to invest in a failing hotel business on the contractual terms which include a monthly payment plan that represents recoupment of his investment. There are no changes in the hotel and it does not make any money but still manages to pay out to Mr. X every month. By doing this, Mr. X has cleaned and reintegrated his funds into

---

155 Daniel Adeoye Leslie, Legal Principles for Combatting Cyberlaundering (Basel: Springer, 2014) at 15.

156 Id.

157 It has already been identified that pre-paid debit cards for instance are sometimes used in facilitating money laundering although the extent or magnitude of this occurrence is not known nor is it the subject of this work but it will be discussed in a little more detail in the chapter 4.

158 This is the subject of chapter 4 of this work.

159 Kris Hinterseer, Criminal finance: The political economy of money laundering in a comparative legal context (The Hague: Kluwer Law International, 2002) at 19. See also Doug Hopton, Money Laundering: A concise Guide for all Businesses (London: Gower, 2009) at 3.

160 Daniel Adeoye Leslie, *supra* note 155.

the legitimate economy.[161] Upon completion of these steps, the launderer would successfully achieve conversion of their bulk cash, conceal the origin and ownership of funds, and essentially create an alibi for the funds.[162] The newly legitimized funds can now be used in continuing the crimes or for other licit purposes.

2.4.2 Money Laundering and Transnational Crime

Money laundering is a necessary facilitator in the perpetration of predicate or underlying transnational crimes.[163] The nexus between money laundering and other transnational crimes can be seen from two dimensions.

First, transnational crimes serve as a source for the funds that require obscuring through the process of money laundering. Because the crimes captured under this category generally involve a financial element, and are sustained by generating funds that are used to further perpetrate the predicate crimes, it follows that if the funds generated cannot be ploughed back into the illicit activities or for the daily activities of the perpetrators, their source of income (i.e. the transnational crimes) is inhibited.

Due to the illicit nature of the predicate crimes, the funds cannot simply be deposited with traditional banking institutions without any questions asked. By law, such funds constitute the proceeds of crime and are subject to seizure and confiscation upon detection.[164] The proliferation of AML regulations requires due diligence on the part of banking institutions to ensure legitimacy of transactions and proper identification of customers (Know Your Customers (KYC)). The AML regulations also impose reporting requirements where transactions are considered suspicious. Given that the funds are required by the illicit actors to further perpetrate the predicate crimes and

161 Id.

162 Stephen Schneider, "The Incorporation and Operation of Criminally Controlled Companies in Canada (2013) 7:2 Journal of Money Laundering Control 126. See also Peter M. German, An Independent Review of Money Laundering in Lower Mainland Casinos, *supra* note 154.

163 Cyrille FIjnaut, "Transnational Crime and the Role of the United Nations" *supra* note 86 at 122.

164 The international framework for asset seizure is discussed in the next chapter.

for their livelihood, such actors continue to seek out new ways to obscure the link between their transnational crimes and their funds.

Money laundering also serves as a financial source for facilitating other transnational crimes. Here the crimes facilitated after obscuring the source of funds are referred to as the postdicate crimes. The techniques for money laundering to facilitate the financing of terrorist activities, for instance, are essentially the same as for concealing the link with the predicate crimes. The funds used for financing terrorist activities may have legitimate or illegitimate origins. However, it is necessary to obscure the link to its origins.[165] If the funds are successfully concealed, they can be used to support future terrorist activities.

The FATF recommends criminalizing the financing of terrorist activities as predicate offences for money laundering. Contrary to most forms of transnational crimes, terrorist financing occurs in the aftermath (post) of the laundering of funds. Therefore, it may be more appropriately described a 'postdicate' crime to money laundering or more generally as an underlying offence even though its link to money laundering is much the same as predicate offences.[166] As such the objective is not so much the generation of funds as it is the perpetration of terrorist activities. The funds themselves may not be illicit in themselves but are laundered to obscure the link to the terror which they seek to finance. It is also worth noting that in the instance of postdicate offences, the source of the funds may be legitimate such as donations to foundations or charities that are in turn used to fund terrorist activities. The FATF Recommendation for instance requires states in this regard to consider extending the scope of their AML framework to non-profit organizations or charities to ensure that such organizations are not operating used to disguise illicit purposes.[167]

---

165 International AML instruments criminalize terrorist financing. Such instruments include the UN Convention on Financing of Terrorism and the FATF Recommendations which was modified in 2012 to integrate the Special Recommendations on Terrorist Financing into the original Recommendations.

166 See *supra* note 38.

167 FATF, International Standards on Combatting Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations (Paris: FATF, 2012).

2.5 Problems with Combatting Transnational Crime through Tracing the Proceeds of Crime

The methodology of addressing transnational crimes by focusing on the proceeds of the predicate crimes involves a 'follow the money' approach: by tracking the funds to their origin, one will be led to the perpetrators of the predicate crimes. In doing so, the proceeds of crime are targeted and by correlation, underlying crimes are tackled without reverting to the challenging process of obtaining victims' testimonies.[168]

Research by the International Monetary Fund (IMF) suggests that the magnitude of the money laundering problem equates to about 2 to 5 per cent of the global GDP.[169] This estimate is much quoted in literature though now dated given that the research is nearly two decades old. Peter Reuter goes as far as to note that efforts by the FATF between 1996 and 2000 towards producing estimates on the sheer size of global money laundering failed.[170] The Australian Institute of Criminology report published in 2004 aimed at proffering some sort of estimates in money laundering in Australia puts the number at somewhere between AUD$2.8 and 6.3 billion.[171]

This wide margin in the figures – commonly referred to as a "dark figure" in the criminology and sociology disciplines[172] – is somewhat problematic and also evidence of the difficulty with quantifying money laundering. Even if the more conservative of those numbers are taken, the problem is still an enormous one. Various agencies with AML mandates point out that the amount of money being laundered is exorbitant and continues to rise. This in turn facilitates financial,

---

168 Problems with relying on victims in the context of transnational crimes is especially significant where the predicate offences involve traumatization of the victims through sexual, physical, and emotional abuse. Requiring such victims to recount their ordeal may in cause them to relive horrifying experiences.

169 Id.

170 Peter Reuter & Edwin M. Truman, Chasing Dirty Money: the Fight Against Money Laundering (Washington DC: Institute for International Economics, 2004) at 4.

171 Approximately between CAD$ 2.6 and 5/7 billion. See John Stamp & John Walker, "Money laundering in and through Australia" (2004) 342, Trends & issues in crime and criminal justice No. 342. (Canberra: Australian Institute of Criminology) online: <https://aic.gov.au/publications/tandi/tandi342>.

172 See Anthony Walsh & Craig Hemmens, *Introduction to Criminology: A Text/Reader*, 3rd ed. (Thousand Oaks: Sage, 2014).

social, and political corruption; and supports organized criminals, human and firearms trafficking, and finances terrorism.[173]

On the basis of the 'crime as business' understanding of transnational crimes, it follows that inhibiting opportunities for money laundering would have a correlating effect on the cycle of the transnational crime businesses. This would be the outcome as the incentive (political or personal gains)[174] to continue with those crimes diminishes.

2.6 Underlying Transnational Crimes

This section highlights some types of transnational crimes. All transnational crime can be categorized as 'international smuggling activities',[175] emphasizing the common feature of cross-border transportation of illicit, licit but controlled or highly taxed goods. Transnational crimes include trafficking or smuggling of drugs, human beings, migrants, child pornography, embargoed or pirated technology, pirated textiles, conflict natural resources, cigarettes, vehicles, protected animals, protected cultural artefacts, organs, information, etc.[176] This list is not a closed one. The category of transnational crimes continues to expand and transform.[177] As demonstrated above, globalization creates the opportunity for criminals to increase their networks across domestic borders has the ability to increase continually expands with changes in society as a result of globalization and increase in the network of criminals across borders which in turn opens up previously untapped illicit markets.[178]

---

173 Cyrille FIjnaut, "Transnational Crime and the Role of the United Nations, *supra* note 86.

174 Louise I. Shelley & John T. Picarelli, "Methods and Motives: Exploring Links between Transnational Organized Crime and International Terrorism" (2005) 9:2 Trends in Organized Crime 52 at 53.

175 Klaus von Lampe, "The Practice of Transnational Organized Crime" in Felia Allum & Stan Gilmour (ed.) *supra* note 14 at 187. I use the term 'smuggling' in a very lose sense, acknowledging that in field of transnational crime, smuggling and trafficking are different concepts, not least because the motivations therein differ. See Anne T. Gallagher, The International Law of Human Trafficking, ed. (Cambridge: Cambridge University Press, 2010) at 3.

176 Id.

177 This observation is also reflected in the AML regime categorization of predicate and postdicate offences as "all serious crimes" – departing from the Vienna Convention conception of drug trafficking as the only predicate offence to money laundering).

178 Though beyond the scope of this thesis is the phenomenon of cybercrimes (hacking, cyberattacks), facilitated by advances in technology, which does not necessarily involve 'smuggling' but whose effects pervade domestic borders.

Given the impracticality of examining the list above, my focus will be on two underlying crimes, drug trafficking (predicate) and terrorist financing (postdicate).

To do this, the predicate offences of drug trafficking together with the postdicate offence of terrorist financing will be described in brief. Drug trafficking is chosen as the most developed and documented form of transnational crime facilitated by money laundering. On the other hand, terrorist financing is chosen as its transnational nature highlights the role of money laundering from a different perspective to most transnational criminal activity, given that it occurs in the aftermath of the money laundering transaction.

2.6.1 Drug Trafficking

As the first illicit activity (initially the only one) to be recognized as a transnational crime, an overview of drug trafficking is essential in examining transnational criminal activity. Even with the diversification of transnational crime over time to other forms of illicit activities, drug trafficking continues to play a significant role in organized crime. Research reveals that illicit drug trafficking constitutes the single largest organized crime market in Europe.[179]

Calculating the global value of drug trafficking is particularly difficult as evidenced in varied estimates from different organizations. For instance, the UNODC in its 2017 World Drug Report estimates that the proceeds from drug trafficking represent the second largest income of transnational crime groups (second only to "counterfeiting in a broad range of goods") with the most recent figures placing the income here at $426 to $652 billion out of the transnational crime market estimated market value of $1.6 trillion to $2.2 trillion in 2014.[180]

---

179 Europol, European Union Serious and Organised Crime Threat Assessment (SOCTA) (Hague: European Police Office, 2013).

180 United Nations Office on Drugs and Crime, "World Drug Report 2017" online: <https://www.unodc.org/wdr2017/field/Booklet_1_EXSUM.pdf> at 23. To exemplify the gravity of the problem, a previous World Drug Report by UNODC in 2005 placed the estimate at $230 billion. See United Nations Office on Drugs and Crime, "World Drug Report," 2005: 2, accessed September 27, 2010, <http://www.unodc.org/pdf/ WDR_2005/volume_1_web.pdf>.

The FATF in the late 1980s was one of the first organizations to estimate that the amount of illicit drug trafficking proceeds laundered accounts for two-thirds of the billions of dollars estimated above.[181]

The proceeds of trafficking in drugs are laundered through a diverse range of methods. The laundering of these funds mostly follows one or all of the three-pronged process of money laundering detailed above. The laundering of such proceeds also predominantly occurs in sectors with weaker monitoring mechanisms and a greater opportunity for infiltration.[182] Such sectors include: cash-based businesses (restaurants, red-light entertainment), labour intensive operations, and the gaming industry.[183] The proceeds are also laundered through the purchase of property and construction companies, luxury goods like yachts and jewellery, and investment in offshore centres.[184]

2.6.2 Terrorism Financing

Terrorism constitutes a grave challenge facing all societies today. A problem compounded by globalization, terrorism continues to pose a significant threat to international peace and societal stability. It causes severe human devastation in terms of injury and the loss of lives. Terrorism also undermines governmental authority, as well as economic and social development.

The international community has taken greater recognition of terrorism financing following the 9/11 terrorist attacks in the United States. In doing so, alternative means of financial remittances

---

181 *Id.*at 25. Other research is in line with this estimate with literature emanating from the US, Australia, and the Netherlands placing the average proceeds laundered at an average of 70 per cent. See John Walker, "Estimates of the extent of money laundering in and through Australia," for Australian Transaction Reports and Analysis Centre, (Queanbeyan: John Walker Consulting Services, 995); John Walker and Brigitte Unger, "Measuring Global Money Laundering: the Walker gravity model" 5 (2009) Review of Law and Economics; Douglas Farah, "Money Laundering and Bulk Cash smuggling: challenges for the Mérida Initiative" (2010) in Working Paper Series on U.S.-Mexico Security Cooperation Woodrow Wilson Centre for Inter- national Scholars/Trans-Border Institute).

182 United Nations Office on Drugs and Crime, "World Drug Report 2017, *supra* note 180 at 26.

183 *Id.*

184 Id. In overseas or offshore centres bank secrecy laws make for nearly anonymous operations. Locations such as Switzerland, the Cayman Islands, Panama, Hong Kong, and Singapore make for a fertile environment for deposit of laundered funds. Anonymity, undocumented transactions, lax banking regulations, and inexpensive bribery are some of the features that facilitate laundering in some of these locations. See David Hicks & Adam Graycar "Money Laundering" in Mangai Natarajan, ed., International Crime and Justice (Cambridge: Cambridge University Press, 2010) 171.

have come to the forefront of regulatory attention. Alternative means of financial remittance such as Hawala, Western Union, and MoneyGram provide a crucial service in many parts of the world, allowing individuals in diaspora to send money to family members in their countries of origin. Although such services come at a steep cost, they are often preferred by individuals who do not own bank accounts. Significant, in the context of this work, is the Hawala mechanism, used predominantly in Asia.[185] Hawala had been on law enforcement radar for some time but concrete action only became pertinent in the wake of 9/11.[186] The importance of the Hawala mechanism for this work is that parallels are often drawn between its operation and that of cryptocurrencies. Although Hawala does not necessarily utilize technology such as internet facilities for its, it does not require the disclosure of personal information; nor a central issuance or remittance authority.[187]

The provision of financing for terrorist activities is now recognized as a transnational crime. Article 2 of the UN Convention on the Suppression of the Financing of Terrorism defines terrorist financing: "where a person commits or aids the commission of terrorism through finance with the aim of furthering some criminal activity or purpose."[188]

---

185 The hawala is an informal and mostly low-technology money remittance mechanism based given that it is based on mutual trust between the parties to the transaction. Here money is made available internationally without moving it or leaving a record of the transaction. It can be likened to the Western Union remittance service. The FATF defines alternative remittance mechanisms such as hawala as "a financial service that accepts cash, cheques or other monetary instruments or other stores of value in a location and pays a corresponding sum in cash or other form to a beneficiary in another location by means of a communication, message, transfer or through a clearing network to which the MVT (money or value transfer) service belongs [Financial Action Task Force (FATF), "Combatting the Abuse of Alternative Remittance Systems: International Best Practices," Special Recommendation VI (SR VI) (Paris, France: FATF/GAFI, 2003). Available online at http://www.oecd.org/fatf/pdf/SR6-BPP_en.pdf. The FATF issued an interpretative note to SR VI in February 2003, online: <http://www.oecd.org/fatf/pdf/INSR6_en.pdf>. This will be unpacked further in chapter 4.

186 The Federal Bureau of Investigations (FBI) in the U.S. claims that its investigations into the 9/11 tragedy revealed that the hijackers received funds through a hawala mechanism. See U.S. General Accounting Office (GAO), Terrorist Financing: U.S. Agencies Should Systematically Assess Terrorists' Use of Alternative Financing Mechanisms (Washington, DC: U.S. GAO, 2003) at 19, online: <http://www.gao.gov/new.items/d04163.pdf>.

187 Victor Dostov & Pavel Shust, "Cryptocurrencies: an unconventional challenge to the AML/

CFT regulators?" (2014) 21:3 Journal of Financial Crime 249 at 253. Parallels can also be drawn in the characteristics of both such as speed, lower transaction costs, cultural convenience, versatility, and potential anonymity. See Elizabeth Joyce "Expanding the International Regime on Money Laundering in Response to Transnational Organized Crime, Terrorism, and Corruption" in Philip Reichel (ed.) *supra* note 76 at 80.

188 Convention on the Suppression of the Financing of Terrorism.

Financing of terrorism is closely linked with money laundering.[189] Research emanating from the UNODC links the objective of curbing money laundering and transnational organized crime to that of curbing terrorism financing.[190] Notably, the FATF, in October 2001, extended its AML mandate to the fight against terrorism financing. To operationalize this additional mandate, the FATF adopted Special Recommendations to supplement the initial Recommendations.[191] The UN Security Council (UNSC) at the same time (post-9/11) adopted resolution 1373 towards the prevention and suppression of the financing of terrorism. In the resolution, the UNSC also notes the nexus between "international terrorism and transnational organized crime, illicit drugs, money laundering, illegal arms-trafficking, and illegal movement of nuclear, chemical, biological and other potentially deadly materials, and in this regard emphasizes the need to enhance coordination of efforts on national, sub regional, regional and international levels in order to strengthen a global response to this serious challenge and threat to international security."[192]

This highlights the centrality of financial means in facilitating terrorism. Given that such activities are criminalized, terrorism financiers would be concerned with ensuring they obscure the link between themselves and the terrorists. This in turn creates the need to adopt money laundering methods.

2.7 Conclusion

This chapter has demonstrated that money laundering facilitates transnational crimes. It also showed how various factors contribute to the growth of transnational crimes. These catalysts, as I

189 For instance, see UN Security Council Resolution 1373 adopted by the Security Council at its 4385th meeting, on 28 September 2001 (S/RES/1373 (2001).

190 Information on the Law Enforcement, Organized Crime and Anti-Money-Laundering Unit of UNODC notes that it has the mandate of implementing the Global Programme against Money-Laundering, Proceeds of Crime and the Financing of Terrorism. See online: <https://www.unodc.org/documents/money-laundering/GPML-Mandate.pdf>.

191 The FATF eventually harmonized its AML Recommendations by incorporating the Special Recommendations on terrorism financing into main text of the Recommendations. See FATF, "International Standards on Combatting Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations" (Paris: FATF, 2018) available online: < http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>.

192 UN Security Council Resolution 1373 adopted by the Security Council at its 4385th meeting, on 28 September 2001 (S/RES/1373 (2001). The details of these instruments and others are examined in more detail in the next chapter of this work.

refer to them, are corruption, globalization, state sovereignty, technological advancements, and the third world dimension.

As the above evaluation pointed out, globalization and technological developments continue to bring societies closer to one another. By doing so, they also widen the reach of illicit markets. The extent to which such illicit markets are widened is not examined and may be a problem to be examined in future research.

Corruption and state sovereignty are intertwined as they could work together to create an enabling environment for transnational crimes. Corrupt practices affect both public and private institutions. Where corruption occurs in the context of public authorities, the sovereignty of the state is jeopardized. By accepting personal gratification, the independence of domestic authorities is compromised and the perpetrators of transnational crimes (in this context) are able to influence state policy concerning their areas of operations. For transnational crimes such as drug and human trafficking, such criminal actors affect the implementation of policy on security, immigration, and any other policy issue which the government can implement.

Perpetrators of transnational crime are also able to exploit third world countries. Drug trafficking, for instance, often involves violence and interference with the security of the state. As a result, states, often those with already with limited resources, tend to expend what they do have in protecting their territory from the activities of traffickers. This is seen, for instance, in the context of the cost of trafficking in Mexico for instance.

The second part of this chapter provided an overview of money laundering in the context of transnational crimes. Thus far, the amount of illicit funds laundered across the globe has eluded accurate quantification. However, the modest estimates presented above show the gravity of money laundering, and how transnational crimes (including money laundering) are facilitated by certain factors (the catalysts) identified above.

The painstaking attention to detail in laundering the proceeds of crime, often using the three stages of money laundering identified above (placement, layering, and integration) points towards a deliberate effort by criminal actors to mystify their illicit activities in order to prevent detection

and confiscation of the enormous proceeds of their crimes; and also, to avoid prosecution by law enforcement authorities.

In this chapter, I have argued that a policy which seeks to combat the laundering of funds will also be useful in curbing transnational crime. Above, I have referred to the 'crime as business' model pursuant to which transnational organised crimes are often perpetrated for profit. Blocking the opportunity to launder the proceeds of such crimes could disincentivize the criminal actors from engaging in illicit activities.

Academic research relating to methods of terrorist financing, shows that money launderers will turn to the next mechanism that promises to make their illicit activities less traceable or vulnerable to seizure.[193] It follows that technological developments that add further complexity to the laundering process by enabling further obfuscation of their activities would likely be embraced by illicit actors. This work will examine the extent to which cryptocurrencies could advance the objective of mystifying the laundering process that facilitates transnational crimes.

In the next chapter, I will present an overview and evaluation of the current international AML regime. This analysis will serve as a segue to the rest of the thesis which examines how cryptocurrencies facilitate money laundering and transnational crimes. The key provisions of the international AML regime examined in the subsequent chapter are crucial in evaluating whether money laundering using cryptocurrencies could be addressed within the existing framework.

193 Elizabeth Joyce "Expanding the International Regime on Money Laundering," *supra* note 186 at 85.

Chapter 3: The International Anti-Money Laundering Regime

The international community has taken several steps in response to concerns about the rise in money laundering activities and the illicit activities they facilitate. While the exact nature of the steps taken vary across institutions, a common thread amongst them is a recognition that with each new iteration of technological development comes new dimensions in (transnational) crimes.

The underlying strategies of these AML initiatives is aimed at weakening the power of terrorist or other criminal organizations by curtailing their economic capabilities.[194] To achieve this, it is important to tackle the opportunities that enable such perpetrators to launder the proceeds of their crimes.[195]

Such efforts commenced (on the international scene) with the adoption of the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substance (Vienna Convention) in 1990. [196] This treaty recognized the transnational nature of both money laundering and drug trafficking. Although drug trafficking was recognized as the only predicate offence to money laundering in the Vienna Convention, subsequent international instruments identify more crimes as predicate (and postdicate) to money laundering. Such crimes include trafficking in persons, smuggling of migrants, and terrorist financing.[197]

While initiatives to tackle money laundering comprise of treaties, such as the Vienna Convention mentioned above, it also includes guidelines, recommendations, policy papers, and best practices

---

194 Kristen E. Boon, Aziz Huq, and Douglas C. Lovelace, Terrorism: Commentary on Security Documents vol. 106 (Terrorist Financing and Money-laundering) (Oxford: Oxford University Press, 2010) at 379.

195 Id.

196 Vienna Convention, *supra* note 38. Money laundering is recognized as the only predicate offence to money laundering in the Vienna Convention. At present. the Vienna Convention has 87 signatories and 190 parties.

197 As detailed earlier in this work (in both chapters 1 and 2), predicate offences are initial 'substantive' crimes, perpetrated for financial gain, the proceeds of which require obfuscation (laundering) in order for the criminal actors to utilize them within legitimate society without tracing back to its criminal origin. Pursuant to article 6(2)(b) of the UN Convention on Transnational Organized Crime (UNTOC) all "serious crimes" constitute predicate offences to money laundering. In chapter 2 of this work, I demonstrate that the term 'postdicate' offences more appropriately reflects the relationship between money laundering and terrorist financing. In this context, money laundering occurs before the 'serious crime' of terrorist financing, thus the objective of its perpetrators is not so much the generation of funds. Rather the objective is facilitating terrorist activity and the funds are not necessarily illicit.

that all work together under the framework commonly referred to as the international AML regime. In considering the extant international AML mechanisms, the scope of this chapter will be limited to a select few international instruments that together make up the international anti-money laundering (AML) regime. They include: the Vienna Convention, United Nations Convention on Transnational Organized Crime (UNCTOC), United Nations Convention Against Corruption (UNCAC), and the International Convention for the Suppression of the Financing of Terrorism (the CFT Convention).[198] I have chosen these instruments as they are the treaty-based instruments within the international AML regime. In addition, I have included the Financial Actions Task Force (FATF) Recommendations as one of the instruments to be examined.[199] The FATF Recommendations (though technically 'soft-law') are recognized to be effective and persuasive in dealing with the problem of money laundering within the international financial system, and have become foundational in the international AML regime. [200] Beyond these chosen instruments, a host of other inter-governmental and non-governmental policy institutions contribute to the success of the AML regime by creating forums to support and coordinate AML initiatives by domestic

198 Vienna Convention, supra note 38. UNCTOC, *supra* note 34. The UNCTOC enjoys relatively wide acceptance with 147 signatories and 189 ratifications. UNCAC, *supra* note 38. CFT Convention, *supra* note 34.

The FATF Recommendations, *supra* note 38. FATF membership comprises 37 countries, 2 regional institutions (European Commission and the Gulf Cooperation Council), 3 observer countries, associate members (regional organizations) and observer organisations (made up of various international and regional financial and security minded institutions such as African Development Banks, Basel Committee on Banking, and the International Monetary Fund (IMF). The level of involvement in the FATF by other established international institutions is a credit to its influence since from the time of its inception. FATF, "Members and Observers" online: < http://www.fatf-gafi.org/about/membersandobservers/>.

200 Chris Brummer, "How International Financial Law Works (and How it Doesn't)" 99 (2011) *Georgetown Law Journal* 257. Customary international law is part of the foundation of international law and a principle qualifies as such where it has attained the status of jus cogens and state practice. See for instance, James Crawford, Brownlie's Principles of Public International Law , *supra* note 126 at 23-30. Malcom Shaw defines soft law as "instrument or provision […] not of itself 'law' but its importance in the general framework of international legal development is such that particular attention requires to be paid to it." See Malcom Shaw, International Law (6th ed.) (Cambridge: Cambridge University Press, 2008) at 117. Anthony Aust refers to customary international law as having two elements: evidence of substantial uniform practice by a number of states; and opinion juris i.e. a general recognition by states of settled practice enough to amount to a binding obligation under international law (Anthony Aust, Modern Treaty Law and Practice, 3rd ed. (Cambridge: Cambridge University Press, 2013) at 13. The Recommendations are widely adopted by states, have become very persuasive, especially due to FATF's intermittent publication of lists of non-cooperative countries and territories (NCCTs), which states are eager to avoid. Over time, the FATF recommendations especially, have gained recognition and emulation in most countries (even through creation of FATF-style national and regional bodies who take up the FATF mandate) leading to arguments that it has attained the status of customary law in the field of AML law. See Daniel Adeoye Leslie, *supra* note 155 at 120.

agencies.[201] Key amongst these institutions are the United Nations Security Council,[202] the International Police Organization (Interpol),[203] and the International Monetary Fund.[204] The initiatives of these bodies with respect to money laundering, while relevant, are beyond the parameters of the LLM thesis but are cited where it is necessary to do so.

Furthermore, focusing on international initiatives in the first instance is pragmatic. Earlier in this work, I demonstrated that transnational crimes pervade domestic borders. Concentrating on international instruments therefore aligns with the recognition that the issues under consideration are not within the exclusive jurisdiction of any given state. This approach, in turn, accords with the New Legal Realism framework and methodology chosen for this work. Gregory Shaffer, for instance, notes that the parameters of transnational networks and the problems that arise in that context necessitate that an international perspective be used in tackling them.[205]

3.1 The AML Framework

In this chapter, the international AML initiatives I have chosen for analysis have been categorized under the following themes: prevention, prosecution/enforcement, and international cooperation.

---

201 Other include: Organisation for Economic Co-operation and Development (OECD) – The OECD Project against Illicit Tax Competition; The Basel Group of Bank Supervisors in connection with its revised standards for assessing risk to bank capital; the Egmont Group of Financial Intelligence units, an informal group of financial intelligence units for cooperation and informational sharing. Standards have also emanated from the European Union and although they are not the subject of the present research, including the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, May 16, 2005; the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, November 8, 1990; Directive 2005/60/EC: European Parliament and Council Directive on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.

202 United Nations Security Council (UNSC) Resolution 1373, *supra* note 189, mandating member countries to deny safe havens to terrorist groups by inhibiting avenues for financing.

203 Interpol's Global Complex for Innovation located in Singapore, created its own digital currency to combat cryptocurrency fuelled crime and as a training tool for law enforcement agencies. The organization also conducts working groups on the Darknet and cryptocurrencies. See Interpol "International Global Complex for Innovation, *supra* note 63. See also Interpol, "INTERPOL holds first DarkNet and Cryptocurrencies Working Group: Altcoins identified as serious law enforcement challenge" April 3, 2018, online: < https://www.interpol.int/en/News-and-media/News/2018/N2018-022>.

204 Its research on AML/CFT includes "Compliance with the AML/CFT International Standard: Lessons from a Cross-Country Analysis;" "Research Projects: An Overview of projects on AML/CFT;" "Recent Developments in International Monetary Fund Involvement in Anti-Money Laundering and Combating the Financing of Terrorism Matters;" "Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism;" "Regulatory Frameworks for Hawala and Other Remittance Systems;" "Money Laundering - Muddying the Macroeconomy;" "The Methodology for Assessing Compliance with Anti-Money Laundering and Combating the Financing of Terrorism Standards."

205 Gregor Shaffer, "New Legal Realism in International Law" in Heinz Klug, Elizabeth Mertz, & Sally Engle Merry, *supra* note 56.

This grouping is intended to highlight certain issues that are essential in understanding the global AML regime.

Preventative measures deal with the steps that inhibit opportunities for money laundering. These measures place emphasis/burden on the role of financial institutions as well as non-financial institutions involved in financial transactions. The theme of prosecution/ enforcement focuses on the illicit acts that must be criminalized by states pursuant to the international AML regime. Finally, the theme of international cooperation focuses on other aspects of the AML regime that recognize the transnational nature of the problem: mutual legal assistance, extradition, and asset recovery.

3.1.1 Preventive Measures

3.1.1.1 Customer Due Diligence (CDD)

The typical customer due diligence (CDD) requirements are detailed in the FATF Recommendations. This part of the AML regime has to do with measures such as due diligence (know your customer (KYC)), record-keeping, reporting, supervision, and applicable sanctions for any failure to comply. Their aim is to counter bank secrecy laws of domestic jurisdictions as states are now required to ensure such laws do not prevent the domestic implementation of CDD provisions.[206]

These requirements place the burden of effecting CDD on financial institutions, third parties or intermediaries, and relevant non-financial institutions.[207] The core requirements of the CDD

---

206 FATF Recommendations, r9 at p12. Previously bank secrecy laws and policies dictated that financial institutions maintain confidentiality concerning certain client information such as identify keep certain information about their customers private. Accordingly, banks could not disclose information concerning its customers to anyone, including law enforcement authorities, without the customer's specific permission. See Duncan E. Alford, "Anti-Money Laundering Regulations: A Burden on Financial Institutions" (1994) 19:3 N.C. J. Int'l L. & Com. Reg. 437 at 441.

207 'Financial institutions' as defined by the FATF constitutes a person (natural person or legal entity) conducting (including but not limited to) one of the following business practices on behalf of a customer:

Acceptance of deposits and other repayable funds from the public; The transfer of money or value, which includes financial activity in both the formal and informal sector, for example, alternative remittance activity, excluding any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds. See Financial Action Task Force International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation. See

provisions mandate all businesses handling large sums of money to report such transactions to the authorities where they regard such transactions as suspicious.[208] For instance, recommendation 10 of the FATF Recommendations provides that CDD is required where a business is being established with a customer, where transactions are carried out above the "applicable designated threshold of USD/EUR 15,000", or where there is suspicion of money laundering or terrorist financing.[209] To ensure CDD has been performed effectively, the FATF Recommendations suggest that customer and beneficiary identify verification is conducted using independent data, information regarding the transaction is obtained, and on-going due diligence is performed throughout the course of the relationship with the client to maintain KYC requirements.[210]

The FATF Recommendations (r15) also make provision for the development of new technologies. As a preventive measure, recommendation 15 stipulates that providers of virtual currency asset services be regulated from an AML perspective. This provision requires licencing and registration of such services to ensure they can be effectively monitored, and that they comply with the measures contained within the Recommendations.[211]

The objective of this aspect of the AML regime is for the institutions to satisfy themselves that they are dealing with *bona fide* clients and if they suspect something unusual, to comply with the

---

<http://www.fatfgafi.org/media/fatf/documents/recommendations.pdfs/FATF%20Recommendations%20(approved%20February%202012)%20reprint%20May%202012%20web%20version.pdf>. p. 115).

According to the FATF Recommendations, "Designated non-financial businesses and professions means: a) Casinos; b) Real estate agents; c) Dealers in precious metals; d) Dealers in precious stones; e) Lawyers, notaries, other independent legal professionals and accountants; f) Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under these Recommendations".

208 Caroline Doughty, "Know your customer: Automation is key to comply with legislation" (2005) 22:4 (Business Information Review) 248 at 248.

209 Id.

210 FATF Recommendations at r10. The beneficial owner is explained by the FATF Recommendations as "the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement." The inclusion of beneficial owner is intended to target "smurfing" where transactions are conducted at the instance of another attempt to disguise the true identity of the beneficiary. See FATF Recommendations, "General Glossary" at p110.

To buttress the point on customer identification, the Wolfsberg Group recommendations provide that the identity of customers should be disclosed to enough of the banking staff as a means of undertaking requisite due diligence. The Wolfsberg Group is a consortium of international banks (including Barclays, Citigroup, Goldman Sachs) that set standards to ensure uniformity in measures against money laundering. See further online: <http://www.wolfsberg-principles.com/index.html>.

211 Together with the FATF guidance on virtual currencies, this provision is especially significant for CCs and the following chapter will analyse it in more detail.

duty to report such suspicious transactions to the relevant regulatory authorities.[212] These CDD provisions are significant because they essentially alter banking practices that previously facilitated (intentionally and otherwise) money laundering.[213]

Furthermore, non-adherence to the AML rules dealing with CDD results in sanctions for offending financial and non-financial institutions. FATF recommendation 35 dictates that the countries themselves are to ensure that criminal, civil, and administrative sanctions are put in place within their respective jurisdictions.[214] Such sanctions include but are not limited to the imposition of financial and criminal sanctions on the directors and senior management of financial institutions, as well as on the institutions themselves.[215] A comprehensive analysis of the effectiveness of such sanctions on financial institutions is beyond the scope of this work. However, it is worth mentioning that hefty sanctions have occasionally been imposed on banks in the past for weaknesses in their AML policies (distinguished from an actual engagement of money laundering practices). For instance, in July 2015, a fine of $140 million was imposed on Citigroup by US federal and California regulators for purported AML weaknesses in its subsidiary, Banamex.[216] A $300 million fine was also imposed on Standard Chartered for lapses in its AML standards in 2014.[217] In these instances, the sanctions were imposed for inadequate AML controls at the financial institutions even though there were no identified instances of actual money laundering.

---

212 Id.

213 Daniel Adeoye Leslie, *supra* note 155. Banking secrecy policies were previously legally mandated or in some instances, voluntarily adopted by regions and financial centres around the world guaranteeing confidentiality of client transactions. See Black's Law Dictionary, 10th ed., *sub verbo* "Bank Secrecy. Rule 9 of the FATF Recommendations also requires states to ensure that their banking secrecy laws do not inhibit the implementation of FATF Recommendations.

214 FATF Recommendations

215 Id.

216 Citigroup, Press Release, Citigroup Statement on Banamex USA (July 22, 2015), online: <http://www.citigroup.com/citi/news/2015/150722a.htm.>; see also Jude Joffe-Block, "Banamex USA Bank to Pay $140 Million Fine and Shut Down," KJZZ (July 23, 2015), http://kjzz.org/content/169775/banamex-usa-bank- pay-140-million-fine-and-shut-down.>.

217 Written Agreement Between Standard Chartered Bank and New York State Department of Financial Services, Consent Order Under New York Banking Law §§ 39 and 44 (Aug. 19, 2014), online: <http://www.dfs.ny.gov/about/ea/ea140819.pdf>.

3.1.1.2 Reporting, Monitoring, and Detection

Various AML rules provide that upon reasonable suspicion that funds constitute the proceeds of crime, or relate to the financing of terrorist activities, that the financial institution where such transaction is to take place should report such activity to the applicable financial intelligence unit (FIU).[218] In fulfilling this requirement, financial institutions are prohibited from notifying ("tipping off") a customer that their activity is or has been reported as suspicious to the relevant authorities.[219]

As part of their reporting obligations, the AML rules indicate that banking staff should receive training on key indicators, monitoring, and detection of suspicious activities.[220] For instance, article 29 UNCTOC provides that each state party shall "initiate, develop, or improve specific training programmes for […] personnel charged with the prevention, detection, and control of the offences covered by the Convention."[221] Such programmes should include training on routes and techniques used in committing offences, detecting and monitoring the movement of proceeds of crime, and their disguise or concealment.[222] Importantly, article 29 requires training on

---

218 FATF Recommendations, R20. Financial Intelligence Units are defined in the revised statement of the Egmont Group of Financial Intelligence Units in 2004 as "A central, national agency responsible for receiving (and as permitted, requesting), analyzing and disseminating to competent authorities, disclosures of financial information: i. concerning suspected proceeds of crime and potential financing of terrorism, or ii. required by national legislation or regulation, in order to combat money laundering and terrorist financing." See The Egmont Group, Revised Statement of Purpose (June 23, 2004), <http://www.egmontgroup.org/>. The UNCTOC adopts this definition and explains in article 7(1)(b) that each member state "[…] shall consider the establishment of a financial intelligence unit to serve as a national centre for the collection, analysis, and dissemination of information regarding potential money laundering" (UNCTOC, *supra* note 34). See also FATF Recommendation at R29.

219 FATF Recommendations, R21(b).

220 See Paul Alan Schott, *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* (World Bank Publications, 2006) online: <https://elibrary.worldbank.org/doi/abs/10.1596/978-0-8213-6513-7> at VI-19-20. For instance, a very high account turnover not commensurate with the balance size or the withdrawal of assets immediately after deposit.

221 See UNCTOC, *supra* note 24 at article 29(1). See also, recommendation 18 of the FATF Recommendations, which requires financial institutions to develop programmes against money laundering and terrorism financing across all branches and subsidiaries, wherever located. In the interpretive note to recommendation 18, the suggestion is for such programmes to include ongoing employee training, policies, procedures, and screening policies when hiring staff. To encourage the reporting of suspicious activities, financial institutions and their employees are protected from criminal and civil sanctions for any alleged violation of confidentiality when such reporting was done in good faith.

222 Id. at 29(1) (b).

"combatting organized crime committed through the use of computers, telecommunications networks or other forms of modern technology.[223]

Article 52 of UNCAC goes further to specify provisions that enable states to prevent and detect the transfer of proceeds of crime relating to customer identification, especially where the accounts in question are high value accounts.[224] This provision emphasizes the monitoring of accounts for bank clients, particularly politically exposed persons, for whom the identity of their family members, and close associates should also be scrutinized.[225] Furthermore, article 52 also stipulates that in furthering the aim of prevention and detection of proceeds of crime, states should implement measures that regulate the establishment of banks that have no physical presence or affiliation with a regulated financial group.[226]

To encourage the reporting of suspicious activities, the FATF Recommendations specify that financial institutions and their employees are protected from criminal and civil sanctions for any alleged violation of confidentiality when such reporting was done in good faith.[227]

In addition to financial institutions, FATF recommendation 23 also provides that designated non-financial businesses and professionals are required to report suspicious transactions on the basis of their due diligence obligations.[228] The intent appears to be the capture of all forms of financial transactions and avoidance of defences on the basis that an operator does not come within the traditional understanding of banking facilities. FATF Recommendations, though not binding, provide for the implementation of dissuasive sanctions to be applied to financial institutions and

---

223 Id at article 29(1)(h). The importance of this requirement will be explored further in the next chapter.

224 See also The CFT Convention, article 18(b).

225 This requirement recognises the prominent public function of certain government officials and the high risk for potential involvement in corrupt practices by virtue of their position. It does not recognize the import of private officials such as government contractors who could also be considered politically exposed persons by virtue of their interaction with government agencies. As demonstrated in chapter 2 of this work, corrupt practices occur beyond the realm of public authorities.

226 Although its nature is still the subject of much contention (to be discussed in the next chapter), the applicability of this provision may be used to regulate the conditions of its operations to ensure that in instances where it may be used to facilitate money laundering, tracing efforts are not hampered by lack of domicile of the particular cryptocurrency involved.

227 FATF Recommendations, R21(a). This provision is also contained in the other AML instruments, see for instance CFT Convention at article 18(b)(iii).

228 Id, R23.

designated non-financial institutions that fail to comply with their reporting obligations under the relevant AML obligations.[229]

The Convention on Financing of Terrorism (CFT Convention) contains similar provisions to the UNCTOC and UNCAC on the prohibition of account opening by unidentified or unidentifiable holders or beneficiaries. State parties, under the CFT Convention, are also required to implement measures imposing obligations on financial institutions report all "complex, unusual large transactions and unusual patterns of transactions, which have no apparent economic or obviously lawful purpose."[230]

In complying with the reporting, monitoring, and detection obligations, the financial institutions and their officials are not expected to be able to detect all incidents of money laundering. The FATF has clarified that while it "expects financial institutions to identify, assess and understand their money laundering and terrorist financing risks and take commensurate measures in order to mitigate them, this does not imply a "zero failure" approach."[231] This point is significant and could neutralize the burden on financial institutions. This is especially so given the complexity of money laundering schemes that are primarily aimed at avoiding detection by bank officials.

3.1.1.3 Supervision

Article 14 of the UNCAC, in terms similar to article 7 of the UNCTOC, pronounces that each state

> *shall* institute a comprehensive domestic regulatory and supervisory regime for banks and non-bank financial institutions […] that provide formal or informal services for the transmission of money or value and, where appropriate, other bodies particularly susceptible to money laundering […] emphasize requirements for and, where appropriate, beneficial owner identification, record-keeping and the reporting of suspicious transactions [emphasis added].[232]

---

229 Id, R35. Details can be found above in the previous section.

230 CFT Convention at article 18(b)(iii).

231 FATF Press Release, "FATF Clarifies Risk-Based Approach: case by case not wholesale de-risking" October 23, 2014, online: < http://www.fatf-gafi.org/publications/?hf=10&b=0&s=desc(fatf_releasedate)>.

232 UNCAC supra note 38. See also CFT Convention, article 18(2)(a) & (b). FATF at r26-28 also contains provisions of effective supervision to ensure compliance with AML rules by financial institutions and non-financial business persons.

The framing of this provision, in comparison to the UNCTOC and Vienna Convention, is more encompassing as – unlike the UNCTOC and the Vienna Convention – it recognizes the role of informal money transfer services in money laundering.

Another relevant provision in the UNCAC on the supervision of financial institutions is article 14(3) which mandates state parties to consider implementing procedures towards regulating money remitters on electronic funds transfers, to ensure proper documentation of the payment chain for such transfers, and to enhance the scrutiny applied to transactions where the details of the parties involved are absent.[233]

3.1.2 Prosecution/ Enforcement

3.1.2.1 The Money Laundering Offences

For the purpose of combatting money laundering, certain activities are noted in the various instruments under consideration as money laundering offences with the intention that they be criminalized by the member states.

The term used in the UNCTOC in this context is the 'laundering of the proceeds of crime'. Amongst other things, the Convention criminalizes the "conversion or transfer of property […] for the purpose of concealing or disguising the illicit origin […] knowing that such property is the proceeds of crime."[234]

The UNCTOC provides that all serious offences constitute predicate crimes for money laundering and urges states to apply the convention to the widest range of predicate offences whether or not committed within the jurisdiction of the particular state.[235] A serious offence means "conduct

233 Id.

234 UNCTOC, *supra* note 34, at article 6(1)(a). Crime in the context of this provision refers to all predicate offences.

235 Id at article 6(2)(a) - (c). The Vienna Convention recognises drug trafficking as the only predicate offence for money laundering. The provisions in the UNCAC (art 23) requiring states to criminalize money laundering offence is similar to the UNCTOC. All serious crimes are considered predicate offences for the purpose of the convention. A serious offence means "conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty." .

constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty."[236]

The UNCTOC urges that state parties should criminalize money laundering whether committed within or outside the domestic borders of a given state.[237] The conversion or transfer of property knowing that such property is the proceeds of a crime for the purpose of disguising its illicit origin, and the concealment of the true nature or source of property, are some of the conduct identified for criminalization in the convention.[238]

In addition to the criminalization of the act of laundering the proceeds of crime, article 5 of the UNCTOC also provides that states should criminalize participation in an organized criminal group.[239] This offence includes agreeing with one or more persons to commit a serious crime (the predicate offences) for the purpose of obtaining financial or material benefit or engaging in conduct with the knowledge, intent, or agreement to achieve a criminal aim. By formulating participation in an organized criminal group in this way (agreeing with one or more persons) this provision seems wide enough to encompass more informal (loose) criminal associations that may not have a typical organizational structure that is traditionally associated with organized crime groups. It could also include one-off associations and criminal networks that are linked through technological infrastructure. This is discussed further in chapter 5.

The UNCTOC also urges states to consider adopting measures that detect and monitor the movement of cash and appropriate negotiable instruments across borders.[240] However, given the complexities in the nature of cryptocurrencies, it would seem that detecting and monitoring the movement of such instruments (other than cash) may be much more challenging than initially

---

236 UNCTOC, supra note 34 at article 2. All serious crimes are considered predicate offences for the purpose of the convention.

237 Id at article 6.

238 Id at article 6. Recommendation 3 of the FATF Recommendations is framed in similar terms.

239 An organized criminal group is defined in article 2(a) UNCTOC as "a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit."

240 Id, article 14(2).

anticipated at the drafting of the convention.[241] The UNCAC recognizes and seeks to address this challenge. By Article 14(3) of the UNCAC, member states are mandated to consider implementing procedures that regulate "money remitters" on electronic funds transfers, to ensure proper documentation of the payment chain for such transfers, and that enhance the scrutiny applied to transactions where the details of the parties involved are absent.[242] The FATF Recommendations similarly recognizes the emerging role of money or value transfer services such as money remittances in facilitating money laundering.[243]

The CFT convention does not criminalize money laundering explicitly. Instead, the convention frames the offence of money laundering slightly differently, stating that an offence is committed, for the purpose of the convention, where any person "(1) […] *by any means*, 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" an offence defined in the CFT Convention (emphasis added).[244] The approach here is broad enough to include provision or receipt of funds for terrorist activities whether or not such funds are obscured. In doing so, the postdicate nature of terrorist financing becomes apparent. Also evident is the criminal intent of the actors in this context who are not necessarily as preoccupied with concealment as they are with the achievement of a terrorist objective. Accordingly, scholars note that unlike other transnational crimes, the motivation for terrorist financing activities to make a political statement.[245]

The CFT Convention defines funds as:

---

241 This is discussed further in chapter 4.

242 UNCAC, article 14(3). Although the term money remitter is not defined in the UNCAC, the FATF Recommendations categorizes money remittances as money or value transfer services and therefore non-bank financial institutions. See FATF Recommendations – Glossary.

243 See FATF Recommendations – Glossary.

244 CFT Convention, article 2(1) (a)-(b). The offence referred to in the CFT Convention includes an offence within the scope of any treaty annexed to the CFT Convention or the commission of an act with the intent that it causes serious bodily harm or death to a person not taking active part in armed hostilities.

245 Louise Richardson, *What Terrorists Want* (London: John Murray, 2006) at 14; Martin Innes & Michael Levi, "Terrorism and Counter-Terrorism" in Rod Morgan, Mike Maguire & Robert Reiner (eds.) *The Oxford Handbook of Criminology*, 5th ed. (Oxford: Oxford University Press, 2012) at 665.

> *assets of every kind*, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including, but not limited to, bank credits, travelers checks, bank checks, money orders, shares, securities, bonds, drafts, letters of credit (emphasis added).[246]

The framing of this definition by the CFT convention is quite comprehensive. Due to such an exhaustive definition of assets, categorizing cryptocurrencies one way or another (for instance, as a negotiable instrument or digital technology) almost becomes moot – though important in its own right – for the purpose of establishing liability for its use in money laundering.[247]

3.1.3 International Cooperation Provisions

To reiterate the assertion made at different points so far throughout this thesis, the cross-border nature of transnational crimes demonstrates that international cooperation is essential. This approach ties in with the New Legal Realism (NLR) theoretical framework. Legal realists were previously concerned with law and the actors therein in the broader social (but domestic) context. They were also preoccupied with international relations from the perspective that interstate relations were the only concerns within which problems in international law emanate. The NLR theory goes beyond legal realism to recognize that globalization affects both economic and cultural situations of society in a manner that is contrary to the state of affairs which existed at the time when the legal realism approach was initially propounded.[248]

---

246 Id, article 1(1). Other instruments in the international AML regime in substantially similar terms also define funds in this manner.

247 The issue of whether CCs could be categorized as assets for the purpose of this provision is discussed further in the following chapters.

248 Gregory Shaffer, "The New Legal Realist Approach to International Law" *supra* note 54 at 189. The three pillars of jurisprudence identified by Brian Tamanaha are moral theorizing as in natural law, analytical jurisprudence as with legal positivism, and historical jurisprudence where law is assessed in relation to society. See Brian Z. Tamanaha, "The Third Pillar of Jurisprudence: Social Legal Theory," (2015) 56:6 *Wm. & Mary L. Rev*. 2235 at 2237.

This NLR theoretical approach is applicable in the context of transnational crimes. So far, this work has found that with increasing opportunities for cross-border crimes (as facilitated by globalization) efforts by any singular country to tackle them effectively within their domestic laws face heightened difficulties.[249] Thus, money launderers rely on the differences among countries with regards to their domestic AML regime (particularly those jurisdictions found to have less stringent AML laws) as a means of facilitating their operations.[250] Therefore, international cooperation is crucial in order to prevent particular jurisdictions with less stringent AML laws from becoming safe havens for launderers.

A similar reflection on the NLR approach is likewise important as technologies that could facilitate such crimes emerge. In existing literature, scholars have observed that the essentiality of interstate dialogue in dealing with emergent technologies is nothing new.[251] In other contexts, collective state action has been employed where technological developments intersect with public policy.[252] Thus, when it comes to enforcement, mutual legal assistance (as discussed below) plays a crucial role as elements of the transnational criminal transaction or tracing of the proceeds of crimes necessitate the involvement of multiple jurisdictions.

3.1.3.1 Mutual Legal Assistance (MLA)

The goal of MLA is to achieve an efficient administrative system in investigating criminal cases with transnational aspects.[253] MLAs are founded on the international law principle of sovereignty whereby every state has jurisdiction to investigate and enforce its own criminal law to the

---

249 In the 'suppression conventions' referred to in chapter 1, states are obliged to assist one another in their efforts to supress the illicit activities which the conventions aim to curb. The UNCTOC and UNCAC both refer in their preambles to the importance of international cooperation among states on the relevant matters, as do most of the other international instruments. The FATF recommendations also emphasize the importance of intensifying cooperation among domestic authorities in the fight against money laundering.

250 Paul Alan Schott, Reference Guide to Anti-Money Laundering, *supra* note 220 at I-6.

251 See Isaac Pflaum & Emmeline Hateley, "Bit of a Problem: national and extraterritorial regulation of virtual currency in the age of financial disintermediation" (2013) 45 Georgetown Journal of International Law 1169 at 1196. Tony Porter, "Technical Collaboration and Political Conflict in the Emerging Regime for International Financial Regulation" (2003) 10:3 Review of International Political Economy 520.

252 *Id.*

253 Robert J. Currie & Dr Joseph Rikhof, supra note 72 at 515.

exclusion of other states. In order to access the jurisdiction of another state for this purpose, a request for assistance is required.[254]

MLA is "the process whereby one state provides assistance to another in the investigation and prosecution of criminal offences […] such as in the provision of evidence for use abroad, search and seizure of evidence used in foreign proceedings, transfer of witnesses for interview or to give testimony, and the service of documents originating in another state."[255] It does not include arrest or detention with a view to extradition, or transfer of persons in custody abroad for sentencing or for criminal proceedings, although these factors play a role in the framework of AML.[256]

The importance of MLA in money laundering can be observed from a simple scenario. The proceeds of drug trafficking, for instance, are taken out of the country where the drugs were trafficked and deposited in another country (the placement step). Subsequently, these proceeds were transferred through various other financial (and non-financial) institutions in different countries (layering step), and then dispersed to various corporations in any country of choice (integration step). The authorities of the initial country would be unable to conduct their investigations, trace the proceeds of the crime, or prosecute the alleged trafficking without the assistance of law enforcement of the other relevant countries.[257]

The MLA provisions under article 7 of the Vienna Convention are extensive. These provisions require, for instance, that parties are to "afford the *widest measure of mutual legal assistance*[258] in investigations, prosecutions, and judicial proceedings in relation to criminal offences […]" (emphasis added) to achieve any of the aims listed in 7(2).[259] Pursuant to article 7(5), parties may

---

254 Id at 516.

255 Id at 515 citing William C. Gilmore (ed.), Mutual Assistance in Criminal and Business Regulatory Matters (New York: Cambridge University Press, 1995) at xii.

256 Arrest or detention with a view to extradition, or transfer of persons in custody abroad for sentencing or for criminal proceedings, are separate issues although these play a role in the framework of AML. See William C. Gilmore, supra note 255.

257 George J. Kriz, "International Co-operation to Combat Money Laundering: The Nature and Role of Mutual Legal Assistance Treaties" (1992) 18:2 Commw. L. Bull. 723 at 726.

258 See also article 18 UNCTOC and r37 FATF Recommendations.

259 Vienna Convention Article 7(1) and (2) paraphrased. This includes taking evidence, serving documents, executing searches and seizures, providing copies of relevant documents and records, including bank, financial, corporate, or business records, tracing proceeds and other instrumentalities for evidentiary purposes.

not refuse to assist a requesting state on the basis of bank secrecy rules. The UNCTOC contains similar provisions but in article 18, it goes on to add, in this context, that assistance to other states shall be rendered "where the requesting State Party has reasonable grounds to suspect that the offence referred to in article 3, paragraph 1 (a) or (b), is transnational in nature, including that victims, witnesses, proceeds, instrumentalities or evidence of such offences are located in the requested State Party and that the offence involves an organized criminal group."[260]

UNCTOC contains MLA provisions in articles 7 and in 18 described above. Article 7(1)(b) of the UNCTOC stipulates that member states should ensure that their authorities are dedicated to combating money laundering and have the ability to cooperate and exchange information with other authorities, whether domestic or international. Article 7(4) of the UNCTOC also adds that states are also to work towards developing and promoting cooperation at all levels (domestic, regional, bilateral, global) towards combatting money laundering.

The provisions of the CFT convention are prefaced by the need for international cooperation with respect to all of the measures within the CFT convention directed at combatting terrorist financing. The provisions on MLA in the CFT convention is no different. For instance, article 18(3) provides that "States Parties shall *further cooperate in the prevention of the offences* set forth in article 2 by exchanging accurate and verified information in accordance with their domestic law and *coordinating administrative and other measures taken*, as appropriate, to prevent the commission of offences set forth in article 2, […] (emphasis added)." Achieving this requires "(a) establishing and *maintaining channels of communication between their competent agencies* and services to facilitate the secure and rapid exchange of information concerning all aspects of offences set forth in article 2; (b) *cooperating with one another in conducting inquiries*, with respect to the offences set forth in article 2, concerning: (i) the identity, whereabouts and activities of persons in respect of whom reasonable suspicion exists that they are involved in such offences; (ii) the movement of funds relating to the commission of such offences" (emphasis added).[261]

---

260 Article 18(1) UNCTOC, *supra* note 34.
261 See also r 37 and 40 of the FATF Recommendations.

FIUs are also mandated by the FATF Recommendations to engage in mutual information sharing and cooperation, and to facilitate the provision of MLA by the requisite law enforcement authorities.[262] Given that money laundering and transnational crime in general is taking on new dimensions due to globalization and technological advancements, such crimes will often touch on the jurisdiction of multiple states, either as requesting or requested states. Consequently, MLA becomes increasingly significant for an effective AML regime as states require greater assistance from each other.

3.1.3.2 Recovery of Assets

Recovery of (stolen) assets is the term used to describe efforts by international and domestic law enforcement to identify, trace, confiscate, and return the proceeds of crime. [263] Such efforts are typically aimed at reclaiming state assets embezzled by corrupt high-level government officials. Recovery of assets is an important component of international cooperation as the assets are often hidden in foreign jurisdictions. Proceeds are usually hidden in foreign banks, real estate property, vehicles, and precious metals, etc.[264]

Tracing, as an element of asset recovery, is a crucial causal link between the identified offender or criminal activity and the funds sought.[265] Technology enhances tracing but it is also used in obfuscating the link between the illicit act and its proceeds. This part of the AML framework is often one of the most challenging for authorities as illicit actors go to great lengths to ensure that any links between the proceeds of their crimes and the criminal activity are completely obscured. Unravelling this labyrinth requires advanced skill and expertise on the part of law enforcement

---

262 FATF Recommendation 40 Interpretive notes, paras. 7, 8, and 9. The AML regime requires, in substantially similar terms, that member countries assist each other upon request and "spontaneously" if needed.

263 Mark V. Vlasic & Gregory Cooper, "Recovery of Stolen Assets" in Margaret E. Beare (ed.), Encyclopedia of Transnational *supra* note 83 at 2, online: <http://sk.sagepub.com/reference/download/transntlcrime-justice/n138.pdf>.

264 Id. the next chapter will consider the extent to which cryptocurrencies could be used to conceal and cart away such funds.

265 Daniel Adeoye Leslie, *supra* note 155 at 151.

officials. This is especially the case the proceeds of crime or ill-gotten funds are intertwined with legitimate funds or transformed into some other form of asset.[266]

Recovering the proceeds of crime is one of the objectives of AML not just for punitive purposes but also as a means of eliminating a major facilitator of transnational crime.[267] For many criminals, deprivation of their funds is thought to be a worse consequence than spending some time in prison and subsequently enjoying the proceeds of their crimes upon release.[268] Furthermore, asset recovery is an important strategy in combatting transnational crimes where the beneficiaries of the assets (proceeds of the predicate crimes) are elite actors who employ others to perpetrate the predicate offences. As a result, even when a predicate offence is established, such elite actors are unlikely to serve the attaching penal sanctions. By targeting their finances, the criminal organization may eventually be dismantled.[269] The strategy of asset recovery is also important for the relevant state where the recovered assets can be used in developing the economy or compensating victims.

The task of asset recovery is usually facilitated by MLA requests to obtain information that may otherwise be protected, such as bank records.[270] The framework for such requirements are contained in the AML provisions. Pursuant to article 5(4) of the Vienna Convention, for instance, a request for confiscation of assets can be made by a party having jurisdiction over an offence

---

266 Despite the challenges, there are also identified successes. In 2005, the Nigerian efforts at recovering the proceeds of government funds looted by the late former military dictator, General Sani Abacha, amounted to a total of $ 1.2 billion. This was possible as a result of requests for designation (identification) of the Abacha family as a criminal organization, and the seizure and confiscation to jurisdictions such as Liechtenstein, Switzerland and Jersey. Success is also recorded concerning lootings by Ferdinand Marcos of the Philippines, Jean-Claude "Baby Doc" Duvalier of Haiti, Vladimiro Montesinos, the former head of the Peruvian intelligence service. See Mark V. Vlasic & Gregory Cooper, "Recovery of Stolen Assets" supra note 263.

267 The World Bank estimates that the value of cross-border illicit flow of funds is $ 1.6 trillion, with half of that amount coming from developing economies. From a development perspective, it is easy to see the far-reaching effects of such activities and the importance of combatting it. See UNODC/The World Bank, Stolen Assets Recovery (StAR) initiative: Challenges, opportunities and action plan (2007) online: <http://www.siteresources.worldbank.org/NEWS/Resources/Star-rep-full.pdf> at p. 9.

268 Katalin Ligeti and Michele Simonato, "Asset Recovery in the EU: Towards a Comprehensive Enforcement Model beyond Confiscation? An Introduction" in Katalin Ligeti and Michele Simonato (eds.) Chasing Criminal Money: Challenges and Perspectives on Asset Recovery (Oxford: Hart Publishing, 2017) at 1. This assumption is the subject of some contention. See for instance Criticism to such an assumption has been expressed, for example, by Hans Nelen, "Hit Them Where It Hurts Most?" (2004) 41 Crime, Law & Social Change 517.

269 Id.

270 Id.

within the provisions of the convention, to another party within whose jurisdiction the proceeds of crime are placed. The procedure for effecting such request is detailed therein, as is the duty to dispose such proceeds placed on the confiscating state.[271] The convention requires that when a request for such proceeds are made, the confiscating state may consider coming to an agreement with the requesting state on contributing the proceeds to international efforts to fight illicit trafficking in drugs, or sharing the assets with other parties in accordance with any relevant recovery of assets agreements.[272]

Similarly, article 12(1) of the UNCTOC provides for confiscation and seizure of the proceeds of crime or property of corresponding value (where such proceeds have been transformed into other types of assets). This article also requires state parties to adopt measures to ensure the relevant authorities are able to identify, trace, seize or freeze the proceeds of crime including proceeds that have been transformed or converted. Article 12(6) UNCTOC adds that together with the aim of confiscation of assets, enabling provisions shall be put in place to respond to a request by another state party towards confiscation. Such requests are made possible in the UNCTOC under article 13. This article requires that upon receipt of a request from another jurisdiction for confiscation of proceeds situated within its jurisdiction, the receiving state must ensure that it acts to the "greatest extent possible within its domestic legal system" to give effect to the request.[273] Such efforts extend to initiating tracing, freezing, or seizure proceedings towards that objective.[274]

The provisions of the UNCAC on the subject of confiscation of proceeds of crime are much more extensive than those of the preceding conventions. This is likely due to the enormity of sums often associated with corruption by public officials who maintain high level public office positions.[275] As mentioned earlier in this section, recovery of assets is mainly used to recover funds embezzled by high-level corrupt officials. Consequently, the UNCAC makes the return of assets a

---

271 Articles 4 and 5 of the Vienna Convention.

272 Article 5 Vienna Convention.

273 Similar requirements are contained in article 55 UNCAC.

274 UNCTOC, article 14 also contains administrative requirements for making such a request as well as procedure for disposal of proceeds along lines similar to article 5 of the Vienna Convention.

275 See Daniel Adeoye Leslie, Legal Principles for Combatting Cyberlaundering, *supra* note 155 at 151.

fundamental principle of the convention and mandates states to offer one another the widest possible assistance and cooperation.[276]

To further the aim of international cooperation, article 54 of the UNCAC also provides that each member state is to provide MLA as is necessary to give effect to an order of recovery of assets used in the commission of an offence contained in the convention. Such an order may be given in the courts of another jurisdiction or be issued by the requested member state itself pursuant to a request from another state. This article also urges members to consider permitting such confiscation whether or not a criminal conviction is obtained, given that in certain instances (flight or death for instance) offenders cannot be prosecuted.

In detailing the requirements for recovery of assets, the CFT convention dictates that states should take appropriate measures aimed at the identification, detection, freezing or seizure of any funds used in or derived from the commission of offences within the context of the convention.[277] It also recommends that states should enter into agreements on the utilization of confiscated funds, including its use for compensating victims and their families.[278]

Similarly, the FATF contains recommendations on the recovery of assets. Pursuant to recommendation 38 and interpretive notes, the FATF Recommendations provide that "countries should ensure that they have the authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize and confiscate property laundered; proceeds from money laundering, predicate offences and terrorist financing; instrumentalities used in, or intended for use in, the commission of these offences; or property of corresponding value." In its interpretive notes to recommendation 38, states are urged to consider establishing a fund where all or a portion of

276 UNCAC, article 51.
277 CFT, article 8.
278 Id at 8(3) & (4).

any confiscated funds are deposited for use by law enforcement, health services, or other similar purpose particularly where such funds are a result of cooperative law enforcement efforts.[279]

3.1.3.3 Jurisdiction and Extradition

The jurisdiction and extradition aspects of AML is important given the difficulties in determining where a crime actually takes place in the context of AML, with components of the crimes likely taking place in different jurisdictions. In transnational crimes, there may be differences between the physical location of the perpetrator, the physical manifestations of his actions, the electronic manifestations of his actions, and where the effects are felt.[280] These differences are discernable both for the predicate/postdicate conduct and the money laundering dimension of this conduct, further confounding the problem. When technological developments for instance in the context of finance or communications are added to the mix, the complexity of the scenario multiplies.

Each affected country in any of the above stages could assert jurisdiction under the principles of jurisdiction in public international law – territoriality, passive personality, protective, or nationality.[281] Where more than one state wishes to take up prosecution in such a cross-border scenario, it sets up a situation of concurrent prescriptive jurisdiction and potential for inter-state conflict.[282]

Given the differences in procedural and substantive criminal law amongst states, as well as the fragmented international AML framework, the resulting lack of uniformity in regulation and enforcement could lead to certain countries inadvertently becoming "crime havens" on account of

---

279 The rationale for such provisions, also seen in the context of the conventions above, is unclear but the reference to collaborative efforts in the FATF interpretive notes suggests the complexity that may be associated with splitting such funds or of allowing the country in whose jurisdiction the funds are deposited to keep the entire recovered assets. This seems to be the happy medium.

280 Robert J. Currie & Dr Joseph Rikhof, "Transnational Crimes of International Concern" *supra* note 72 at 423.

281 James Crawford, "Jurisdictional Competence" in Brownlie's Principles of Public International Law, *supra* note 125 at 456-464. Territoriality principle gives jurisdiction to a state where a criminal act is committed. Nationality principle gives jurisdiction to a state over its nationals whether the acts are committed within their jurisdiction or extraterritorially. Passive personality principle enables a state exercise jurisdiction over harmful acts by aliens which affect its own nationals. The protective principle, also referred to as the security principle enables a state exercise jurisdiction over acts done abroad that affect its internal or external security or other state interests e.g. currency or immigration offences. See James Crawford, *id*.

282 Id.

their relatively lax laws.[283] This presents a problem for extradition purposes where the principle of "double criminality" is required for extradition to take place.[284] Robert Currie and Joseph Rikhof give the example of a Canadian ("X") who sets up an online gambling business using a server from a state where gambling is legal.[285] When investigations into X's actions are commenced in Canada, X flees to that state which is unlikely to extradite X given that his conduct is legal according to their laws.[286]

Extradition seeks to facilitate the suppression of crime by addressing loopholes that permit an individual to evade criminal responsibility. Extradition is based on the international law principle, *aut dedere aut iudicare* (prosecute or extradite) and is reflected in the AML instruments under consideration.[287]

For instance, signatories to the Vienna Convention are required to ensure that domestic legislation is enacted which gives them jurisdiction, on the basis of prescriptive jurisdiction as discussed above, over offences established in accordance with article 3(1).[288] Where a convention offence is committed outside a state's territory with a view to commission within its territory, a state may also exercise jurisdiction.[289] The convention also provides for the duty to prosecute or extradite

---

283 Id.

284 Extradition is defined as "the formal rendition of a criminal fugitive from a state that has custody (the requested state) to the start which wishes either to prosecute or, if the fugitive has already been convicted of an offence, to impose a penal sentence (the requesting state). Double criminality requires that the conduct in question must be a criminal act in the requesting state as well as the requested state. See Robert J. Currie & Dr Joseph Rikhof, "Transnational Crimes of International Concern" supra note 72 at 478 and 424 respectively.

285 Robert J. Currie & Dr Joseph Rikhof, "Transnational Crimes of International Concern" supra note 72 at 424.

286 Id.

287 Id.

288 See Vienna Convention at article 4(1).

289 Vienna Convention, article 4(2)(iii). The offences referred to here, as contained in article 3(1), are mentioned above including relevant provisions for our purpose i.e. "the conversion or transfer of property, knowing that such property is derived from any offence or offences established […] or from an act of participation in such offence or offences, for the purpose of concealing or disguising the illicit origin of the property or assisting any person who is involved in the commission of such an offence to evade the legal consequences of his actions."

when an alleged offender is within its jurisdiction.[290] This is a duty to extradite or prosecute any offenders found within their jurisdiction without delay.[291]

In addition, all offences established by the convention are extraditable offences and are deemed to be included in any extradition treaty concluded between parties.[292] The Vienna Convention becomes the treaty basis of an extradition request if the requested state's laws make it the condition of effecting an extradition.[293]

Pursuant to the UNCTOC, parties are required to criminalize all offences recognized therein, as well as to instigate adjudication and sanction provisions with respect to these offences.[294] In accordance with the jurisdictional principles mentioned above, article 15(2) stipulates that a state may exercise jurisdiction where an offence is committed against its nationals or by its nationals or habitual residents.[295] Article 15 grants jurisdiction on similar terms as that contained in the Vienna Convention. The UNCTOC provides that a state is also empowered to exercise jurisdiction over offences (e.g. participation in an organized criminal group or money laundering) that are committed outside its territory which are intended to facilitate the commission of an offence within its territory.[296]

Furthermore, article 16 of the UNCTOC stipulates that for extradition requests, the principle of double criminality is applicable. Double criminality is a condition for executing an extradition request together with provisions on prosecution or extradition. This condition is seen as essential for the prevention loopholes that enable evasion of liability for transnational organized crimes.[297]

---

290 Id at article 4(2).
291 Id at article 4(2)(b).
292 Id at article 6(1) & (2).
293 Id at article 6(3).
294 UNCTOC, *supra* note 34 at article 11. The UNCAC contains similar provisions on this point. See UNCAC at article 42.
295 See also UNCAC, at article 42(2), (5) and 44(1); CFT Convention, article 7(2) and 9.
296 Article 15(2)(c).
297 This provision is also contained in UNCAC, article 44(1) & (2).

In the CFT convention, article 7 provides that states shall take measures to prosecute or extradite alleged offenders within their jurisdiction. This article also adds that when more than one state claims jurisdiction, all relevant states are to work together to coordinate their actions on prosecution and MLA.[298] In addition to the usual provisions on extradition described above, the CFT convention also requires states to ensure the human rights of the alleged offender are protected by specifying measures such as fair treatment in custody and guaranteeing all rights in accordance with human rights and humanitarian law are observed.[299]

The FATF Recommendations on the subject of extradition requires that the condition as to double criminality should be considered fulfilled if both states criminalize the underlying conduct covered in the offence regardless of the formal terminology used in their legislation. For the FATF recommendations, extradition requests concerning money laundering and terrorist financing shall be executed without undue delay and states are also urged to ensure their jurisdictions do not turn into safe havens for alleged offenders.[300] The recommendations suggest that one way of achieving this is to ensure money laundering and terrorist financing offences are extraditable. Additionally, the FATF recommends transparency and timeliness be employed in the process of executing such requests. When it comes to a state's own nationals, the recommendations provide that such states should extradite its nationals or commence prosecution for the relevant offences without delay.[301]

3.2 Conclusion

Although developed initially to combat drug trafficking, the AML framework now extends to "all serious crimes" as predicate offences and applies to illicit activities ranging from trafficking in persons to terrorist financing. This change reflects a recognition by the international community of the evolving nature of transnational crimes that are facilitated by money laundering. It also demonstrates the importance of ensuring that the framing of predicate or postdicate crimes within

298 CFT Convention, at article 7(5).
299 Id at article 17.
300 FATF Recommendations, r39.
301 Id.

the AML framework does not hinder efforts to combat money laundering and other transnational crime.

The initiatives detailed above present key aspects of the patchwork that makes up the current international AML regime. The instruments adopt similar provisions for dealing with the thematic areas identified. They also show the importance of international cooperation amongst financial and AML institutions in tackling transnational crimes. Information sharing and mutual assistance regarding illicit activity has become crucial as such crimes now habitually operate beyond the territorial limits of any given country.

Nevertheless, differences exist amongst the AML instruments. These could be attributed to peculiarities in the predicate/postdicate crimes addressed. While the UNCTOC contains broad provisions on transnational crimes generally, certain considerations are highlighted in the UNCAC and the CFT convention to reflect specific challenges which require emphasis within those conventions. This could account for the comprehensive provisions of the UNCAC on asset recovery. It could also explain the comprehensive definition of assets in terrorist financing where funds could take a variety of formats.

Interestingly, the FATF Recommendations appear to be the only instrument of the group examined which, although voluntary, are widely adhered to by countries. This could be attributed to the fact that the FATF relies on a monitoring mechanism of country inspection and the publication of an annual list of non-compliant countries to garner compliance. [302] Being included in the FATF's non-compliance list reflects poorly on a country's international profile and in some instances, its ability to secure loans in the international financial system.[303] Countries that have been placed on this list in the past often make great effort to ensure their names are taken off the list in order to avoid these consequences.

However, the provisions reveal that with regards to prevention of money laundering, a great deal of emphasis is placed on the responsibilities of financial institutions (e.g. to investigate customer

302 This outcome is most likely the result of the annual publication, by the FATF, of a list of non-compliant countries.
303 See Chris Brummer, "How International Financial Law Works" *supra* note 200.

identities and report suspicious transactions). Furthermore, sanctions may be issued against these institutions by regulatory bodies where such institutions fail to comply with investigatory and reporting obligations. From evaluating the existing international AML regime, I find that there are already provisions in existence that could be useful in combatting money laundering even where cryptocurrencies are used for that purpose. However, while the preventive approach as embodied in the instruments examined above is important for curtailing the laundering of funds in traditional currency (traceability improves once funds are deposited in a banking institution), it remains to be seen these AML provisions would fare in the context of non-traditional financial instruments such as cryptocurrencies.[304] In the next chapter, I will provide an overview of cryptocurrencies, highlighting significant features that could enable them to become attractive for money laundering.

304 In the course of this research, I observed an unsurprising divergence of opinions in the existing literature evaluating the effectiveness of the global AML regime. However, a comprehensive analysis of the effectiveness of the global AML regime is beyond the scope of this work.

Chapter 4: Cryptocurrencies and Transnational Crime

Gray areas […] are dangerous, which may be why Nakamoto constructed Bitcoin in secret. It may also explain why he built the code with the same peer-to-peer technology that facilitates the exchange of pirated movies and music: users connect with each other instead of with a central server. There is no company in control, no office to raid, and nobody to arrest.

– Joshua Davis, The New Yorker)[305]

Cryptocurrencies continue to grow and permeate society. Cryptocurrencies are a type of financial technology (FinTech) and Bitcoin its most popular example. Bitcoin gained recognition as a subcultural phenomenon amongst technology enthusiasts as well as among libertarians and neo-libertarians keen to avoid government involvement in their financial transactions. Its growth is also attributable to the current zeitgeist of technology-assisted social interaction.[306]

Over the past couple of years, awareness of cryptocurrencies has grown in part due to wild fluctuations in its value, high-profile instances of people cashing in on the 'bitcoin bubble', as well as noted instances of investment loss.[307] As awareness (and use) of Bitcoin continues to increase, cryptocurrency enthusiasts often speak of it as a 'disruption' to well-established traditional banking mechanisms.[308] In making this argument, cryptocurrency advocates observe that general

---

305 Joshua Davis, "The crypto-currency", The New Yorker, October 10, 2011, 62.

306 The Internet has spurred the growth of e-commerce and the rise in a variety of online payment and transaction mechanisms in support. Social media (a form of technological advancement) facilitates the sharing of information, interests, as well as creating forums for networking amongst like-minded individuals and groups. When individuals using these mediums wish to engage in financial transactions, natural they rely on technology in the form of financial technology (fintech) to facilitate their business arrangements, complete financial transactions, and conclude contractional agreements.

307 Tugce Ozsoy & Jeremy Herron, "Bitcoin Rebounds to Surpass $16,000 as Five-Day Selloff Ends" Bloomberg (December 26, 2017) online: <https://www.bloomberg.com/news/articles/2017-12-26/is-bitcoin-back-cryptocurrency-passes-15-000-as-rebound-begins>. Anthony Cuthbertson & Andrew Griffin, "Bitcoin Price - Latest Updates: Cryptocurrency Recovers from Eight-Month Low", The Independent (6 July 2018) online: <https://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-price-live-updates-latest-value-exchange-rate-digital-cryptocurrency-futures-investment-a8203081.html>. Aaron Brown, "Bitcoin Billionaires May Have Found a Way to Cash Out" Bloomberg (December 21, 2017) online: <https://www.bloomberg.com/view/articles/2017-12-21/bitcoin-billionaires-may-have-found-a-way-to-cash-out#footnote-1513870741754>.

308 Disruption here refers to the term 'disruptive technologies' proffered by Bower and Christiansen to describe technologies that introduce a new service package with attributes that differ from that historically valued by mainstream customers. They are at first valued mainly in new markets and facilitate the emergence of new markets but eventually make inroads in the mainstream market that reduce the dominance of the big players. See Joseph L. Bower & Clayton M. Christensen, "Disruptive Technologies: Catching the Wave" (1995) 73:1 Harvard Business Review 43

consumer behaviour already reflects a move away from traditional payment mechanisms for online transactions (credit cards) towards alternative payment types (from JCB and UnionPay, to PayPal and Apple Pay). [309] These payment types appeal to the desire of consumers for low cost transactions, security, and user-friendliness.[310]

The use of cryptocurrencies continues to rise. It is used by individuals who desire to keep their (legitimate) financial transactions private. At the same time, there are claims that cryptocurrencies also attract the attention of illicit actors seeking to hide the proceeds of their crimes under a cloak of 'anonymity'.[311] This concern is also raised with regards to the transnational crimes discussed so far in this work.[312] Its attraction for illicit purposes is as a payment or money transfer mechanism. This is because, the regulation of cryptocurrencies remains fragmented (at best), limited, and uncoordinated. Such an environment is fertile ground for laundering proceeds of crime as we will see. Using cryptocurrencies, criminal actors could still achieve the objective of money laundering which were previously conducted through the traditional banking institutions. Such laundering practices are now increasingly hindered by anti-money laundering (AML) controls designed to monitor banking transactions as discussed in the previous chapter.[313]

This chapter presents an overview of cryptocurrencies. Bitcoin will be used as a case study of cryptocurrencies. Bitcoin was identified in chapter 1 as having well developed processes. Bitcoin is also the genus of the recent cryptocurrency phenomenon such that other cryptocurrency

---

309 Aaron W. Baur et al, "Cryptocurrencies as a Disruption? Empirical Findings on User Adoption and Future Potential of Bitcoin and Co" in Marijn Janssen, Matti Mäntymäki, Jan Hidders, Bram Klievink, Winfried Lamersdorf, Bastiaan van Loenen, Anneke Zuider- wijk (eds.), Open and Big Data Management and Innovation: 14th IFIP WG Conference on e-Business, e-Services, and e-Society, I3E 2015, Delft, The Netherlands, October 13-15, 2015, Proceedings (Basel: Springer International Publishing) 63-80 at 63-64.

310 Visa and Mastercard experienced growth rates of 9.5 % and 9.6 %, respectively compared with JCB and UnionPay performance of 20.7 % and 44.8 % respectively in 2013. See Tapomoy Koley, "End of Duopoly in Credit Card Payment Scheme Industry" (2014) 4:1 IOSR Journal of Economics and Finance 67 at 68.

311 The issue of anonymity of cryptocurrency users remains a contentious one and will be discussed further later in this chapter. Criminal networks here develop through exploitation of globalization and other technological developments so far (discussed in chapter 2).

312 *Id.*

313 The extent to which this money laundering through traditional banking institutions has been impeded by AML control remains the subject of much debate. See for instance Margaret Beare, "Responding to Transnational Organized Crime: Follow the Money" *supra* note 13; Marco Arnone & Leonardo Borlini, "International anti-money laundering programs: Empirical assessment and issues in criminal regulation" *supra* note 150. Bruce Zagaris, "Money Laundering and Counterterrorism Financial Enforcement" *supra* note 36 at 67.

protocols are largely modelled on the Bitcoin protocol. In focusing on Bitcoin, this work recognizes that it is the largest, most popular cryptocurrency to date.[314] 'Bitcoin' will be alternately referred to as 'bitcoin' (no capitalization) where the currency rather than the protocol is under discussion. Bitcoin will also be used interchangeably with cryptocurrencies as the research for this work predominantly on Bitcoin given the paucity of information on other forms of cryptocurrencies (generally referred to as 'altcoins').

In this chapter, I also consider the benefits and shortcomings of Bitcoin. Key amongst its drawbacks is its potential use for facilitating money laundering, the issue at the core of this thesis. To consider actual and potential money laundering in the Bitcoin ecosystem, I evaluate empirical research and apply theories from the criminology discipline.[315] Next, I situate the bitcoin money laundering problem in the context of the conventional three-stages of money laundering to understand how this form of laundering could occur. I apply these findings towards understanding why cryptocurrencies (in their present state) could prove even more attractive to criminal actors.

4.1 Overview and Evolution of Cryptocurrencies

A cryptocurrency or virtual currency is a type of digital currency which is not issued or influenced by any central authority such as a nation's central bank.[316] Cryptocurrencies are created using mathematical techniques (cryptography) and are intended to operate as a monetary system independent of any country.[317] They allow their users to conduct financial transactions without the

---

314 This argument is discussed in the methodology section of chapter 1 of this thesis. According to Jessica Meek "Bitcoin regulation challenges and complexities. Operational Risk & Regulation" (2014) risk.net online: <http://www.risk.net/operational-risk-andregulation/feature/2328022/bitcoin-regulation-challenges-and-complexities> "Since 2009, over 75 virtual currencies have been created and are traded globally, representing about $11 billion in state market value, of these, Bitcoin is the leader, representing about $10 billion or 90% of the total market." United Nations Economic Commission for Africa, Draft Report on Blockchain Technology in Africa (2017) at 11 online: <https://www.uneca.org/sites/default/files/images/blockchain_technology_in_africa_draft_report_19-nov-2017-final_edited.pdf> accessed September 5, 2018 estimates that as of September 2017, Bitcoin's market capital stood at 47.3% (an estimated value of 69.871 billion dollars) and it continues to grow.

315 As no primary empirical study was possible within the confines of this thesis, a passive analysis of publicly available empirical research will enrich the work.

316 These terms are used interchangeably especially by AML policy, regulatory, and enforcement organizations. The term 'cryptocurrency' is a fusion of cryptography and currency.

317 Cryptography is "a field of mathematics focusing on encryption, security, and data protection. Cryptography is the basis of cryptocurrencies that allows the creation, management, and security of the networks to operate." See Mark Gates, Blockchain: The Ultimate Guide to Understanding Blockchain, Bitcoin, Cryptocurrencies, Smart Contracts and the Future of Money (2017).

involvement of an intermediary (financial institution or other trusted third party). In contrast, traditional financial transactions often require the involvement of an intermediary to confirm the transaction and to add, to the transaction, the element of trust and certainty.

The Financial Action Task Force's (FATF) definition of "virtual currency" is often relied on by other institutions involved in AML initiatives as their starting point for research in this area:[318]

> a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have a legal tender status […] in any jurisdiction. It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within its community of users of the virtual currency.[319]

The FATF report adds a further qualifier for identifying virtual currencies: they are convertible given their computable equivalent value in fiat (centralised national currency) and can be exchanged for real currency, noting Bitcoin and Liberty Reserve as examples.[320] In maintaining this definition, the FATF aligns with scholarly definitions. It distinguishes virtual currencies from fiat by the fact that the latter is legally designated as the tender of a country.[321]

Each cryptocurrency protocol possesses its own unit of accounting that is similar to the units of accounting used in fiat currency (i.e. Canadian dollar, British Pound, Nigerian Naira). For instance, the unit of accounting for Bitcoin is bitcoin (lowercase) and abbreviated to BTC. However, unlike

---

318 See for instance UNODC, "Basic Manual on the Detection and Investigation of the Laundering of Crime Proceeds Using Virtual Currencies," online, *UNODC:* https://www.imolin.org/pdf/imolin/FULL10-UNODCVirtualCurrencies_final.pdf >; The Commonwealth, Commonwealth Working Group on Virtual Currencies, *supra* note 3 at 5.

P14195

319 FATF, FATF Report: Virtual Currencies, *supra* note 40 at 4. The FATF definition of cryptocurrencies refers to them as virtual currencies but its meaning suggests that this reference is to cryptocurrencies as they are popularly known. By this definition no government can claim ownership of cryptocurrencies which is the intent of the original developers of Bitcoin and is a challenge for regulatory measures in this area. will likely impede regulation in this area.

320 *Id* at 6.

321 Id. See also, David Descôteaux, "How should Bitcoin be regulated?" (2014) Montreal Economic Institute (Regulation Series: Economic Note) online: <http://www.iedm.org/files/note0114_en.pdf>.; Christian Brenig, Christian, Rafael Accorsi, Rafael & Günter Müller, "Economic Analysis of Cryptocurrency Backed Money Laundering" (2015) 20 ECIS Completed Research Papers, online: < https://aisel.aisnet.org/ecis2015_cr/20/>. Scholars also include the following descriptive qualities: its descriptive qualities: non-fiat, Internet-based, decentralized (not issued by a central authority), and operating according to a trust system.

fiat currency, BTC operates in a particularly volatile market with a wildly fluctuating value. Some experts claim that this market volatility stems from non-regulation by any financial institution and a value entrenched in the demand and supply behaviour of its peer-to-peer users.[322] Additionally, there is also no central bank authority for cryptocurrency.

Although some literature uses the terms 'virtual currencies' and 'cryptocurrencies' interchangeably, the FATF report noted above suggests that virtual currencies as a category include but are not limited to cryptocurrencies. Interestingly, the lack of a conclusive and singular definition of cryptocurrencies may also be a contributor to its presently unregulated state. The absence of a consensus on how to categorize or define cryptocurrencies, whether as currency, commodity, asset, or even financial technology could signify that uniform regulation of cryptocurrencies remains unfeasible at present.[323]

For the purpose of this work, the term cryptocurrency rather than virtual currencies will be used. My position aligns with the FATF explanation above that although cryptocurrencies are virtual currencies, all virtual currencies are not necessarily cryptocurrencies.

4.2 Bitcoin's Development

The evolution of Bitcoin can be traced back to 1998 when the concept of a cryptographic-based currency was described by Wei Dai (a computer science engineer) on the 'cypherpunks' mailing list. Dai described a new form of money that will use cryptography to control its creation and transactions rather than a central authority.[324] Inspired by Dai's idea, a person or group of persons known as Satoshi Nakamoto authored a whitepaper introducing Bitcoin. The paper described

---

322 Id, François R. Velde "Bitcoin: A primer." See also Nicholas Plassaras, "Regulating digital currencies: Bringing Bitcoin within the reach of the IMF" (2013) 14:1 *Chicago Journal of International Law* 377 at 382.

323 Classifying cryptocurrencies one way or the other could prove to be an important aspect of developing the legislative framework that is essential to contend with the challenges presented by cryptocurrencies. In chapter 5 of this thesis, I attempt such categorization.

324 The cypherpunks mailing list is described as a "forum with technical discussion ranging over mathematics, cryptography, computer science, political and philosophical discussion, personal arguments and attacks, etc., with some spam thrown in." Cypherpunks are considered activists who advocate the widespread use of strong cryptography and privacy-enhancing technology as a route to social and political change. See Arvind Narayanan, "What Happened to the Crypto Dream? Part 1" (2013) 11:2 IEEE Security & Privacy, 75.

Bitcoin as the world's first feasible decentralized currency and the alternative to traditional electronic payment channels.[325] For Nakamoto, Bitcoin is the solution to e-commerce's reliance on centralized intermediaries (financial institutions) to serve as trusted third parties to online transactions.[326] Nakamoto argues that the existing model of a centralized intermediary creates inefficiencies for the digital transfer of wealth, such as the risk of double-spending.[327] Nakamoto suggests that such risks could be precluded by an alternative system built on cryptographic proof rather than trust. Using this alternative system, parties would now be able to transact directly without relying on an intermediary to confirm the transaction.[328]

In 2009, Bitcoin went from a white paper to actualization as an open source software designed for peer-to-peer transactions.[329] Instead of banks, Bitcoin relies on cryptographic algorithms and peer-to-peer technology to facilitate its users' financial transactions both securely and pseudonymously.[330] In designing Bitcoin, Nakamoto's ideal is that the cryptocurrency should be user-friendly and allow anyone anywhere in the world to participate so long as they have access to the Internet.[331] Its format therefore affords those who do not have access to traditional banking facilities (or choose not to use them) an alternative means of conducting their financial transactions.[332]

As a means of payment, awareness of cryptocurrencies amongst merchants continues to increase.[333] Researchers credit its increasing popularity to the fact that transaction charges

---

325 Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2012) Bitcoin.org online: <https://bitcoin.org/bitcoin.pdf>. I use the term 'person or group of persons' because no one is able to identify with certainty who Nakamoto is and attempts to do so have been discredited.

326 Id.

327 Id. Double spending is a problem of digital currencies that arises when the same money is spent twice. It is a potential flaw for any digital money mechanism given that the money (or token) consists of a digital file that could be duplicated or falsified as with counterfeit money. See Usman W. Chohan, 'The Double-Spending Problem and Cryptocurrencies' (2017) University of NSW Discussion Papers Series <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3090174> accessed 21 February 2018. See also Samuel Elliott, "Bitcoin: The First Self-Regulating Currency?" (2018) 3, LSE Law Review 57.

328 Id.

329 Pierluigi Cuccuru, "Beyond bitcoin: an early overview on smart contracts" (2017) 25 International Journal of Law and Information Technology 179 at 181.

330 Satoshi Nakamoto, "Bitcoin," *supra* note 325. See also Primavera De Filippi, "Bitcoin: A Regulatory Nightmare to a Libertarian Dream" *supra* note 50 at 2.

331 Satoshi Nakamoto, "Bitcoin," *supra* note 325.

332 This feature is considered one of the benefits of cryptocurrencies and explored further below.

333 While numbers in this regard vary, Chainalysis, a software company that blockchain and cryptocurrencies, notes that at the beginning of 2015, the amount of bitcoin received by top merchant processors was estimated around $11 million. Fast-track

administered by Bitcoin are reportedly between 0-2 percent.[334] This is in contrast to the 2-3% or more per transaction charge by financial intermediaries such as Visa and MasterCard.[335]

The value of Bitcoin also continues to fluctuate, at times wildly. As of January 1, 2013, a purchase of 1 BTC would yield an estimated $13 and by the end of that year, 1 BTC was worth an astonishing $1242 (an appreciation of nearly 1000%) resulting I industry and mainstream recognition of the phenomenon.[336] Again in 2015, the 1 BTC had slumped to $250 at the start of the year. The value of bitcoin continued to fluctuate and in 2017 rose drastically to $20,000.[337] After a price crash at the end of 2017, by July 2018 Forbes Magazine once again reported that 1 BTC was above $8,000 and was estimated to control about 47% of the cryptocurrency market.[338] This rise is attributed to the anticipated approval of a bitcoin exchange traded fund as well as interest from recognized giants of the finance industry.[339]

4.3 How Bitcoin Works

Bitcoins are generated in the first instance through a process known as "mining" whereby users contribute computing power to the resolution of a complicated mathematical equation (the 'proof of work').[340] The design of Bitcoin is such that the number of bitcoins that can be generated is

---

to September 2017, this figure had risen to $411 million. However, the volatility of bitcoin's value also reflects in its acceptance amongst merchants and by May 2018, this figure had dipped to $69 million, according to the Chainalysis research conducted for Bloomberg News. See Olga Kharif, "Bitcoin's Use in Commerce Keeps Falling Even as Volatility Eases" August 1, 2018, Bloomberg, online: < https://www.bloomberg.com/news/articles/2018-08-01/bitcoin-s-use-in-commerce-keeps-falling-even-as-volatility-eases?srnd=cryptocurriences>.

334 Lam Pak Nian & David Lee Kuo Chen, "Introduction to Bitcoin" *supra* note 49.

335 Id.

336 Lam Pak Nian & David Lee Kuo Chen, "Introduction to Bitcoin" *supra* note 49.

337 Billy Bambrough, "Binance CEO Predicts A Bitcoin and Crypto 'Bull Run'" *supra* note 67.

338 Id.

339 Id. See also Securities and Exchange Commission, "Self-Regulatory Organizations; Cboe BZX Exchange, Inc.; Notice of Filing of Proposed Rule Change to List and Trade Shares of SolidX Bitcoin Shares Issued by the VanEck SolidX Bitcoin Trust" June 26, 2018, online: < https://www.sec.gov/rules/sro/cboebzx/2018/34-83520.pdf>.The United States Securities and Exchange Commission (SEC) is considering whether to approve exchange traded fund filed by New York-based Van Eck and the blockchain platform SolidX. If the application is approved, people would be able to buy into the bitcoin market without the currently cumbersome exchange process and the issues associated with an unregulated market.

340 Id. Satoshi Nakamoto, "Bitcoin," *supra* note 325. Miners contribute computing power such as electricity to the blockchain network which uses it to confirm transactions. The miners are rewarded for verifying a block with transaction fees and block rewards. The reward for solving a block is automatically adjusted so that, ideally, every four years of operation of the bitcoin network, half the number of bitcoins created in the prior 4 years are created. Thus, the total number of bitcoins in existence can never exceed 21,000,000. See Primavera De Filippi, "Bitcoin: A Regulatory Nightmare to a Libertarian Dream" supra note 50 at 2. Satoshi Nakamoto notes in his work that "the steady addition of a constant amount of new coins is analogous

finite, with the cap set at 21 million bitcoins.[341] The design of the mining process ensures the security and integrity of the bitcoin system by providing a means to verify transactions. Verification is achieved through the decentralized network of peers who simultaneously process transaction data (sometimes for a fee) and are subsequently recorded on the blockchain ledger (the public ledger for all transactions on the Bitcoin network).[342] Through this process, new bitcoins are created.

In order to use the bitcoins to pay for goods and services, users install a Bitcoin wallet on their mobile or computer devices which generates a public and private encryption key used for verifying transactions.[343] The Bitcoin protocol assigns value to Bitcoin addresses (public keys) and the assigned value is denominated in BTC (the bitcoin currency). The public keys serve as account numbers for users.[344] The 'accounts' can only be controlled by persons who hold corresponding private keys to the accounts.[345] Anyone can generate a fresh pair of bitcoin keys: the public key where value is assigned and which is used to receive BTC payments, and the private key for effecting transactions with the bitcoins contained in each address such e.g. payments to other bitcoin users. The operation of Bitcoin accounts in this way may be likened to numbered bank accounts commonly associated with banking secrecy in a number of countries including Switzerland, Luxembourg, Monaco, and the Cayman Islands. Accordingly, bank clients are only identified using multi-digit numbers, only known to the client and select bankers. [346]

---

to gold miners expending resources to add gold to circulation." Satoshi Nakamoto, "Bitcoin," *supra* note 325 at 4. See also Ole Bjerg, "How is Bitcoin Money?" (2015) 33:1 Theory, Culture & Society 53 at 56.

341 Judith Lee et al, "Bitcoin Basics: A Primer on Virtual Currencies" (2015) 16:1 Business Law International 2 at 24. There are currently over 17 million bitcoins in circulation (approximately 80% of the entire bitcoins that can be mined). See Blockchain, online: <https://www.blockchain.com/en/charts/total-bitcoins>. The cap on the number of bitcoins that can be mined is intentional to give it value and combat inflation or deflation unlike fiat currency whose value is backed by law and underwritten by the state. This ties in with Nakamoto's desire to create a solution to the effects of the economic downturn. Given its finite nature, the idea is that their rarity and value will increase especially when mining is no longer possible. See Nicholas A. Plassaras, "Regulating Digital Currencies" supra note 322 at 383.

342 Arvind Narayanan et al, *Bitcoin and Cryptocurrency Technologies: a comprehensive introduction* (Princeton: Princeton University Press, 2016) at *xx*.

343 Id.

344 Id.

345 Id.

346 Id. Numbered accounts are a practice outlawed by some state governments arguing that they are associated with minimization of government scrutiny (the Libertarian ideal) or tax avoidance. Public-key cryptography is often seen as the FinTech equivalent of banking secrecy given that it enables anonymous Internet banking. See Sebastien Guex, "The Origins of the Swiss Banking Secrecy Law and its Repercussions for Swiss Federal Policy" (2000) 74:2 The Business History Review, 237.

Alternatively, bitcoins can be obtained by transfer from one user to another using a bitcoin wallet and the encryption keys. The way this works is that a bitcoin owner sends his public key to the receiver in a manner similar to sending a file. The difference here is that once the transfer is made, it is irrevocable and the sender loses his access to the bitcoins.[347] This is set up to prevent double-spending whereby the sender transfers the same bitcoins to multiple users.[348]

Bitcoin operates a decentralized system, which means that the users in the bitcoin community, rather than a centralized authority, are required to verify each transaction as legitimate. Upon doing so, a new block is published on the publicly accessible blockchain.[349] The blockchain is an online ledger where records of all transactions in the system are recorded.[350] While the entries on the ledger (blockchain) are available for all to see, what is actually recorded on the ledger is how much is sent or received. The record does not reveal any information about the transacting parties, which is the key reason for anonymity claims concerning the use of Bitcoin. However, in this system it is possible (although requiring strenuous effort and a great deal of technical expertise) to trace the ownership of bitcoin(s). This is so, given that where its ownership has been reassigned, each transaction includes a reference to all connected previous transaction.[351] The decentralized process of the Bitcoin network has not raised concerns about illicit transactions so far.[352] However, applying KYC (know your customer) regulations to the Bitcoin network would prove challenging. This is because a decentralized system would mean that no individual within the Bitcoin network (unlike with traditional centralized banks) could be identified or held accountable for monitoring transactions and identifying illicit activities if and when they occur.

---

347 That is unless the receiver decides to send it back to him (now as a sender).

348 Judith Lee, et al, "Bitcoin Basics" *supra* note 341 at 24.

349 Ole Bjerg, "How is Bitcoin Money?" *supra* note 340 at 56. Bitcoin exchanges and merchants that accept bitcoin sometimes specify how many confirmations on the blockchain is required before funds are considered verified. The reason for this is that the merchants will often bear the risk of double spending.

350 Malte Möser, and Rainer Böhme, "The price of anonymity: empirical evidence from a market for Bitcoin anonymization" (2017) 3:2 Journal of Cybersecurity, 127 at 128.

351 Id. This operation is a reason put forward to contradict the anonymity claims. The issue of anonymity is discussed in more detail later in this chapter.

352 Isaac Pflaum & Emmeline Hateley, "A bit of a problem", *supra* note 251 at 1169. Perri Reynolds and Angela S.M. Irwin "Tracking Digital Footprints" *supra* note 52.

Instead, AML regulators and existing literature have focused on the most common method for buying or selling bitcoins. This method involves exchanging them for fiat currency through bitcoin exchange operators (centralized bodies). Bitcoin exchanges are predominantly Internet-based and can be domiciled anywhere in the world. They are unregulated and thus able to operate without complying with customer due diligence requirements typically applied to financial institutions. However, some bitcoin exchanges voluntarily comply with AML and terrorism legislation as a mean of asserting their legitimacy as financial mechanisms.[353] These exchanges may charge a fee for the transaction (usually lower than bank charges). Once bitcoins are purchased through a bitcoin exchange operator, the user can store their assets within the exchange itself or in digital wallets for future use in financial transactions.

Just like in traditional exchange markets, the price of bitcoin floats against other currencies, with its value based on supply and demand.[354] Other online marketplaces such as Coinbase and Bitsquare also provide a platform for connecting bitcoin buyers and sellers privately either online or in person.[355]

Bitcoin and other cryptocurrencies are now accepted as payment for goods and services directly from merchants (bricks and mortar as well as online merchants).[356] These include both licit and illicit vendors offering the sale of goods ranging from flowers, groceries, computers, jewellery, to items like gun parts and hacker handbooks.[357] Worrisome is the acceptance of bitcoin as payment for child pornography and illicit drugs, and by charitable organizations known known to be a front

353 See for instance, the Slovenia-based bitcoin exchange, Bitstamp. Bitstamp, "Bitstamp Limited Anti Money Laundering ("AML") and Counter Terrorist Financing ("CTF") Policy" online: < https://www.bitstamp.net/aml-policy/>.

354 Nicholas A. Plassaras, "Regulating Digital Currencies" supra note 322 at 386.

355 See CoinTelegraph Guide, "How to Sell Bitcoin" online: <https://cointelegraph.com/bitcoin-for-beginners/how-do-i-sell-bitcoins#exchanges>.

356 Overstock.com in 2014, became the first US online retailer to accept bitcoin and later in the same year, started accepting payments in all foreign currencies. Later the same year, retailers including Dish Network, Expedia and Dell also started accepting bitcoin as payment for their services. Bitcoin can now also be used to make purchases from Amazon, CVS, Target, Zappos, Home Depot and Whole Foods, using the retailers' gift cards that can be purchased from eGifter or Gyft who accept bitcoin payments. See Judith Lee, et al, *supra* note 341 at 25.

357 Judith Lee, et al, supra note 341 at 25.

for terrorist financing (these constituting some of the transnational crimes under evaluation in this thesis).

4.4 Benefits of Cryptocurrencies

As mentioned above, cryptocurrencies continue to experience mainstream recognition. However, their use is still limited when compared to traditional currencies even if we restrict the comparator pool to digital payment mechanisms that rely on traditional banking systems to operate.[358] Given its relatively limited use, I will refer to the potential or anticipated benefits of bitcoin in the event that it continues to gain acceptance as a legitimate financial mechanism.[359]

One benefit of cryptocurrencies is that it provides a forum for financial transactions to those who do not have access to traditional banking facilities (the 'unbanked').[360] The World Bank's Global Financial Development Report on Financial Inclusion indicates that about half of the world's adult population (about 2.5 billion) do not have an account at a formal banking institution.[361] The report acknowledges that some individuals included in this figure are those who do not have any need or want for such an account. However, the World Bank Report also it observes that the majority lack such access due to certain barriers. Some of the barriers include the cost of maintaining an account, the distance from their domicile to the nearest banking facility, and the ownership of paperwork required in opening a bank account.[362] Mobile phone compatibility with cryptocurrencies increases enfranchisement within that demographic (the unbanked). [363] For instance, the M-Pesa in Kenya (a mobile banking service which is based on centralized fiat currency) addresses this lack of access to banking facilities by capitalizing on widespread individual access to mobile phone facilities.[364] Their approach hints at the potential for cryptocurrencies to achieve similar results as individuals

---

358 Aaron W. Baur, et al, "Cryptocurrencies as a Disruption? *supra* note 309.

359 The Commonwealth, Commonwealth Working Group on Virtual Currencies, *supra* note 3 at 23.

360 My use of the term 'unbanked' is inspired by a 2017 World Bank Report authored by Asli Demirgüç-Kunt, Leora Klapper, Dorothe Singer, Saniya Ansar & Jake Hess, The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution (Washington DC: World Bank, 2017) at p.25 identifying the unbanked as individuals "without an account at a financial institution or through a mobile money provider."

361 World Bank, Global Financial Development Report 2014, *supra* note 4 at 1.

362 Id.

363 The Commonwealth, Commonwealth Working Group on Virtual Currencies, *supra* note 3 at 23.

364 *Id.*

which is accessible using Internet-enabled mobile phones and is not tethered to traditional banking institutions.

Another benefit of cryptocurrencies in comparison to other, more traditional, methods of payment or money transfer is the reduced costs associated with financial transactions. According to the European Central Bank, the cost of a BTC transaction is approximately 1% of the value of the transaction compared with about 8-9% charged as fees for fiat money transfers.[365] Furthermore, unlike other remitters, cryptocurrency transfers are not scaled by size of transaction (large funds attract higher charges) or destination of the funds.[366] With remitters such as Western Union Money Transfer or Money Gram, the cost of sending funds from the diaspora to individuals and communities in developing countries is significant. In 2014 for instance, the use of money remitters to the Caribbean and Africa from developed countries exceeded any other form of external finance meaning that a lot of funds are spent effecting those transactions.[367]

Based on World Bank estimates of global money remittances, the use by consumers of cryptocurrencies could potentially result in an annual net savings of over $43 billion USD over traditional remittance operations.[368] In this way, Bitcoin has the potential to develop into a legitimate alternative financial institution. Bitcoin could achieve this by providing a lower cost alternative means of financial transactions and facilitating a more equitable distribution of wealth.

Cryptocurrencies could also be beneficial in the context of charitable operations. The usual costs associated with raising and transferring donation funds will likely be reduced through the use of cryptocurrencies.[369] Calls for funds in aid of charitable causes as well as to support persecuted individuals (political dissidents, journalists) are becoming more widespread. In December 2017, Julian Assange, founder of Wikileaks, urged his supporters to donate to the Wikileaks publication

---

365 European Banking Authority, "EBA Opinion on 'Virtual Currencies'" (European Banking Authority: London, 2014) at para 46 online: < https://www.eba.europa.eu/documents/10180/657547/EBA-Op-201408+Opinion+on+Virtual+Currencies.pdf> (last accessed 9 September 2018).

366 Nicholas Godlove, "Regulatory Overview of Virtual Currency", *supra* note 3 at 13.

367 Id. India received the highest amount of money remittance globally (about $21 billion USD) in 2014.

368 World Bank, Global Financial Development Reports, *supr*a note 4 at 1. Roman Leal, "Is Bitcoin the Future of Payments?" (2014) 21 *Goldman Sachs Global Investment Research Paper* 18.

369 Id.

using cryptocurrencies such as Bitcoin, ZCash, Monero, and Litecoin. He did so in order to circumvent the financial 'Blockade" imposed against the Wikileaks by national governments.[370] This incident highlights the usefulness of cryptocurrencies such as bitcoin where the free speech of civil rights activists or anti-government sentiments are stifled.[371]

4.5 Drawbacks to Cryptocurrencies

A constant source of concern with cryptocurrencies is volatility with respect to their value. In particular, this is a recurring challenge for Bitcoin. In the space of a two-year period spanning 2011 to 2013, for instance, the value of BTC fluctuated between $0.30 USD to $1,135 USD.[372] David Descoteaux observes that volatility will likely be reduced if Bitcoin is increasingly accepted as a medium of exchange, as this would decrease the ability of a small number of actors to influence its price.[373] However, the goal of achieving mainstream acceptance, remains compounded by a residual hesitancy by merchants. The concern in this regard has to do with potential devaluation of the BTC leading to devaluation of their business assets.[374] Such hesitation, in turn, impedes the potential 'mainstreaming' and increase in cryptocurrency use – compounding the problem.

Another drawback to cryptocurrencies is that, at present, risks relating to incorrect or disputed transactions are borne mostly by the consumers. Consumer protection legislation does not

---

370 John Buck, "Julian Assange Urges Donors to Use Cryptocurrencies, Thwart Government" Coin Telegraph (December 20, 2017) online: <https://cointelegraph.com/news/julian-assange-urges-donors-to-use-cryptocurrencies-thwart-government>. Assange often tweets his support for governments that use Bitcoin or other cryptocurrencies to bypass crippling 'western' financial sanctions. In the same vein, donations to illicit activities are also becoming the norm with terrorist financing groups garnering funds under the guise of charitable causes. Wikileaks leveraged the perception of anonymity when it asked for 'anonymous' donations and received over 1,000 Bitcoin donations (over $32,000 in value at the time). Jon Matonis observes that this move by WikiLeaks and support by donors signalled that publishers and journalists acting would not be silenced by governments. Donations to WikiLeaks were blocked by credit card organizations such as Mastercard and Visa, as well as PayPal following pressure from the US government. See Jon Matonis, "WikiLeaks bypasses financial blockade with bitcoin." http://www.forbes.com/sites/jonmatonis/2012/08/20/wikileaks-bypasses-financial-blockade-with-bitcoin/> Forbes. Accessed 20 Aug 2018. The writer observes that

371 In the same vein, donations to illicit activities are also becoming the norm with terrorist financing groups garnering funds under the guise of charitable causes.

372 United Nations Office on Drugs and Crime (UNODC), "Basic Manual on the Detection," *supra* note 318 at 8. The figure from 2011 may be attributed to the fact that this was really in the early stages of Bitcoin operations rather than evidence of its volatility.

373 David Descoteaux, "Bitcoin: More Than a Currency: a Potential for Innovation" Montreal Economic Institute (Regulation Series: Economic Note, January 2014) online: <http://www.iedm.org/sites/default/files/pub_files/note0114_en.pdf> at 3.

374 Id.

expressly provide a recourse for consumers where problematic transactions arise.[375] For instance, Bitcoin transactions are irreversible, save for the receiver initiating a subsequent transaction to 'return' the funds to the original sender. As a result, where problems arise in a transaction, or a user loses access to their private keys or inadvertently reveals private keys, the assets may be permanently lost.[376]

Another drawback to cryptocurrencies concerns its notoriety for illicit use (no doubt heightened by such incidents as Silk Road discussed below). There are persisting concerns that cryptocurrencies facilitate both cybercrimes and cyber-enabled crimes.[377] This concern is attributed to the ease with which transactions can take place pseudo-anonymously on the Internet, a feature considered attractive for money laundering activities and its affiliated crimes.[378] As Internet availability continues to spread, particularly darknet services, it could also inadvertently facilitate the ease of conducting illicit transactions.[379] Research from the European Union Agency for Law Enforcement Cooperation (Europol) in 2014 estimates that 2.8 billion people together with 10 billion devices across the globe are Internet-enabled.[380] This increasing access to mobile phone and internet technology could both creates new opportunities for crime as well as amplify existing opportunities. Furthermore, research by McAfee finds that cyber-enabled crime costs the

375 This is much the same as the problem I contend with in this thesis where the AML regime does not contain express provisions on cryptocurrency facilitated transactional crimes.

376 The Commonwealth, Commonwealth Working Group on Virtual Currencies, supra note 3 at 24. The Commonwealth Working Group found one Bitcoin wallet provider, Elliptic Vault which is based in London, that offers insurance for deposits held with them and this constitutes part of their marketing strategy. A rise in this practice would likely illicit more consumer trust in the Bitcoin system.

377 To differentiate, reference to cyber-enabled crimes consists in traditional crimes (theft or sexual violence for instance) that are able to proliferate using technology like computers and Internet facilities. These crimes are not dependent on informational communication technology (ICT) but the use of ICT increases opportunities for its perpetration. With cybercrimes (or cyber-dependent crimes), on the other hand, the crime itself takes place on the Internet or technology itself is the weapon or target of the attack e.g. use of Malware or data-theft. Cyber-enabled crimes best describe the form of criminal activity I contend with in this thesis. See Mike McGuire & Samantha Dowling, Cybercrime: A review of the evidence Research Report 7 (2013) (UK: Home Office, 2013).

378 Europol observes that the abuse of anonymization techniques is one of the key facilitators of cybercrimes Europol, The Internet Organised Crime Threat Assessment (iOCTA) (Hague: European Police Office, 2014) at 12.

379 The darknet is a term used to describe portions of the internet that are not publicly accessible and where illicit activity takes place using anonymization tools such as 'The Onion Router' (discussed further later in this chapter). See Laurent Gayard, *Darknet: Geopolitics and Uses* (Hoboken: John Wiley & Sons, 2018) at 158.

380 Id.

global economy an estimated $400 billion USD.[381] As mentioned in chapter 2, globalization together with advances in technology creates opportunities for loose criminal networks to develop with members in different parts of the world.[382] Such criminal networks often converge to fulfil a specific criminal objective, in contrast with organized crime groups, and disband just as quickly, obscuring any link amongst them as a result.[383]

Left unchecked, cryptocurrencies could be used to increase the opportunities for such criminal methods. Cryptocurrencies such as bitcoin could facilitate sharing of proceeds of payment for to illicit actors if he risks of detection by law enforcement remain minimal. Isaac Pflaum and Emma Hateley note that if cryptocurrencies remain unregulated, it could expose users to "risks that regulatory regimes are intended to mitigate, and impede efforts of authorities and banks that are tasked with combatting fraud, money laundering, and tax evasion."[384]

4.6 Evidence of Cryptocurrency Use in Transnational Crimes

4.6.1 Drug Trafficking

Drug trafficking is predominant amongst the illicit activities facilitated by bitcoin. For instance, the online marketplace Silk Road is known for the anonymous sale of illicit drugs and the provision of other illicit services.[385] Silk Road operated on the darknet and transactions therein were conducted anonymously, using bitcoin for payments and other obfuscation techniques such as TOR which disguised user locations. In doing so, its founder, Ross Ulbricht, accumulated millions in commission while avoiding law enforcement scrutiny for a period of time.[386] The available data

---

381 Centre for Strategic and International Studies, Net Losses: Estimating the Global Cost of Cybercrime: Economic Impact of Cybercrime II (Washington, DC, 2014) online: <http://www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf> at 2.

382 Sarah Meiklejohn et al, "A fistful of Bitcoins: characterizing payments among men with no names" (2013), IMC, online: https://cseweb.ucsd.edu/_smeiklejohn/files/imc13.pdf (accessed August 23 2018).

383 This phenomenon is referred to as 'crime-as-a-service' where criminals advertise and sell their services to other criminals on an individual task basis and receive their fees using cryptocurrencies to obfuscate any law enforcement efforts at tracing. See Europol observes that the abuse of anonymization techniques is one of the key facilitators of cybercrimes Europol, The Internet Organised Crime Threat Assessment (iOCTA) supra note 378 at 12.

384 Isaac Pflaum & Emmeline Hateley, "A bit of a problem", *supra* note 250 at 1194.

385 United States v Ross William Ulbricht, *supra* note 26. See also id.

386 The darknet is considered a sort of underworld of the Internet and consists of non-indexed domains which cannot be found using regular search engines like Google. To access the darknet, TOR (the Onion Router) is used in enhancing privacy as it routes the user's Internet traffic though a global network of computers volunteering to conceal the user's location and Internet

demonstrates that during the period of Silk Road's operations between February 2011 and July 2013, the site generated a total revenue of 9,519,664 bitcoins with commissions amounting to 614,305 for Silk Road. These figures translate to $1.2 billion in revenue and $79.8 million in commission. During the existence of its operations, it is estimated that almost half of all bitcoin transactions were conducted on Silk Road. The marketplace was shut down by the US Federal Bureau of Investigation in 2013. An estimated 174,000 Bitcoins (valued at $33 million at the time) were subject to seizure and confiscation, and nearly 13,000 drug listings were taken down. Silk Road founder Ross Ulbricht was convicted of charges including narcotics trafficking and money laundering.[387]

In another cryptocurrency-based marketplace, Evolution, drugs were also found to account for about 63% of all illicit listings on the marketplace with bitcoin constituting its main form of payment.[388] Marie-Helen Maras observes that the intent in using cryptocurrencies such as bitcoin in online marketplaces such as Silk Road and Evolution is to obfuscate the identification and location of users.[389] Maras also notes a problem of displacement in darknet marketplaces. As with Silk Road, when law enforcement cracked down on their operations, others were set up by the same operators that managed Silk Road with Ulbricht.[390]

With the Silk Road operations, it is observed that while it may prove difficult to trace the users of such services,[391] it is not impossible to do so. However, the approach taken by national governments so far is to target the operators of such websites and their financial gains (most of the commissions received by Ulbricht were confiscated as proceeds of drug trafficking).[392] However,

---

footprint. See Marie-Helen Maras, "Inside Darknet: the takedown of Silk Road" (2014) 98 *Centre for Crime and Justice Studies* 22.

387 A similar online marketplace is Liberty Reserve operated by Arthur Budovsky which was also shut down by the FBI. The United States Attorney's Office Southern District of New York Press Release, "Liberty Reserve Founder Arthur Budovsky Sentenced in Manhattan Federal Court To 20 Years for Laundering Hundreds of Millions of Dollars Through His Global Digital Currency Business" (9 May 2016), *The U.S. Attorney's Office Southern District of New York*, online: <https://www.justice.gov/usao-sdny/pr/liberty-reserve-founder-arthur-budovsky-sentenced-manhattan-federal-court-20-years>.

388 Judith Lee, et al*, supra* note 340 at 90.

389 Marie-Helen Maras, "Inside Darknet: the takedown of Silk Road" supra note 386.

390 Id. see also Judith Lee, et al, *supra* note 341 at 25.

391 Silk Road operations utilize TOR as well as other obfuscating mechanisms to make it nearly impossible to locate any users of the marketplace users. See Marie-Helen Maras, "Inside Darknet: the takedown of Silk Road" supra note 386.

392 United States v Ross William Ulbricht, Superseding Indictment, *supra* note 26.

similar to what Maras notes above, with this approach, the main perpetrators (the drug traffickers) may simply move on to the next black market to conduct their transactions.

4.6.2 Terrorist Financing

In the 2015 FATF report on the risks and threats of terrorism financing, a special section is included for virtual currencies which highlights the various ways they are implicated in terrorist activities.[393] In the report, the FATF observes that although the original purchase of virtual currency such as bitcoin may be visible (for instance if it is purchased through the banking system), the subsequent transfers of the currencies may be difficult to detect.[394] This is because the operations involved in transferring bitcoin involve greater anonymity than traditional banking, enabling illicit proceeds to be moved quickly from one country to another.[395]

To highlight how this may occur, an example is given in the case of Ali Shukri Amin who was sentenced to 11 years in prison in 2015, followed by a lifetime supervised release.[396] Amin admitted to using Twitter to propagate the ideology of ISIL. He also used his Twitter account to give his followers instructions on how to use bitcoin to obscure the link between themselves and the facilitation of ISIL terror.[397]

The FATF notes that traditionally, cash has been the preferred medium of support for terrorists for the same reason that it is preferred for money laundering. It is probably for this reason that scholars have also noted that the use of cash-based Hawala has in the past been predominant for facilitating terrorist-financing.[398] However, terrorist financers are increasingly appreciating the risks involved in moving cash even when the Hawala system. This is because law enforcement agencies

---

393 FATF (2015). FATF Report. Emerging Terrorist Financing Risks, online: <http://www.fatfgafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf

394 Id at 35.

395 Id.

396 Id.

397 Id at 36. In addition to these activities, Amin also wrote and tweeted a link to his article on how bitcoin could be utilized by Jihadists to fund their efforts while remaining relatively anonymous.

398 Angela S.M. Irwin & George Milad "The use of crypto-currencies in funding violent jihad"(2016) 19:4 Journal of Money Laundering Control, 407 at 408. Hawala (meaning transfer) is an informal low-tech funds transfer system used by millions of individuals in diaspora to send money to their families in their home countries.

increasingly recognize the techniques used for terrorist-financing using the Hawala system. [399] With increasing Internet accessibility, cryptocurrencies could become even more attractive to those intending to finance terrorist activities as it could enable them avoid tracing and other ramifications from their country of domicile.[400]

4.7 Anonymity in the Bitcoin Ecosystem

The concern over anonymity in the Bitcoin ecosystem is one that scholars are constantly seeking to understand. Empirical research on this issue suggests that complete anonymity within the bitcoin ecosystem is a fallacy. Given that it may be possible to apply heuristics towards deanonymization of a user's details, what exists instead is a form of 'pseudo-anonymity'.[401]

As mentioned above, the claims of anonymity stem from the operations of bitcoin which do not require a user to disclose their personal information. In the Bitcoin network, users may create multiple public keys which are not linked to each other, strengthening the perception of anonymity in conducting transactions.[402] On the blockchain, records of transactions do not disclose any personal details of those engaging in the transactions beyond their public keys and transaction amount. However, it may be possible to monitor the transaction chain in bitcoin and identify which e-wallet is sending or receiving bitcoins. Despite this, Reynolds and Irwin observe that users may still feel anonymous while using bitcoin given that the due diligence requirements are insufficient when it comes to bitcoin transactions.[403] This is likened to the situation before the arrival of KYC and CDD measures, where a single individual could open multiple bank accounts with different personal information, but which are all controlled by the same person. The aim of doing so remains

399 It can become time consuming and slow down the terrorist planning operations where speed is required. Hawala is low-tech and involves the movement of cash on trust using many middlemen. It is a funds exchange system evolving from Indian and Chinese civilizations for transferring funds across borders. Hawala is reported to be vulnerable to money laundering and terrorist financing because the actual funds do not cross borders (a Hawala broker arranges for funds given to him by a sender to be made available to the receiver for a small fee), thereby negating any money trail. Records are also not kept stringently in order to maintain the confidence of the sender and receiver. See Angela S.M. Irwin & George Milad "The use of crypto-currencies in funding violent jihad," *supra* note 398.

400 Id.

401 Studies on anonymity in the Bitcoin ecosystem support this claim e.g. Perri Reynolds and Angela S.M. Irwin "Tracking Digital Footprints" *supra* note 52.

402 Id.

403 Id at 187.

the same i.e. to circumvent any AML measures that inhibit one's ability to launder the proceeds of crime through the financial system.

Claims of anonymity or pseudo-anonymity arise more in transactions using bitcoin than in the mining process. This is because the mining process introduces new coins into the bitcoin ecosystem and does not involve transactions per se. On the other hand, there are difficulties in keeping track of bitcoin transactions given the lack of personal details in the course of those transactions.

Bitcoin offers transactional anonymity given that the sender need not meet the receiver in person for the transaction to take place. The only information disclosed for all to see is the public keys and the amount of the transaction. While cash is also relatively anonymous, the total amount of cash in circulation is known because it is produced from a single source (usually the Federal Reserve or central bank of a country) and marked according to serial numbers. However, no one would be able to say for certain who is holding what particular note or coin of the currency at any time unless in law enforcement 'sting operations' where marked bills are put in circulation often for the purpose of tracing its use to drug dealers and traffickers. As discussed in chapter 2, the downside (from the perspective of the criminal actors) when it comes to using cash is mainly that its bulk prevents it from being moved easily (particularly across borders) as this heightens the chance of detection. In contrast, bitcoin use does not have this disadvantage as it does not require the physical movement of any object. To conclude a bitcoin transaction, all that is required is access to the Internet in order to connect to the Bitcoin network and thereafter send or receive bitcoins from anywhere in the world. Consequently, the ability to keep transactions anonymous could make bitcoin more attractive to criminal actors.

4.7.1 Mixers

The use of "mixers" has become more popular as a technique for further concealing transactions in the bitcoin ecosystem. Mixers are an anonymizing tool used to obscure the source of funds or

the details of transactions by combining multiple transactions.[404] In so doing, they help to obfuscate the blockchain record of a transaction which its sender or receiver desires to remain private.[405]

This service, where employed by criminal actors, facilitates the laundering of illicit funds.[406] The mixing service Bitcoinfog.com advertises that its service prevents third parties from tracking the origin of a particular address, stating: "if properly done […] you can eliminate any chance of finding your payments and make it impossible to prove any connection between a deposit and a withdrawal inside our service."[407] Often times those desirous of hiding their online activity use a combination of mixing services and TOR and by doing so, add an extra layer of obscurity to transactions. While these software services are not impenetrable, they add an extra layer of difficulty to the already challenging efforts at combatting money laundering.

The above evaluation of mixing services and bitcoin exchanges demonstrates their significance for illicit activity. Attempts to regulate cryptocurrencies face the added challenge that such services often employ further anonymization techniques (usually TOR), which further complicates efforts to trace the identity or location of illicit users.[408]

4.7.2 De-anonymizing and Tracing Bitcoin Transactions

In order for the use of bitcoin to be truly attractive for money laundering, anonymity within the bitcoin ecosystem must be realised. To this end, various scholars have conducted empirical studies on whether anonymity or some variation thereof ('pseudo-anonymity') exists in a form that could obfuscate the link between proceeds and crimes and the beneficiaries of those proceeds. These

404 Sarah Gruber, "Trust, Identity and Disclosure: Are Bitcoin Exchanges the Next Virtual Havens for Money Laundering and Tax Evasion (2013) 32 Quinnipiac Law Review 135.

405 *Id*.

406 Id, observing that TORwallet, a mixing service, advertises on its website that by using its service, clients can mix their funds with a large Bitcoin pool and their Bitcoins would then be returned to them "freshly laundered."

407 See Sarah Gruber, "Trust, Identity and Disclosure" *supra* note 404 at 176 quoting information from bitcoinfog.com.

408 The regulation of cryptocurrencies including these challenges are discussed in detail in chapter 5.

research projects specifically focused on whether bitcoin is a tool for money laundering, terrorist financing and other transnational crimes have varied in their findings. [409]

Fergal Reid and Martin Harrigan, for instance, conclude that using heuristics that identify ownership relationships, it is possible to identify a link between IP addresses and bitcoin keys.[410] Philip Koshy, Diana Koshy, and Patrick McDaniel also found that transactions cannot be tracked in some instances, especially where the bitcoin exchanges choose to use mixers and other anonymization tools to obscure both their location and source of funds.[411]

In Reid and Harrigan's study, they were able to identify distinct characteristics of Bitcoin users[412] which could be combined with external online information on forum posts to deanonymize the real identify of the Bitcoin users.[413] Perri Reynolds and Angela Irwin apply a similar methodology, considering whether information provided to four bitcoin exchanges by clients at the initial sign-up of the relationship can later be used by law enforcement for investigation purposes. [414] They collate information external to the bitcoin network and then link that information to the bitcoin transactions towards tracing the transaction to the originator.[415] Reynolds and Irwin's study found that there were lapses in KYC and due diligence by these bitcoin exchanges. [416] Such lapses in the bitcoin exchanges could enable technologically clever (illicit) users to conceal their identities and

---

409 Some literature on this point (not highlighted here) include: Ralph Gross, & Alessandro Acquisti, "Information revelation and privacy in online social net- works" Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, Alexandria, VA, 7-10 November 2005, 71-80. Elli Androulaki et al, "Evaluating user privacy in bitcoin" in Ahmad-Reza Sadeghi. (ed.) Financial Cryptography and Data Security FC 2013 Lecture Notes in Computer Science Vol. 7859 (Berlin: Springer, 2013). Sarah Meiklejohn, et al, "A fistful of Bitcoins," *supra* note 382.

410 Fergal Reid and Martin Harrigan, "An Analysis of Anonymity in the Bitcoin System" in Yaniv Altshuler, et al, (eds.) Security and Privacy in Social Networks (New York: Springer, 2013) at 197. See also Ralph Gross, & Alessandro Acquisti, "Information revelation and privacy in online social networks" *supra* note 409.

411 Philip Koshy, Diana Koshy, and Patrick McDaniel, "An analysis of anonymity in Bitcoin using P2P network traffic" (2014) Financial Cryptography and Data Security, 469.

412 The researchers draw from mathematical topology towards an analysis of what details of bitcoin transactions and its users remain following efforts to obscure transactions. The topology of bitcoin users are the properties that are preserved through any attempts to obscure transactions or identity within the bitcoin network. Fergal Reid and Martin Harrigan, "An Analysis of Anonymity in the Bitcoin System" supra at note 410 at 15.

413 Id.

414 Id.

415 Perri Reynolds and Angela S.M. Irwin "Tracking Digital Footprints: anonymity within the bitcoin system" *supra* note 52 at 187.

416 *Id.* Irwin *et al* also find that bitcoin transactions have a high potential for anonymity given that a bitcoin account can be set up without identification which if required at any point, can be circumvented. See Angela S.M. Irwin, *et al,* "Are the financial transactions conducted inside virtual environments truly anonymous?" *supra* note 16.

ensure their transactions are not traced back to them. This, Reynolds and Irwin conclude, could facilitate the circumvention of AML standards. [417]

Reynolds and Irwin's study highlights the significance of due diligence protocols for financial institutions. [418] They note that bitcoin accounts are not tied to any traditional bank account that carries out KYC/CDD. [419] Furthermore, bitcoin exchanges permit their account holders deposit huge sums of cash which can then be transferred to another account anywhere in the world. [420] Consequently, a combination of these two factors (amongst others) could further complicate tracing efforts.[421] The authors also point out that technologically savvy criminals may circumvent identify controls by carefully selecting Bitcoin exchange providers that do not require identifying information in the first place, or who may be easily satisfied by fraudulent information.[422]

The outcome, it is suggested, is that large criminal organizations such as the transnational organized crime groups considered in this work would be able to employ technological expertise which understands the operation of cryptocurrencies, and also which exchanges lack robust AML practices. Given their size and capacity, together with a probable history of avoiding detection, such groups could avoid detection by law enforcement by using cryptocurrencies.[423] In addition, the possibility for data obtained in the course of the above research projects to be unreliable casts a shadow over its potential for evidentiary purposes. Both Reid and Harrigan, and Reynolds and Irwin apply heuristics in making conclusions on the identity of bitcoin users. Inaccuracies in the findings could stem from the use of the heuristic analysis. This is because heuristics involves

417 *Id.*
418 Id at 31.
419 Id.
420 Id.
421 Id.
422 Perri Reynolds and Angela S.M. Irwin "Tracking Digital Footprints" *supra* note 52 at 180. In addition to this is the use of mixing services who exist to protect the privacy of bitcoin users. See Sarah Gruber, "Trust, Identity and Disclosure," *supra* note 404 at 176, referring to bitcoinfog.com, a "mixing service" (amongst many other) whose aim to protect its users from third-parties seeking to track their bitcoin transactions.
423 Perri Reynolds and Angela S.M. Irwin "Tracking Digital Footprints" *supra* note 52 at 181.

making assumptions on the basis of anecdotal evidence.[424] Such conclusions may, in the absence of other supporting, be rejected as evidence linking an individual to illicit bitcoin transactions.

Arvind Narayanan & Malte Möser also comment that it is the open source nature of the bitcoin software (all transactions are contained on the blockchain ledger and are "public, global, and immutable") that motivates users seeking anonymity towards obfuscation techniques that enable them to maintain financial privacy.[425] Importantly, their study highlights that although anonymity is possible through the use of bitcoin,[426] this does not guarantee privacy as the pseudonyms can be linked to identities as noted by Reid and Harrigan above.[427]

The focus of these studies on anonymity in the context of bitcoin exchanges rather than the Bitcoin network itself is interesting. It is also in keeping with the observation made earlier in this thesis that illicit activity using bitcoin appears to be a greater concern in the context of bitcoin exchanges as opposed to the Bitcoin network itself. This is especially likely in the context of those bitcoin exchanges that employ mixers and obfuscating techniques such as TOR.[428] These disguising tools exist for the purpose of "exponentiating the complication of deanonymization attempts" of bitcoin transactions.[429]

Malte Möser and Rainer Böhme note that the market for anonymization tools for bitcoin transfers is growing with transactions conducted by JoinMarket ("a growing marketplace for more anonymous transfers in the Bitcoin ecosystem"[430]) worth an estimated $29.5 million USD in just 13 months.[431] In addition to this, the fees for such anonymization average <0.01percent of the

---

424 See Daniel Kahneman, Paul Slovic, and Amos Tversky (eds.), *Judgment Under Uncertainty: heuristics and biases* (Cambridge: Cambridge University Press, 1982).

425 Arvind Narayanan & Malte Möser, "Obfuscation in Bitcoin: Techniques and Politics" presented at the International Workshop on Obfuscation: Science, Technology, and Theory, New York University, April 7-8, 2017, online: <https://arxiv.org/pdf/1706.05432.pdf>.

426 Using a bitcoin "wallet", anyone can generate a pseudonym to send or receive payments without providing personal information. See Arvind Narayanan et al, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, *supra* note 342.

427 Fergal Reid and Martin Harrigan, "An Analysis of Anonymity in the Bitcoin System" supra at note 410.

428 Malte Möser, and Rainer Böhme, "The price of anonymity" supra note 349 at 127. Perri Reynolds and Angela S.M. Irwin "Tracking Digital Footprints" supra note 52 at 180. Arvind Narayanan & Malte Möser, "Obfuscation in Bitcoin" *supra* note 425.

429 Id at 128.

430 Id at 127.

431 Id at 134.

transaction which is minimal given the (likely underestimated) money laundering figures discussed in chapter 2. Though estimates, what the figures do tell us is that the combination of low-cost and anonymized bitcoin transactions is likely to attract money launderers looking for ways to launder the proceeds of their crimes.

4.8 Why is Bitcoin Attractive for Criminal Purposes?

The empirical research analysed above demonstrates a potential for cryptocurrencies to be used for facilitating money laundering and other transnational crimes. The extent to which this is possible, and its attraction in that regard, remains the subject of speculation. To support the argument for the expansion of the AML regime to cover cryptocurrency operations, I draw on theories from the criminology discipline to identify factors that could explain the potential for illicit use of cryptocurrencies in facilitating money laundering. Expanding the existing AML regime in this manner could inhibit the potential growth of cryptocurrencies for laundering proceeds of transnational crimes.

Criminologist Ronald Clarke observes that technology is attractive for criminal purposes where it creates a new environment for social interaction. By creating such opportunities, technology could be exploited for both licit and illicit purposes.[432] The logic behind this claim is that in the current global environment, relationships and transactions are heavily reliant on the Internet and technology. This is because technology enables fast-paced (often instant) transactions that are also cost-effective. At the same time that these tools are being used for legitimate purposes, criminal actors are also evolving in their methods and techniques (mixers and TOR discussed above) and adapting to new and improved ways of committing crimes. Conversely, law enforcement moves at a relatively slower pace, continuing to focus on established and entrenched criminal methods leaving technologically-savvy criminals with room to perpetrate their illicit activities.[433]

---

432 This idea is discussed in detail in chapter 2. See also Ronald V. Clarke, "Technology, Criminology, and Crime Science" *supra* note 57.

433 Id.

A few criminological theories are intertwined in this analysis. First, environmental criminology suggests that an individual's environment determines and facilitates potential opportunities for criminal activity.[434] Where a criminal opportunity presents itself, the offender decides whether to commit the crime by conducting a cost-benefit analysis (the rational choice analysis).[435] At the foundation of the Rational Choice Theory is the idea that crime is a choice and every individual as a rational being has an equal likelihood of committing crime. Criminal actors will engage in crime if the perceived benefits that accrue if the crime is successfully committed outweigh the risks associated with the crime.[436]

Clarke and Cornish suggest that a criminal actor would arrive at the decision to commit a crime following an internal rationalization of the cost and benefits that accrue to their specific circumstances.[437] Therefore the decision to commit or not involves both general factors and those peculiar to each individual. This analysis applies both at the time of an initial decision to commit a crime as well as to a decision to reprise the criminal activity.[438] On this basis, the authors suggest that engaging with these factors for each specific crime would enable policymakers to better control crime.

Drawing from the overview of cryptocurrencies and their use in the context of illicit activities, the potential offender may consider whether the crime is one where comprehensive legislative framework and law enforcement oversight exists, the likelihood of apprehension by authorities, the amount of financial benefit obtainable, opportunities to successfully launder the proceeds of the crime upon completion, and the ability to integrate such proceeds seamlessly into the legitimate financial economy.

---

434 Environmental criminology suggests that criminogenic potential is determined by the moral context of the environment together with exposure to temptation and provocation in the physical environment. See Richard Wortley & Lorraine Mazerolle, Environmental Criminology and Crime Analysis. (London: Willan, 2008); Gerben J.N. Bruinsma, Lieven J.R. Pauwels, Frank M. Weerman, Wim Bernasco, "Situational Action Theory: Cross-Sectional and Cross-Lagged Tests of Its Core Propositions" (2015) 57:3 Canadian Journal of Criminology and Criminal Justice, 363 at 366.

435 Ronald V. Clark & Derek B. Cornish. "Modelling Offenders' Decisions: A Framework for Research and Policy." (1985) 6 Crime and Justice, 147.

436 Id.

437 Id at 151.

438 Id.

Furthermore, where the objective of the criminal actor is to launder the proceeds of transnational criminal activities, they are also likely to have additional concerns. For instance, perpetrators of predicate crimes such as drug trafficking place greater emphasis on laundering methods that obfuscate the source of their funds as much as possible – they are operating businesses (albeit illicit ones) whose objective is to generate funds.[439] For terrorist financing (as a postdicate offence) on the other hand, perpetrators may place greater emphasis on ensuring the funds reach their destination as rapidly as possible especially where they are directed at a specific terrorist activity.[440]

The criminal actor may also consider the features of cryptocurrencies and conduct a cost and benefit analysis on its viability as an alternate means of laundering the illicit proceeds. For instance, the cost of transacting with bitcoin is minimal when compared to fiat currency and thus a criminal whose illicit activities are geared towards generating as much profit as possible from their crimes may find it beneficial to use bitcoin or other cryptocurrency to launder the proceeds of his crime. Such an individual may also consider the speed of transactions and their desire to minimize tracing of the funds as much as possible, both of which are benefits of bitcoin. Consequently, the unregulated and decentralized nature of cryptocurrencies could enable criminals to explore ways of advancing their fund-generating criminal enterprise. In doing so, they further circumvent the AML regime which they may not have done previously for fear of suspicion by banking institutions or apprehension by law enforcement officials.

One of the cost considerations in using bitcoin is tracing the proceeds of the crime back to the perpetrators. This may be a low cost for illicit actors given the speed and pseud-anonymity of transactions in the bitcoin ecosystem. In addition to this, the aforementioned unregulated state of cryptocurrencies together with the transnational nature of cryptocurrency use enhance the ability of transnational criminal operators to avoid law enforcement interception. This demonstrates that the benefits to criminals, in using cryptocurrencies, presently outweigh the associated costs and

439 Louise I. Shelley & John T. Picarelli, "Methods and Motives" *supra* note 174 at 53.
440 Angela S.M. Irwin, et all, supra note 123 at 6.

will increasingly make cryptocurrencies a more attractive option for money launderers especially where the criminal activity involves transnational crime networks.

Technologically adept offenders or established transnational organized crime groups, could extend their networks to include individuals that are proficient in bitcoin and blockchain networks. This would enable them to move the proceeds of their crimes easily using favourable bitcoin exchanges (i.e. little or no due diligence for customers). Furthermore, the use of such exchanges, together with anonymization tools such as TOR and mixers, could enable crime groups to cover their tracks and compound the difficulties in tracing. [441]

Correlated to rational choice theory is the Routine Activity theory which considers that criminal acts predominantly occur where the following three factors converge: a likely offender, a suitable target, and the absence of a capable guardian.[442] Lawrence Cohen and Marcus Felson suggest that the absence of one of these factors (for instance where a capable guardian is present) is sufficient to prevent the successful completion of the criminal activity.[443] Conversely the presence of a suitable target and an absence of a capable guardian may lead to a large spike in crime rates even without any additional motivation. Therefore, the growing development of Internet and financial technology could prompt societal changes. As these changes occur, a suitable target such as bitcoin (as a tool for financial transacting) emerges. In the absence of a guardian (regulatory measures), existing offenders (money launderers and the transnational crime perpetrators) are motivated to use cryptocurrencies to facilitate their criminal activities. Consequently, it may be the absence of regulatory measures on cryptocurrencies that is attractive to criminal actors. There may not necessarily be new potential offenders looking for criminal opportunities, it may be the case that the existing criminal offenders now discover new methods for achieving their illicit objectives.

Lawrence Cohen and Marcus Felson suggest that by understanding the way these factors influence the development of criminal opportunities, policy makers may be able to identify gaps in regulation

441 Id.

442 Lawrence E. Cohen & Marcus Felson. "Social Change and Crime Rate Trends: A Routine Activity Approach." (1979) 44:4 American Sociological Review 588 at 589.

443 Id.

and act more effectively. Wortley and Mazerolle also point out that the development of Internet technology also enabled the development of the darknet, where criminal actors can network and share techniques for evading regulatory and enforcement mechanisms put in place to prevent crime.[444]

The situational crime prevention approach (SCP) draws from the above theories to develop a strategy for reducing opportunity for criminal activity. For SCP, the first step is to understand that each crime is unique and specific techniques are required to counter each type of crime.[445] Therefore SCP focuses on the crime itself and the necessary changes to the environment that would make it harder for a criminal actor to commit an offence. For instance, the SCP approach suggests that law enforcement authorities could create situations where the potential offender has the impression that there is a high likelihood that he will be caught. By causing him to have such apprehension, he is deterred from the criminal behaviour. Incorporating rational choice, the criminal path becomes less attractive. Unlike other criminological approaches, SCP focuses more on preventing criminal activity than tackling criminality (the social causes that exacerbate crime).[446] Rather, it focuses on creating the conditions through which the offender (potential or actual) desists from a specific from of crime i.e. displacing the specific opportunity for crime.[447]

To tackle specific criminal activity, the variables that lie in favour of an attractive criminal opportunity must be varied according to SCP. In our context, the criminal opportunity is money laundering of the proceeds of transnational crimes using cryptocurrencies such as bitcoin. This method is could become more attractive for money laundering. As the AML regime takes strides to tighten traditional opportunities for money laundering, traditional modes of money laundering (through banks and by smuggling cash across borders) may become less attractive. At the same time, the use of cryptocurrencies for illicit activities could grow in appeal amongst for laundering the proceeds of crime. This analysis is informed by a few factors. First, the use of cryptocurrencies remains mostly unregulated. Secondly, cryptocurrencies and the crimes they could facilitate are

444 Richard Wortley & Lorraine Mazerolle, Environmental Criminology and Crime Analysis, supra note 433.
445 Ronald V. Clarke, “Situational crime prevention” (1995) 19 Crime and Justice 91.
446 Emmanuel P. Barthe, "Situational Crime Prevention" in Kenneth J. Peak, *Encyclopedia of Community Policing and Problem Solving* (Thousand Oaks: SAGE Publications, 2013) 387-389.
447 Id.

transnational in nature. Finally, cryptocurrencies are decentralized and users can operate pseudo-anonymously. These features could inhibit the ability of law enforcement to implement effective AML measures for cryptocurrency transactions and as a result, make bitcoins and other cryptocurrencies more attractive to launderers. In order to inhibit this form of laundering, the existing AML regime needs to contend more robustly with the use of cryptocurrencies for criminal purposes. Furthermore, failure to do so could create gaps in the existing international AML regime, create new methods for money laundering, and detract from the effort made so far towards addressing money laundering and transnational crimes.

This approach has been applied successfully in related contexts. For instance, in increasing the cost of drug trafficking and reducing the rewards obtained therein.[448] Drug trafficking operations of various sizes were previously exceptionally profitable – its present profitability remains the subject of much debate as discussed in chapter 2. The proceeds of the crimes were relatively easy to launder, and it was difficult to establish a nexus between the drugs being trafficked and organized crime groups involved. By implementing a 'follow the money' approach, the illicit proceeds could be traced to beneficiaries of drug trafficking. As a result, the risks involved in drug trafficking increased, establishing a form of displacement to money laundering using banking institutions.[449] While this is not perfect, the development of this technique put a dent in that area, where previously the activities were taking place with minimal risk of detection.[450]

In the context of cryptocurrencies, these theories illustrate the potential for growth in cryptocurrency facilitated money laundering as well as strategies that could be put in place to combat them. The empirical studies on money laundering in the bitcoin ecosystem, for instance, show some illicit use. However, such studies do not reveal the gravity of the problem or why

448 For detailed exposition of this approach see Derek B. Cornish & Ronald V. Clarke (2002). "Analyzing Organized Crimes" in Alex R. Piquero & Stephen G. Tibbetts (eds.) Rational Choice and Criminal Behavior: Recent Research and Future Challenges (New York: Routledge, 2002). Derek B. Cornish, "The procedural analysis of offending and its relevance for situational prevention" in Ronald V. Clarke (ed.) Crime Prevention Studies (Vol. 3) (Monsey: Criminal Justice Press, 1994). Ronald V. Clarke, (1995). "Situational crime prevention" *supra* note 444.

449 The 'follow the money' method includes a wide-range of initiatives such as KYC, confiscation of funds, and notification of suspicious activity which has a correlating effect on trafficking in drugs.

450 Research shows that both money laundering and drug trafficking still occurs. See for instance, Margaret Beare, "Responding to Transnational Organized Crime: Follow the Money" *supra* note 13.

regulatory authorities should concern themselves with cryptocurrency operations. By understanding and applying the criminological theories identified above, the AML regime and law enforcement will be better equipped to identify[451] and tackle[452] loopholes in AML initiatives that may be exploited by launderers using cryptocurrencies.

4.9 Conclusion

At the start of this decade, it was difficult to foresee the potential growth and pervasiveness of cryptocurrencies such as Bitcoin. While cryptocurrency enthusiasts have welcomed its arrival, its volatility has caused some hesitation amongst observers and prospective users. Furthermore, experts and regulators remain uncertain on its legitimacy as a viable means of financial transactions. As this chapter demonstrates, cryptocurrencies such as Bitcoin have lower transaction fees which could be beneficial for various groups in society. Cryptocurrencies also enable financial inclusion amongst those that do not have access to traditional banking facilities. Bitcoin funds can be transferred amongst individuals anywhere in the world through Internet facilities (itself a rapidly spreading technology).

At the same time, criminal actors are also taking note of bitcoin's potential 'benefits' as a tool for laundering the proceeds of their illicit gains. Some may be attracted to cryptocurrencies due to the perception that they will be able to conduct transactions in anonymity. As I have outlined above, however, true anonymity does not exist within the bitcoin network. Existing empirical studies are somewhat speculative as to the anonymization capabilities of the Bitcoin network and bitcoin exchanges. This is understandable given the emerging nature of cryptocurrencies. While possible, it is challenging for instance to determine if an activity involves illicit funds by simply observing its record on the blockchain. However, illicit criminal actors go to great lengths to conceal their identities and associated transactions, and most of the time the same problems with estimating the value of money laundering activities and the proceeds of transnational crimes in the 'offline' world also apply here.

---

451 Here environmental criminology, rational choice, and routine activity theories would be relevant.
452 Application of a SCP approach.

What is obtainable for bitcoin transaction, is a series of tools such as tools such as bitcoin exchanges, mixers, and anonymizers (TOR) that enable bitcoin users obscure their identity. However, researchers and experts find that there are also techniques (mainly heuristics) that could be used to 'deanonymize' such transactions. This approach calls for strenuous effort and expertise on the part of law enforcement officials in order to identity of a bitcoin user or detect an illicit transaction (already arduous tasks).

The likelihood for significant actualization of money laundering using cryptocurrencies may eventually depend on the applicability of AML to cryptocurrency operations. In their present unregulated state, the attractiveness of cryptocurrencies (particularly cryptocurrency exchanges) for criminal purposes may continue to grow. This view draws on criminological theories of rational choice, routine activity, environmental criminology, and situational crime prevention.

In this chapter, I have demonstrated that money laundering does take place within the bitcoin ecosystem. At present, however, it remains marginal when compared to other methods of money laundering. The findings of this chapter are carried over into the next where I attempt to determine whether the existing framework for AML covers ML using cryptocurrencies. In doing so, I intend to identify potentially applicable provisions that could serve as a starting point for the AML regulation of cryptocurrency Thus, the claim that cryptocurrencies could be used in circumventing the existing AML regime is convincing and demonstrated above.

Chapter 5: The AML Regime and Cryptocurrencies

Anti-money laundering (AML) policymakers together with law enforcement agencies are starting to contend with cryptocurrencies as incidences of its use to facilitate money laundering emerge.[453] Chapter 4 introduced cryptocurrencies using Bitcoin as a case study and established that bitcoin facilitates money laundering and other transnational crimes. However, the extent to which such laundering occurs using cryptocurrencies appears limited so far. Nevertheless, AML institutions are concerned that cryptocurrencies allow users to trade (in virtual currency) without revealing their real-world source of income or their own identity. This could in turn, make cryptocurrencies attractive to illicit users such as criminals seeking to obfuscate the links between themselves and the proceeds of their crimes. Furthermore, such criminal actors could then be able to integrate such funds into society without drawing suspicions to themselves or their transactions.[454]

In this chapter, I evaluate whether cryptocurrencies could be categorized as assets in order to bring them within the purview of the international AML regime: the treaty and non-treaty initiatives designed to combat transnational crimes including money laundering.[455] Having established in Chapter 4 that cryptocurrencies could facilitate the laundering of proceeds of crimes, I draw on the AML framework and thematic areas described in chapter 3 to evaluate whether the technique of money laundering using cryptocurrencies can be brought within the current international AML framework. [456] The importance of this approach is that it identifies and examines the jurisdiction

---

453 See United States v Ross William Ulbricht, *supra* note 26.
The United States Attorney's Office Southern District of New York Press Release, "Liberty Reserve Founder Arthur Budovsky Sentenced in Manhattan Federal Court To 20 Years for Laundering Hundreds Of Millions Of Dollars Through His Global Digital Currency Business" (9 May 2016), The U.S. Attorney's Office Southern District of New York, online: https://www.justice.gov/usao-sdny/pr/liberty-reserve-founder-arthur-budovsky-sentenced-manhattan-federal-court-20-years>; FATF (2015). FATF Report. Emerging Terrorist Financing Risks, online: <http://www.fatfgafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf>.

454 Perri Reynolds and Angela S.M. Irwin "Tracking Digital Footprints: anonymity within the bitcoin system" *supra* note 52. A key aspect of the AML regime involves implementation of customer due diligence and Know Your Customer (KYC) procedures which is not usually possible within the cryptocurrency protocols. Most cryptocurrencies do not require their clients to reveal their true identities in order to conduct transactions.

455 The importance of doing this lies in the fact that the international instruments examined in this thesis are applicable to proceeds of crimes where they constitute assets.

456 The following components of the international AML regime are synthesised in this chapter: United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention), United Nations Convention on Transnational Organized Crime (UNCTOC), United Nations Convention against Corruption (UNCAC), United Nations Convention against Financing of Terrorist Activities (CFT Convention), and Financial Actions Task Force Recommendations (FATF Recommendations).

of law enforcement over cryptocurrencies in incidents where they are used in money laundering. Doing so is also crucial for ensuring that cryptocurrencies (especially cryptocurrency exchanges) comply with preventive measures (customer due diligence/know your customer) that are intended to inhibit money laundering.

I also evaluate the potential challenges to applying AML to cryptocurrencies by highlighting the operational features of cryptocurrencies that may limit the effectiveness of the suggested approach e.g. the jurisdictional challenges that may be encountered where a bitcoin operator is beyond the jurisdictional reach of a domestic AML authority.

In the next section, I analyse whether cryptocurrencies constitute assets pursuant to the AML regime. Next, I consider the importance of bringing cryptocurrencies within the international AML regime. Following this, I synthesize the provisions of the international regime to identify how it could be applied to cryptocurrency activities. Finally, I evaluate potential obstacles to the above approach to regulating cryptocurrencies.

5.1 Cryptocurrencies as 'Assets'

Before delving into a discussion on the applicability of the existing AML regime to cryptocurrencies, it is important to consider whether cryptocurrencies such as Bitcoin constitute assets. This is because the international AML instruments, as described in chapter 3, apply to proceeds of crimes. Such proceeds are in turn defined as "assets of every kind". By viewing cryptocurrencies as assets, its use for facilitating money laundering could be considered within the context of the existing AML regime for which property constituting the proceeds of crimes are limited to those categorized as assets.

There have been domestic regulatory efforts to determine the nature of cryptocurrencies in the context of taxation and its ability to generate public revenue. Finland's central bank considers bitcoin to be a commodity (similar to gold) because it neither meets the legislative requirements

of a currency nor is it a payment instrument given that it lacks a "responsible issuer".[457] Sweden deems bitcoin to be an asset, thereby allowing the Swedish government to impose capital gains tax on bitcoin transactions.[458] Norway also considers bitcoin to be a taxable asset. While Canada does not categorize bitcoin as a currency, transactions involving bitcoin are considered barter trades in Canada in order to apply tax to transactions where it is used.[459] The German central bank considers bitcoin to be a "unit of account" which can be used for tax or private trading.[460]

The above state practices suggest that states place a considerable emphasis on the generation of income, through taxation, from the use of cryptocurrencies. Given that the economic value of cryptocurrencies continues to rise (even with its volatility), such policy focus is justified.

However, it is also important to consider the implications of cryptocurrencies from an AML perspective given that there are identified instances of cryptocurrency use in facilitating money laundering. Chapter 4 of this thesis has demonstrated tangible use of cryptocurrencies in money laundering which though minimal at present, has potential for growth when examined through the lens of criminological theories.

Pursuant to the UNCTOC, proceeds of crime refers to any property obtained from the commission of a predicate offence whether such proceeds are obtained directly or indirectly.[461] Property is in turn defined as "assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in, such assets."[462] The CFT Convention notes that proceeds of crime are funds derived from the commission of any of the offences contained in the convention.[463] The CFT convention further

---

457 Kati Pohjanpalo, 'Bitcoin judged commodity in Finland after failing money test', Bloomberg, 20 January 2014 online: <https://www.bloomberg.com/news/articles/2014-01-19/bitcoin-becomes-commodity-in-finland-after-failing-currency-test>.

458 Veronica Ek and Johan Carlstrom, 'Bitcoin turns into art as Sweden rejects creative currency', Bloomberg, 23 January 2014. David George-Cosh, 'Canada says Bitcoin isn't legal tender', Wall Street Journal, 16 January 2014

459 This position is conflicting given that some would consider money to be a means for barter or payment in exchange for goods and services. See Anton Cruysheer, "Bitcoin: A look at the Past and the Future" in David Lee Kuo Chuen (ed.) *Handbook of Digital Currency*, *supra* note 49 at 301.

460 Kim-Wang Raymond Choo, "Cryptocurrency and Virtual Currency: Corruption and Money Laundering/Terrorism Financing Risks? in David Lee Kuo Chuen (ed.) *Handbook of Digital Currency*, *supra* note 49 at 301.

461 UNCTOC, *supra* note 34 at article 2(e).

462 Id.

463 CFT Convention, article 1(3).

defines funds as "assets of every kind, whether tangible or intangible" including the electronic or digital representation of the assets. [464]

The Routledge Dictionary of Economics defines an 'asset' as "a resource with a market value; a unit of value capable of earning and income; […]. Real (or tangible) assets include land and machinery; intangible assets include goodwill and patents; financial assets include cash and stock market securities."[465]

By classifying bitcoins as things of value, we sidestep having to determine which kind of assets they are especially as the definition of property for the purpose of the UNCTOC encompasses "assets of every kind." In an observation that buttresses this point, Malcolm Campbell-Verduyn points out that "the global anti-money laundering governance is concerned with illicit transactions and financial flows whether or not they meet theoretical standards of money."[466] In light of the above literature, I consider that bitcoins constitute financial assets as they provide financial value for their owners. By viewing cryptocurrencies in this manner, its use for facilitating money laundering could be considered within the context of the existing AML regime for which property constituting the proceeds of crimes are limited to those categorized as assets.

5.2 Importance of Bringing Cryptocurrencies within the Existing International AML Regime

Cryptocurrencies just like transnational crimes are cross-border in nature. The cross-border nature of such crimes prompted the development of an international AML regime to tackle difficulties encountered by singular states in dealing with money laundering within their domestic laws..[467] In

---

464 Id, article 1(1). The arguments concerning the UNCTOC is therefore relevant here. The FATF Recommendations (r3) refers to the provisions of the Vienna Convention and the UNCTOC on criminalization of money laundering. The offences include "participation in an organised criminal group and racketeering; terrorism, including terrorist financing; trafficking in human beings and migrant smuggling; sexual exploitation, including sexual exploitation of children; illicit trafficking in narcotic drugs and psychotropic substances; illicit arms trafficking; illicit trafficking in stolen and other goods; corruption and bribery.

465 Donald Rutherford, *Routledge Dictionary of Economics* (3rd ed.) (London: Routledge, 2013) sub verbo "assets".

466 Malcom Campbell-Verduyn, "Bitcoin, crypto-coins, and global anti-money laundering governance" (2018) 69 Crime Law and Social Change 283 at 286.

467 States are obliged to assist one another in their efforts to supress the illicit activities which the conventions aim to curb. The UNCTOC and UNCAC both refer in their preambles to the importance of international cooperation among states on the

the past, launderers were able to rely, to a greater extent, on differences in AML policies among different countries as a means of facilitating their operations.[468] As cryptocurrency use gains momentum, the challenge for a single state seeking to combat its use for facilitate money laundering and other transnational crimes points to the need for a comprehensive framework for regulating cryptocurrencies. The importance of this approach lies in preventing particular jurisdictions with less stringent AML laws from becoming safe havens for launderers.

5.3 Cryptocurrencies and AML Preventive Measures

A key preventative aspect of the AML regime lies in implementation of customer due diligence (CDD) measures. Prevention within the AML regime requires reporting, monitoring, and detection of suspicious financial transactions. It also necessitates the establishment of a supervisory regime for banks and non-bank financial institutions. In this section, I examine cryptocurrencies within the context of these provisions for the purpose of highlighting how they could be regulated under the existing international AML regime.

5.3.1 Due Diligence Under the AML Regime

CDD involves know your customer (KYC) procedures whereby banks verify the identity of potential and existing customers before opening bank accounts or carrying out certain transactions. CDD also involves keeping records of transactions, reporting suspicious transactions to the relevant oversight bodies, supervision by said oversight bodies, and application of sanctions for non-compliance.[469] As a preventive measure, CDD assists law enforcement in tracing suspicious transactions back to the initiator or beneficiary.[470]

The preventive approach to AML recognizes that financial institutions play a primary role in facilitating financial transactions. Furthermore, in light of their centralized operational systems,

---

relevant matters, as do most of the other international instruments. The FATF recommendations emphasize the importance of intensifying cooperation among domestic authorities in the fight against money laundering.

468 Paul Alan Schott, Reference Guide to Anti-Money Laundering, *supra* note 220.

469 See for instance FATF Recommendations, at recommendations 9, 10, 15, and 20.

470 Perri Reynolds & Angela S.M. Irwin, "Tracking digital footprints" supra note 52 at 185.

imposing such CDD responsibilities on financial institutions is also considered an effective AML strategy.[471] In contrast, cryptocurrency networks (distinct from the cryptocurrency exchanges), while also facilitating financial transactions, rely on a decentralized network of users who are domiciled all over the world for transaction verification. In the absence of monitoring or supervisory authority within the network it becomes challenging to impose AML requirements and ensure compliance." Thus, AML efforts could be sidestepped in the Bitcoin network by criminals seeking to launder proceeds of crime.

Therefore, the role played by bitcoin exchanges is significant. Literature often fails to make the distinction between the Bitcoin network and bitcoin exchanges. While the former is completely decentralized, the latter may be considered centralized although they facilitate transactions globally. Bitcoin exchanges facilitate the buying, selling, trading, and investment in bitcoin. Therefore, exchanges give the BTC practical utility, accessibility, and universal appeal. Exchanges also have the ability to set policies that govern transactions that occur within their network including AML guidelines. In particular, some bitcoin exchanges – striving for legitimacy – have incorporated AML policies on their own initiative. Bitstamp, for instance, developed an AML policy published on its website. However, Bitstamp's AML policy stipulates that it (Bitstamp) is an unregulated corporation operating outside the scope of AML/CFT obligations.[472] In spite of this disclaimer, Bitstamp seeks to affirm its legitimacy as a bitcoin exchange through compliance with UK AML legislation.[473]

Notwithstanding the absence of express regulations on cryptocurrencies, the definition of financial institutions by the FATF in its recommendations suggest that AML provisions could apply to the activities of cryptocurrency exchanges. The FATF defines 'financial institutions' as a person (natural or legal) conducting (including but not limited to) one of the following business practices

---

471 In addition to international financial advisers, lawyers and accountants pursuant to the Gatekeepers Initiative to perform similar due diligence functions that aid in identifying, reporting, and preventing money laundering by transnational crime perpetrators seeking avenues to launder the fruits of their crimes. See Bruce Zagaris, "Gatekeepers Initiative: Seeking Middle Ground between Client and Government" (2002) 16 Criminal Justice 26; Duncan E. Alford, "Anti-Money Laundering Regulations" *supra* note 206 at 441.

472 Bitstamp, Bitstamp Limited Anti Money Laundering ("AML") and Counter Terrorist Financing ("CFT") Policy, *supra* note 353.

473 Id.

on behalf of a customer: "acceptance of deposits and other repayable funds from the public; the transfer of money or value, which includes financial activity in both the formal and informal sector." The financial activity in the informal sector includes alternative remittance activity. However, excluded from this definition are any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds.[474] As cryptocurrency exchanges engage in the practices attributed to financial institutions above, the FATF definition of financial institutions could apply to their activities. This is especially so given the reference to financial activity in both the formal and informal sector in the FATF Recommendations.

Any institution falling within this definition would constitute a regulated institution and thus is required to carry out regular checks on customers to ensure they are dealing with *bona fide* clients and to enable them to detect and report suspicious activities.[475] On the basis of such an interpretation, cryptocurrency exchanges could be required to implement the recommended CDD obligations as is the case with other financial institutions. Such an approach could in fact be beneficial for exchanges that wish to improve mainstream perception of cryptocurrencies as a legitimate alternative tool for financial transactions. Empirical studies show that bitcoin exchanges wishing to appear legitimate already self-regulate by applying these disclosure standards. [476] However, the same cannot be said for all exchanges as some were susceptible to money laundering. The research by Perri Reynolds and Angela Irwin attributes this vulnerability of exchanges to a failure to implement transparency procedures that would enable law enforcement to trace illicit transactions when they become necessary.[477] For instance, where exchanges have implemented a procedure of rejecting customers who obscure their locations using TOR (which may be used by criminal actors), submit unverifiable information, refuse access to their site, or flag emails

---

474 Financial Action Task Force International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, online: < http://www.fatf-gafi.org/recommendations.html >. p. 115).

475 Caroline Doughty, "Know your customer" supra note 208 at 250.

According to the FATF Recommendations, "Designated non-financial businesses and professions means: a) Casinos; b) Real estate agents; c) Dealers in precious metals; d) Dealers in precious stones; e) Lawyers, notaries, other independent legal professionals and accountants; f) Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under these Recommendations".

476 Perri Reynolds & Angela S.M. Irwin, "Tracking digital footprints" supra note 52 at 185.

477 Id.

associated with an account engaging in suspicious activities, they are essentially complying with CDD requirements which enable law enforcement to track the identity of users during their investigations.[478]

On this point, several cryptocurrency exchanges are already adopting self-regulatory initiatives aimed at legitimizing cryptocurrencies in mainstream finance. A group of leaders in the digital currency sector has established a committee, the Digital Asset Transfer Authority (DATA), to develop best practices and standards for the management of digital asset transfers worldwide.[479] Its guidelines so far include AML policies intended as a self-regulation initiative.[480] DATA consists of best practices based on FATF Recommendations. Its AML policies urge operators who provide digital currency products and services to implement them as a way of preventing the use of their services for illicit purposes. This initiative signals a recognition by cryptocurrency operators of the potential for their networks to be used for illicit purposes. Such recognition may also prove significant when law enforcement authorities are seeking to establish complicity by cryptocurrency exchanges for money laundering offences.

Relying on displacement theory, and given the fact that bitcoin activities remain mostly unregulated, it is plausible that potential users who are blocked by a bitcoin exchange and who wish to facilitate both legitimate and illegitimate transactions would likely take their 'businesses' to other bitcoin exchanges who may not be as particular about the use of TOR or other CDD requirements.[481] Furthermore, the FATF recommendations already provide that "financial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names." [482] It could follow that self-regulation by some but not all bitcoin exchanges

478 Id.

479 Taken from the DATA website at: www.dataauthority.org>.

480 DATA, Anti-Money Laundering Guidelines (2014), online: < http://datauthority.org/blog/2015/07/01/global-aml-kyc-guidelines-data/>.

481 Displacement theory is the idea that a motivated criminal will commit crimes elsewhere when deterred by crime prevention efforts. See Derek B. Cornish & Ronald V. Clarke, "Understanding Crime Displacement" *supra* note 59.

482 Perri Reynolds & Angela S.M. Irwin, "Tracking digital footprints" supra note 52 at 185.

could see the unregulated ones become targets of launderers, highlighting the need for AML regulation beyond voluntary efforts.

Article 18(b) of the CFT convention, in terms similar to the FATF's CDD provision above, directs state parties to implement measures that require financial institutions within their respective domiciles to adopt the most efficient measures available for customer identification.[483] This provision also applies to banking officials as well as any other professionals involved in facilitating financial transactions. The stipulation extends to all customers, whether occasional or regular, as well as to the beneficiaries of such accounts with financial institutions.[484] Consequently, article 18(b) of the CFT convention appears broad enough to capture the use of cryptocurrencies in facilitating the funding of terrorist activities.[485]

To carry out CDD effectively, the FATF recommendations suggest that independent data be used to verify the information submitted by customers as well as information on the beneficiaries of the transactions, where they differ from the customer. [486] Here it is important to point out that bitcoin and other cryptocurrencies have been hailed as a low-cost alternative to traditional banking transactions. However, I would argue that for bitcoin exchanges to implement mandatory CDD requirements, the cost of transactions may increase to an extent that could in turn reduce its attraction for some users (if the costs amount to more than a slight increase). For instance, carrying out customer identity verifications could involve obtaining independent (legitimate) data and may require the skills beyond the capability of a cryptocurrency exchange institution. For legitimate users who are seeking alternative means of financial transactions, an increase in costs may be dissuasive if the margin of increase is wide. For criminally-minded users who are more concerned with perceived anonymity rather than costs (especially where their criminal operations yield enormous proceeds), they are unlikely to be dissuaded by an increase in costs if their aim of

483 The CFT Convention, article 18(b).
484 Id.
485 The CFT Convention, article 18(b).
486 The inclusion of beneficial owner is intended to target "smurfing" where transactions are conducted at the instance of another attempt to disguise the true identity of the beneficiary. See FATF Recommendations, "General Glossary" at p110.

obscuring links to their transnational criminal activities can still be achieved using cryptocurrencies.

5.3.2 Reporting, Monitoring and Detection Under the AML Regime

All businesses engaging in financial transactions (financial institutions, designated non-financial businesses and professionals) are required to report suspicious transactions on the basis of their due diligence obligations under the AML regime.[487] Having established that cryptocurrency exchanges in particular constitute could fall within existing AML provisions, they would also be required to report suspicions that customers may be using their services to launder the proceeds of crimes. In reporting to the relevant financial intelligence units, they are also prohibited from notifying the customer that their activity is being reported.[488]

To carry out these responsibilities, bitcoin exchanges and related service providers would require training on the key indicators of suspicious activities, monitoring and detection skills, and of routes and techniques of laundering activities.[489] Such training should also include training on "combatting organized crime committed through the use of computers, telecommunications networks or other forms of modern technology." [490] Given the rapid and irreversible nature of bitcoin transactions, together with difficulties in tracking transactions and detecting suspicious activities in the bitcoin ecosystem, this provision can be interpreted as requiring training for law enforcement personnel. Pursuant to this provision, training would also be required for AML experts concerning money laundering using bitcoin and other cryptocurrencies in addition to that given to the bitcoin exchanges.

In addition, FATF Recommendations also provide for the implementation of dissuasive sanctions on financial institutions, designated non-financial institutions, their directors, and senior management that fail to comply with their reporting obligations under the relevant AML

---

487 Id, R23.

488 Defined in Chapter 3 of this work.

489 See UNCTOC, article 29. See also Paul Alan Schott, Reference Guide, supra note 220 at VI-19-20. For instance, a very high account turnover not commensurate with the balance size or the withdrawal of assets immediately after deposit.

490 See UNCTOC article 29(1)(h).

obligations.[491] The AML policy statement of Bitstamp indicating AML instruments do not apply to their operations would not be enough to avoid liability in this instance.[492]

In dealing with banks and financial service providers who do not have any physical presence or affiliation with a regulated financial group (a category that would surely include bitcoin service providers), UNCAC urges signatory states to implement measures that regulate such organizations. This category potentially includes bitcoin and other cryptocurrencies given their decentralized nature. It would also include bitcoin exchanges whose operations are predominantly (but not in all instances) Internet-based. Tracing the proceeds of crime may be hampered if the domicile of a bitcoin exchange is unidentifiable or outside the jurisdiction of an investigating authority. Where this occurs, a bitcoin exchange could potentially evade attempts to obtain its customer records or claim lack of jurisdiction by the agency.[493]

5.3.3 Supervision

The UNCTOC and UNCAC both obligate state parties to institute a comprehensive domestic regulatory and supervisory regime for banks and non-bank financial businesses.[494] Such supervision is also intended to cover other businesses that provide formal or informal services for the transmission of money or value and, where appropriate. [495]

The CFT Convention also contains provisions on supervision along the lines of the UNCAC and UNCTOC, stating that measures for the supervision of all money transmission agencies should be put in place together with measures to detect the physical cross-border transportation of cash and bearer negotiable instruments.[496]

---

491 Id, R35.

492 Their policy statement also suggests that they have an appreciation of the import of AML in the context of their operations.

493 Pursuant to CFT Convention, article 18(b), the CFT also contains provision on similar terms to the UNCAC and UNCTOC on opening and operation of accounts by unidentifiable customers.

494 UNCTOC, at article 7(1). UNCAC at article 14, supra note 38.

495 Id.

496 CFT Convention, article 18(2)(a) & (b).

In analysing these provisions, it appears that the work of monitoring suspicious activities is not left solely to banking and non-banking financial institutions. This follows the observation that in some instances financial institutions or their officials may be compromised, particularly where corrupt activities come into play. An example of this is where state funds are laundered at the initiative of corrupt officials.[497] As mentioned above with regards to reporting, monitoring and detection pursuant to article 29 of UNCTOC, training for law enforcement personnel and AML experts on money laundering using bitcoin and other cryptocurrencies is essential to enable them to understand and supervise financial operators who deal with cryptocurrencies.

5.4 Cryptocurrencies and the Money Laundering Offences in AML Instruments

The provisions of the Vienna Convention concerning money laundering are limited in the sense that drug trafficking its only predicate crime. Given the evolution of transnational crimes discussed in chapter 2, a better approach may be to look to later instruments that extend the scope of money laundering offences beyond drug trafficking. Adopting this approach takes account of the diverse forms of predicate offences. It is also in keeping with the use of cryptocurrencies for illicit purposes beyond the realm of drug trafficking.[498]

Money laundering pursuant to the UNCTOC involves, amongst other things, conversion or transfer of property known to constitute the proceeds of crime. Furthermore, money laundering is also employed in order to facilitate the *concealment or disguise* of the illicit origin of the funds or for the purpose of enabling an individual or group of individuals evade the legal consequences of their action. Money laundering also occurs where the true nature, source, location, disposition,

497 The FATF Recommendations use the term politically exposed persons (PEPs) to describe public officials that are particularly susceptible to corrupt practices. The 'Definition' section of the FATF Recommendations explains that PEPs are "individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials."

498 All serious crimes are considered predicate offences for the purpose of the convention (see UNCTOC article 6(2)(b)). The UNCTOC, CFT Convention, and the FATF Recommendations similarly recognise the existence of predicate and postdicate offences to money laundering beyond drug trafficking.

movement or ownership of property knowing that such property constitutes the proceeds of crime.[499]

On the basis of article 6, bitcoin transactions could be interpreted as falling within the provisions of the UNCTOC where such transactions facilitate laundering the proceeds of crime. For instance, one method of obtaining bitcoins involves conversion of property (from fiat money to bitcoins). This interpretation could extend to those involved in processing such a transaction, mainly bitcoin exchanges.

It may be possible to establish the requisite mental fault for money laundering (intentionally converting or transferring property knowing that such property constitutes the proceeds of crime)[500] offences where bitcoin exchanges do not comply with AML requirements such as implementing KYC practices concerning their customers (similar to what banks are expected to do). Article 6(2)(f) of the UNCTOC for instance states that "knowledge, intent or purpose required as an element of an offence […] may be inferred from objective factual circumstances." This provision seems accepting of constructive knowledge (implied based on evidence) but likely falls to the interpretation of domestic courts in any given instance. Moreover, the determination by domestic courts would in turn be influenced by the legal traditions of the court's jurisdiction.[501] For instance, in common law traditions, intent is generally satisfied by establishing wilful blindness but this is not necessarily the case elsewhere.[502] Beyond such traditions however, the lack of uniformity in requirements for mental fault may result in gaps in establishing that an offence has taken place. Such gaps could in turn be exploited by money launderers.

In their empirical study, Reynolds and Irwin find that some bitcoin exchanges do not verify the information supplied by their customers before permitting transactions on their network.[503] By failing to do so, illicit actors who seek to launder the proceeds of their crimes are able to input fake

499 See UNCTOC article 6 on criminalization of the laundering of proceeds of crime.

500 Id.

501 In the *Travaux Préparatoires* to the UNCTOC, *supra* note 67 at 42, one delegation proposed that the text concerning intent to participate in a criminal group be removed from the instrument as its substance fell within the purview of domestic courts.

502 The differences in this regard are discussed further in a later section in this thesis.

503 Perri Reynolds & Angela S.M. Irwin, "Tracking digital footprints" *supra* note 52 at 180.

information concerning their identity with the intention of obfuscating the source of their funds. CDD could address some of the challenges faced by law enforcement agencies seeking to analyze interactions on bitcoin exchanges. Putting CDD in place would also inhibit the ability of technologically savvy or wealthy criminals to circumvent identity controls or transact using fake identities.[504] Such measures could reduce the objective factual circumstances that suggest the involvement of such bitcoin exchanges in money laundering offences.

Article 6 UNCTOC also refers to the offence of concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime. The use of mixers as well as TOR to obscure bitcoin transactions and the identity of persons carrying out bitcoin transactions could potentially fall under this provision. Knowledge that the property is the proceeds of crime could be demonstrated in this instance. As highlighted in chapter 4 of this work, such obscuring techniques are commonly identified as darknet tools used in connection with illicit transactions.[505] The concerns here (as mentioned above) are the difficulty of holding such users accountable where their details and location have been obscured. It is also difficult to try and hold the operators of the mixers responsible for facilitating concealed transactions as such mixers also conceal their location (and identity), making them somewhat difficult to identify.[506]

In what seems to be an attempt to pre-empt some of the above limitations, article 6(b)(ii) contains a 'catch-all' section that provides that attempts to commit, aiding, abetting, *facilitating,* and counselling the commission of any of the offences established in accordance the article also constitutes offences. For cryptocurrencies, I would argue that where operations of certain bitcoin exchanges are structured in a way that facilitates money laundering, this provision would apply to their operations. Additionally, the absence of any due diligence efforts on the part of bitcoin

---

504 Id.

505 The darknet is considered a sort of underworld of the Internet and consists of non-indexed domains which cannot be found using regular search engines like Google. To access the darknet, TOR (the Onion Router) is used in enhancing privacy as it routes the user's Internet traffic though a global network of computers volunteering to conceal the user's location and Internet footprint. See Marie-Helen Maras, "Inside Darknet: the takedown of Silk Road," *supra* note 386.

506 Perri Reynolds & Angela S.M. Irwin, "Tracking digital footprints" supra note 52 at 180.

506 *Id*. Further discussion proving intent takes place later in this chapter.

exchanges may be suggestive of such intent, or at the very least willful blindness, towards the illicit plots of certain clients.[507]

Another provision that is of relevance to bitcoin exchanges and online platforms that facilitate transactions 'denominated' in the bitcoin currency is the UNCTOC stipulation on participation in an organized criminal group. Article 5 stipulates that where two or more persons agree to commit a predicate offence in order to obtain a financial benefit or with the intent of achieving a criminal aim, they participate in a criminal organization.[508] Where exchanges or marketplaces knowingly facilitate illicit transactions by partnering with criminal actors through lax CDD policies for instance, their actions may be interpreted as participation in a criminal organization. Bitcoin exchanges charge fees, which although less than traditional banking fees, constitute financial benefits for the operators. The operatives of Silk Road, for instance, used TOR to obscure their real-world identity.[509] They admitted to knowingly permitting money launders to employ their network to launder and utilize the proceeds of illicit activities and in doing so generated profits for themselves. Though such an admission may not be forthcoming in most instances, the individuals behind similar operations might in fact be considered participants in an organized crime group pursuant to article 5.

The UNCAC provisions are similar to what is contained in the UNCTOC. However, the UNCAC includes more specific requirements that could be applied to cryptocurrencies. Article 14 UNCAC states that a comprehensive domestic regulatory and supervisory regime is required for banks and non-bank financial institutions where such organizations provide formal or informal services for the transmission of money or value, especially where such institution is susceptible to money laundering.[510] In an earlier section, this chapter demonstrated that cryptocurrency exchanges could

---

507 The issue of intent is discussed in more detail later in this chapter.

508 An organized criminal group is defined in article 2(a) UNCTOC as "a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit." See UNCTOC, *supra* note 34.

509 United States Department of Justice, Press Release, "Ross Ulbricht, The Creator and Owner of the "Silk Road" Website, Found Guilty in Manhattan Federal Court on All Counts" (February 5, 2015) U.S. Attorney's Office Southern District of New York, online: < https://www.justice.gov/usao-sdny/pr/ross-ulbricht-creator-and-owner-silk-road-website-found-guilty-manhattan-federal-court>.

510 UNCAC, article 14.

constitute financial institutions where they engage in financial activity commonly attributed to such institutions.[511] Given the analysis in this work on the nature of bitcoin and its function in enabling peer-to-peer financial transactions, this provision could act as authority for the creation of more detailed regulatory and supervisory provisions on cryptocurrencies. This is based on the understanding of bitcoin exchanges as constituting money transmission services.

Likewise, in the CFT Convention, the offence of money laundering is committed where a person "(1) […] *by any means*, 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" an offence defined in the CFT Convention (emphasis added).[512] In the context of cryptocurrencies, this provision would also enable the finding of an offence of money laundering. This is because the CFT convention requires that the provision or receipt of funds can occur by any means. Any means could therefore be interpreted to include provision of funds in the form of cryptocurrencies such as bitcoin.

5.5 Cryptocurrencies and International Cooperation Provisions in the AML Regime

To echo an assertion already made at different points in this work, the cross-border (or transnational) nature of the problem identified in this thesis reveals that international cooperation is essential for combatting transnational crimes such as money laundering. From a theoretic perspective, the new realism approach to international law and the role it plays in addressing society's problems guides this approach. By this reasoning, it is recognized that globalization affects both economic and cultural domains in society.[513]

---

511 This is especially so given the reference to financial activity in both the formal and informal sector in the FATF Recommendations.

512 Id, article 2(1) (a)-(b). The offence referred to in the CFT Convention includes an offence within the scope of any treaty annexed to the CFT Convention or the commission of an act with the intent that it causes serious bodily harm or death to a person not taking active part in armed hostilities.

513 Gregory Shaffer, "The New Legal Realist Approach to International Law" *supra* note 54 at 189. Three pillars of jurisprudence are identified by Brian Tamanaha as moral theorizing as in natural law, analytical jurisprudence as with legal positivism, and historical jurisprudence where law is assessed in relation to society. See Brian Z. Tamanaha, "The Third Pillar of Jurisprudence, *supra* note 248 at 2237.

More specifically, the opportunities and challenges that arise in the context of cryptocurrencies are not confined within domestic borders of individual states. Rather, they permeate domestic borders in much the same manner as the licit opportunities generated by globalization and technological advancements. Transnational crimes including money laundering frustrate any country attempting to combat them in isolation under its domestic laws.[514] These illicit activities are cross-border transcend in nature while the domestic laws designed to combat them are restricted to national boundaries pursuant to international law principles on state sovereignty. Recognition of state sovereignty in turn requires mutual respect for the territorial sovereignty of states. As a result, an international approach is essential to combatting transnational crimes.

5.5.1 Mutual Legal Assistance (MLA)

Chapter 3 highlights the importance of MLA for the effective investigation of transnational criminal cases. In the context of money laundering and its predicate crimes, a combination of scenarios may arise which result in challenges for domestic law enforcement. For instance, a predicate crime may take place in one jurisdiction while the laundering may take place in another.[515] In conducting their investigations or prosecuting the alleged trafficking, authorities of the initial country would be unable to trace the proceeds of the crime across their domestic border without the assistance of law enforcement of the other relevant countries.[516] Given the intrinsically transnational nature of cryptocurrencies, its use in the context of transnational crimes could lead

514 In the 'suppression conventions' referred to in chapter 1, states are obliged to assist one another in their efforts to supress the illicit activities which the conventions aim to curb. The UNCTOC and UNCAC both refer in their preambles to the importance of international cooperation among states on the relevant matters, as do most of the other international instruments. The FATF recommendations emphasize the importance of intensifying cooperation among domestic authorities in the fight against money laundering.

515 On a different but related topic, UNODC study on cybercrime finds that "between 50 and 100 per cent of cybercrime acts encountered by the police involve a transnational element." See United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, February 2013, online: <http://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf> at 117-118.

516 George J. Kriz, "International Co-operation to Combat Money Laundering" *supra* note 257 at 726. In chapter 4, I highlighted that success in apprehending the operators of Silk Road was the result of concerted effort by multiple law enforcement agencies working together on an ad-hoc basis. Just as with the AML regime, a standardized system of cooperation on this emerging form of money laundering is more efficient. See United States Department of Justice, Press Release, *supra* note 509.

to challenges for domestic law enforcement agencies seeking to trace the proceeds of crimes where cryptocurrencies are the medium for laundering.

In the instruments examined in Chapter 3, the emphasis in each text is on affording mutual legal assistance in investigations, prosecutions, and judicial proceedings in order to prevent gaps in the AML regime.[517] For an effective framework, the MLA provisions require implementation in a manner which reflect the rapid pace of cryptocurrency transactions.[518]

The UNCTOC includes detailed MLA provisions in articles 7(1)(b) and 18. First, article 7(1)(b) requires that domestic law enforcement receive proper training so as to permit it to engage in mutual cooperation and exchange of information with their counterparts.[519] Such cooperation could include information sharing on techniques and methods employed by launderers seeking to obfuscate the source of their funds using bitcoin or other cryptocurrencies. Article 18 of UNCTOC buttresses the requirements of 7(1)(b) by stressing the need for member states to afford the widest measure of MLA to each other. Article 18 lists the aims of such MLA which includes "identifying or tracing proceeds, property, instrumentalities or other things for evidentiary purposes".[520] Having demonstrated above that cryptocurrencies are assets and therefore property for the purpose of the AML instruments, this provision could enable MLA in identifying or tracing cryptocurrencies. Where cryptocurrencies are used in money laundering, MLA could possibly require law enforcement agencies to seek access to a bitcoin exchange's network or records. Such exchanges maintain records of their clients and thus could provide information on transactions especially the details of parties involved in a transaction. Adopting this approach may enable law enforcement to make the necessary links between illicit actors and the proceeds of crimes as evidence of money laundering. Contrary to the exchanges, it is also worth noting that for transactions on the Bitcoin network, transaction records on the public ledger (blockchain) does not

---

517 See article 7 of the Vienna Convention, articles 7&18 of the UNCTOC, and article 18 of the CFT Convention.

518 Growth of MLA treaties in the first place were spurred by the slow pace of Letters Rogatory. UNODC notes that an estimated 70% of international cooperation in the context of technology-facilitated crimes are conducted using traditional MLA which does not reflect the time-sensitive nature of the illicit activities. See United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, supra note 515 at 201.

519 The Vienna Convention and the UNCAC contain substantially similar terms to the UNCTOC. See the Vienna Convention, article 7, and the UNCAC article 14 and 46).

520 See specifically, article 18(3)(g) UNCTOC.

contain sufficient information to enable an assessment on illicit use.[521]Therefore, where any illicit activities occur on the Bitcoin network, it could complicate an already challenging investigatory process.

Article 18 UNCTOC also emphasizes that assistance would be required from another state (the requested state), "where the requesting State Party has reasonable grounds to suspect that the offence referred to in article 3, paragraph 1 (a) or (b), is transnational in nature, including that victims, witnesses, proceeds, instrumentalities or evidence of such offences are located in the requested State Party and that the offence involves an organized criminal group."[522] This provision would cover instances of suspected money laundering using cryptocurrencies involving exchanges that are domiciled outside the jurisdiction of the requesting country (thus making money laundering activity transnational in nature). A further provision considered useful in this regard is found in article 27(3) of the UNCTOC: "state parties shall endeavor to cooperate within their means to respond to transnational organized crime committed through the use of modern technology." Cryptocurrencies, though categorized as 'assets' in this work, also constitute a form of technology or digital asset. As such, this provision could prove useful in tracing proceeds of crime denominated in different forms of cryptocurrencies.

The provision on MLA in the FATF Recommendations requires countries to "provide the widest possible range of mutual legal assistance in relation to money laundering, associated predicate offences and terrorist financing investigations, prosecutions, and related proceedings."[523] On terrorist financing specifically, the Recommendations maintain that "countries should ensure that their competent authorities can *rapidly*, constructively and effectively provide the widest range of international cooperation in relation to money laundering, associated predicate offences and

---

521 The blockchain ledger though publicly available, significantly does not reveal the identities of parties to any transaction whose identities remain private while they transact using Bitcoin addresses. Rather is contains a timestamp of the transaction and the amount transacted.

Malcolm Campbell-Verduyn observes that in facilitating money laundering, cryptocurrencies have the potential to reverse the problem traditionally confronting AML efforts from "parties known – transaction unknown to transactions known – parties unknown." See Malcom Campbell-Verduyn, "Bitcoin, crypto-coins, and global anti-money laundering governance" *supra* note 466 at 287.

522 Article 18(1) UNCTOC.

523 See Recommendation 37 FATF.

terrorist financing" (emphasis added).[524] Along with the UNCTOC, the Recommendations also stipulates that countries should assist each other upon request and 'spontaneously' if needed.[525] In doing so, these provisions (UNCTOC and FATF) are important for expediting MLA in the context of cryptocurrencies. As pointed out in chapter 3, the MLA process is a very detailed formal process. In contrast, cryptocurrency transactions are relatively rapid and informal. Therefore, where an investigation into alleged money laundering using cryptocurrencies requires MLA, the above provisions could facilitate rapid assistance in obtaining evidence from a requested state. Supervisory and law enforcement agencies must be able to keep up with the fast pace of cryptocurrency transactions. Meeting this objective may require enforcement agencies to develop new monitoring and investigatory techniques together with revision of their MLA formalities.

The FATF and UNCTOC also place emphasis on the role of Financial Information Units (FIUs) with regards to the provision of MLA. Both instruments direct FIUs to engage in mutual information sharing and cooperation, and to facilitate the provision of MLA by the requisite law enforcement authorities.[526] In order to encourage information sharing and cooperation in the context of cryptocurrencies, Interpol has developed a Global Complex for Innovation (IGCI) in an attempt to propel law enforcement beyond a traditionally reactive model to a proactive model.[527] The IGCI's research builds technological capacity for police authorities around the world, equipping them with techniques and tools to combat the increasingly sophisticated techniques of criminals.[528] In doing this, it recognizes that law enforcement can only keep pace with criminals (or at least not fall too far behind) if they have access to real-time information within and beyond their own borders.[529] Using technology-based tools, Interpol's IGCI seeks to provide secure communication channels and immediate access to criminal information amongst law enforcement. An initiative of note is Interpol's development of a 'Darknet and Cryptocurrency Working Group' which brings together law enforcement officials to share challenges and techniques on cyber-

524 See FATF Recommendation 40. The provisions of CFT article 2 and 18 are substantially similar.
525 Id.
526 FATF Recommendation 40 Interpretive notes, paras. 7, 8, and 9; UNCTOC article 7(1)(b).
527 See Interpol, The Interpol Global Complex for Innovation, *supra* note 63.
528 Id.
529 Id.

related crime.[530] This working group first identified the use of cryptocurrency exchanges, mixers, and anonymization techniques as challenges faced in cryptocurrency investigations.[531]

5.5.2 Recovery of Assets

The ability to trace, confiscate and return the proceeds of crime – to recover assets – is essential for an effective AML regime. Tracing of assets is a crucial means of identifying the offender involved in laundering the illicit funds. [532] Experts note that the tracing and recovery process is often challenging, as the assets may have been mixed with other property, converted or otherwise disposed of, making it difficult to identify the proceeds of crime to be recovered. The problems associated with the recovery of assets is further complicated the funds in question are (as is typically the case with corrupt high-level public officials) hidden in foreign jurisdiction, thus triggering the need for MLA. [533]

The use of cryptocurrencies for conducting transactions further complicates the tracing process. While transactions on the Bitcoin network are publicly available on the blockchain, the network is designed so that the identity of the parties remains unknown. Additionally, cryptocurrency transactions are rapid and irreversible, causing more difficulties in the recovery of assets even where the identity of the illicit actors is eventually revealed. Furthermore, by purchasing cryptocurrencies using proceeds of crimes obtained in fiat currency, the recovery of assets constituting proceeds of crime becomes further complicated.[534] At present, it is unknown whether cryptographic technology allows for assets denominated in bitcoin to be frozen in a manner similar to funds held in bank accounts. Such functionality could somewhat neutralize the complexities of tracing funds dominated in cryptocurrencies.

---

530 Interpol, News: Interpol holds first DarkNet and Cryptocurrencies Working Group. April 3, 2018, online: <https://www.interpol.int/en/News-and-media/News/2018/N2018-022/>.

531 Id.

532 Daniel Adeoye Leslie, *supra* note 155 at 151.

533 Mark V. Vlasic & Gregory Cooper, "Recovery of Stolen Assets," *supra* note 263 at 2, online: <http://sk.sagepub.com/reference/download/transntlcrime-justice/n138.pdf>.

534 Identified successes highlighted in the previous chapter do not involve the technological component of cryptocurrency-facilitated laundering. See Mark V. Vlasic & Gregory Cooper, "Recovery of Stolen Assets" supra note 263 at 2.

The task of recovering cryptocurrency assets where they are used in money laundering is not insurmountable. Where bitcoin exchanges are used for illicit transactions (especially the ones with CDD procedure in place), overcoming the decentralized and therefore transnational of cryptocurrencies could be slightly less tasking. As is observed with Silk Road (bitcoin-based online merchant), in certain circumstances it may be possible to recover bitcoin assets despite bitcoin's decentralized nature. Bitcoin exchanges and merchants like Silk Road inadvertently centralize a typically decentralized mechanism, allowing AML officials recover bitcoin assets through the operators of merchants. With Silk Road, assets were recovered from Ross Ulbricht, despite the customers remaining largely unknown.[535] This would be the case where the bitcoin exchange is domiciled within a particular jurisdiction, having complied with the requisite registration formalities for its operations including information on its operators. As with banking regulations for traditional banks and other financial institutions, cryptocurrency exchanges would be required to submit to the regulatory oversight of the jurisdiction where it is registers. Though the consideration of domestic approaches to cryptocurrencies is beyond the scope of this thesis, the approach of the New York State Department of Financial Services (NYSDFS) serves as a useful example. The NYSDFS adopted (in effect October 8, 2015) regulations that require businesses intending to carry out virtual currency activities to obtain a license to do so (a BitLicense).[536] The NYSDFS regulations in turn provide oversight on the operations of such businesses. Doing so creates a paper trail that could enable supervisory and law enforcement agencies trace the assets of a cryptocurrency exchange. Relevant authorities could use MLA to facilitate the obtaining records of transactions from such exchanges.

AML instruments contain provisions on recovery of assets. Pursuant to those provisions, a request for recovery of assets can be made by one state (with jurisdiction over the crime) to another state

---

535 An estimated 174,000 Bitcoins (valued at $33 million at the time) were subject to seizure and confiscation from Ross Ulbricht.

536 See New York State Department of Financial Services, New York Codes, Rules, and Regulations, *Title 23 Department of Financial Services, Chapter 1 Regulations of the Superintendent of Financial Services, Part 200 Virtual Currencies* (2014), available at http://www.dfs.ny.gov/legal/regulations /adoptions/dfsp200t.pdf>.

See also Michael J. Casey, "NY Financial Regulator Lawsky Releases Final BitLicense Rules for Bitcoin Firms: Rules to Only Regulate Intermediaries with Custody of Customer Funds, not Software Developers" updated June 3, 2015, online: <https://www.wsj.com/articles/ny-financial-regulator-lawsky-releases-final-bitlicense-rules-for-bitcoin-firms-1433345396>.

(in whose jurisdiction the proceeds of crime are located.[537] Asset recovery provisions entail tracing, seizure or freezing of proceeds of crimes including assets that may have been converted or transformed from one type of asset to another.[538] Thus, conversion of assets from fiat to cryptocurrencies, or in fact from one form of cryptocurrency to another, should not place the assets beyond the reach of law enforcement.

In the UNCAC, a criminal conviction is not a prerequisite for recovery of assets. This provision is useful in certain circumstances where the criminal actor cannot be apprehended, such as where the corrupt official has passed away or has fled to a jurisdiction where extradition is not forthcoming.[539] By a similar analogy, it may be that where an illicit transaction is identified as such but the identity of the criminal actor is unobtainable, the assets may be seized. Given the 'pseudo-anonymous' nature of actors within cryptocurrency networks, this provision could prove useful where suspicious transactions have been flagged but the perpetrators have not yet been identified. If nothing else, confiscation in this scenario could inhibit the financial capacity required to for the recurrence of the predicate and postdicate crimes.

5.5.3 Jurisdiction and Extradition

The provisions of the AML instruments evaluated so far are also relevant in for the purpose of establishing jurisdiction over a money laundering offence where cryptocurrency is used. The AML provisions could also facilitate extradition of the alleged offender in this context. This is especially important as cryptocurrencies are still at a nascent stage. Given that cryptocurrencies are by their nature transnational, its use in the context of money laundering may require extradition of an alleged offender to stand trial.

---

537 Articles 4 and 5 of the Vienna Convention. See also articles 12 and 13 UNCTOC and article 51 UNCAC; CFT, article 8; Recommendation 34 FATF Recommendations. The instruments refer to serious crimes of a transnational nature (in the context of the Vienna convention, this provision is limited as predicate offences are limited to drug trafficking crimes.)

538 See article 12 and 13 UNCTOC.

539 UNCAC at article 54.

Cryptocurrency exchanges are in a position to choose which jurisdiction to operate from on the basis of which domestic laws are most 'favorable' for their business practices[540] For individuals with illicit intent, the rational choice theory suggests that the probability of those actors seeking out jurisdictions with relatively lax laws is high. Extradition is important in this context as the laws in those jurisdictions may not favor extradition if requested. Such differences in extradition laws may lead to certain countries becoming "crime havens" their laws are relatively lax.[541] This is a problem for extradition purposes as the principle of "double criminality" is generally required for extradition to take place.[542] Hence, the proprietor of a bitcoin marketplace or exchange could exploit lax domestic laws to evade criminal responsibility while operating a transnational cryptocurrency exchange.[543]

The respective international AML regime requires member states to ensure that the offences detailed in the AML instruments are criminalized within their domestic legislations.[544] This approach by the AML instruments is consistent with the notion of situational crime prevention. As a result, where the AML offences are criminalized across domestic jurisdictions, illicit actors are less likely exploit a domicile initially thought to be 'safe. [545] This approach could inhibit opportunities for bitcoin exchanges to exploit differences in domestic legislation. Accordingly, they are constrained from facilitating illicit transactions while remaining beyond the jurisdiction of an investigating domestic authority. Therefore, the potential offender conducts a rational choice

---

540 In choosing jurisdictions to operate, a bitcoin hedge fund based in Malta (Exante Ltd), offers its services to clients but according to its disclaimer, excludes any person from the United States from participating. It reportedly does so on the basis that "the U.S. jurisdiction is tricky", alluding to US securities registration requirements. See Jon Matonis, "First Bitcoin Hedge Fund Launches from Malta" FORBES (March 8 2013) online: <https://www.forbes.com/sites/jonmatonis/2013/03/08/first-bitcoin-hedge-fund-launches-from-malta/#404a78193e1e> (last accessed October 5, 2018).

541 Id. Reference to this is also contained in FATF recommendation 39.

542 Extradition is defined as "the formal rendition of a criminal fugitive from a state that has custody (the requested state) to the start which wishes either to prosecute or, if the fugitive has already been convicted of an offence, to impose a penal sentence (the requesting state). Double criminality requires that the conduct in question must be a criminal act in the requesting state as well as the requested state. See Robert J. Currie & Dr Joseph Rikhof, "Transnational Crimes of International Concern" in Robert J Currie & Dr Joseph Rikhof, *supra* note 72 at 478 and 424 respectively.

543 He could do this by fleeing upon investigations to a state that is unlikely to extradite him because his conduct is legal according to their laws

544 See Vienna Convention at article 4(1) and 4(2)(iii); UNCTOC articles 15 and 16; UNCAC articles 42(2), 42(5), 44(1) & (2); CFT Convention, article 7(2) and 9; FATF recommendation 39.

545 Ronald V. Clarke, "Situational Crime Prevention: Theory and Practice" *supra* note 58. Ronald V. Clarke, Situational Crime Prevention: Its Theoretical Basis and Practical Scope, *supra* note 58. See also Nicholas Gilmour, "Preventing money laundering" *supra* note 58. Nicholas Gilmour, "Understanding the practices behind money laundering" *supra* note 58.

assessment, possibly realizing that the option of money laundering using cryptocurrencies is no longer worthwhile.[546]

5.6 Challenges to Incorporating Cryptocurrency into the Exiting International AML Regime

5.6.1 Establishing the Requisite Intent

Dotted across the AML provisions above are indications that intent constitutes an important aspect of the offences contained therein. This calls into question the threshold of intent to be applied before a charge of money laundering can be levied in the context of cryptocurrencies.

The issue of the mental element in proving money laundering affects the effectiveness of the international AML regime.[547] The conventional format of international AML instruments is to prohibit offences and then stipulate the parameters for inferring intent (including circumstances for inferring intent). For instance, article 6(1) of the UNCTOC urges state parties to criminalize the laundering of proceeds of crime. This article then issues the proviso that such offence much have been committed intentionally i.e. alleged offender knows that the property or asset is derived from the commission of a criminal activity (the predicate or postdicate offence). Furthermore, in article 6(2)(f), the UNCTOC states that *'knowledge' may be inferred from "objective factual circumstances*"' (even in the absence of actual intent).[548] However, the need to fully observe general principles of criminality such as presumption of innocence and legal certainty often results in varied outcomes for the different jurisdictions when it comes to implementation.[549] Furthermore, obstacles to evidence production especially with tracing (discussed chapter 3 and earlier in this chapter), makes it challenging to establish the offence of money laundering within

546 Derek B. Cornish and Ronald V Clarke, Understanding Crime Displacement" *supra* note 59.

547 Leonardo Borlini, The Economics of Money Laundering" in Philip Reichel & Jay Albanese, Handbook of Transnational Crime and Justice (Thousand Oaks: Sage Publications, 2014) 227 at 236.

548 See for instance, UNCTOC article 6(2)(f). The import of this provision is examined further below in this section.

549 Id.

domestic courts. In particular, such difficulties manifest with regards to operators of the financial institutions used by the launderers who may claim ignorance of the illicit origin of the funds.[550]

It is left to the domestic courts to determine the parameters of the intent that are not explicitly addressed in the international AML instruments. For instance, to what extent can negligence or willful blindness be implied into the provisions on objective factual circumstances? In addition, how is the typical money laundering defense claim that the alleged offender was unaware of the illicit origins of the funds to be treated? If domestic courts are to determine this issue, how can the aspect of uniformity be achieved amongst state practice?

Generally, both domestic and international jurisdictions apply the principle of presumption of innocence. Pursuant to this principle, a prosecutor must prove that an alleged money launderer knew that the funds constitute the proceeds of crime. The launderer may be a financial professional who assists their client in completing a financial transfer. Where the client is an alleged criminal actor, the professional may knowingly or unknowingly aid the criminal actor in concealing the illicit source of their funds. The prosecutor in this instance is required to show that such an individual took steps to manipulate the funds in a manner that alters or disposes or otherwise deals with the property and that their intention is to conceal the illicit origin and ownership of the funds. That is, that the launderer (financial professional) intended that all illicit links to the funds be obscured. This complicates the task for the prosecutor. The addition of a new layer of complexity in the form of pseudo-anonymous transactions presents a further limitation in proving intent given the paucity of information required to carry out such transactions and the absence of applicable customer due diligence regulations.

This problem of establishing intent is dealt with in some domestic jurisdictions by permitting the inference of knowledge from factual circumstances. In Canadian criminal law, for instance, actual knowledge could be satisfied by the establishment of willful blindness. Hence, where the Canadian

---

550 See Daniel Adeoye Leslie, *supra* note 155 at 151.
Mark V. Vlasic & Gregory Cooper, "Recovery of Stolen Assets" supra note 263 at 2, online: <http://sk.sagepub.com/reference/download/transntlcrime-justice/n138.pdf>.

Criminal Code requires knowledge or belief as the *mens rea* for laundering proceeds of crime, willful blindness is deemed to satisfy the knowledge requirement for intent to conceal coupled with knowledge or belief of the illicit nature of the property.[551] In dealing with the principle of willful blindness, the Supreme Court of Canada, in *R v Briscoe*, held that "willful blindness can substitute for actual knowledge whenever knowledge is a component of the *mens rea*."[552] To buttress this point, the Court also noted that "the doctrine of willful blindness imputes knowledge to an accused whose suspicion is aroused to the point where he or she sees the need for further inquiries, but deliberately chooses not to make those inquiries."[553] The German Criminal Code also contains an offence of money laundering even where the individual dealing with the funds fails to recognize the illicit origin of the assets. In that instance, the offence of money laundering could be established on the basis of a high degree of negligence (leichtfertigkeit).[554] This approach appears to be aggressive given that it comes with the risk that persons performing everyday financial tasks may unwittingly become the subjects of money laundering investigations. The rationale of this provision, however, is to lessen the burden of proving knowledge by providing an alternative means for proving the subjective element of the crime. In the United Kingdom, the Proceeds of Crime Act 2002 requires "knowledge or suspicion" that the funds constitute the proceeds of crime.[555] In case law however, the UK House of Lords, in *Westminster City Council v Croyalgrange Ltd*, remarked that where a defendant deliberately averts his eyes from an obvious truth or "refrained from inquiry because he suspected the truth but did not want to have his suspicion confirmed" a finding of knowledge may be made pursuant to available evidence.[556] Pursuant to US law, the requirement for willful blindness is knowledge that the transaction is designed to conceal or disguise the proceeds of unlawful activity or knowledge that the transactions is designed to disguise or evade transaction reporting.[557] In *U.S. v Campbell*, the US Court of Appeal interprets this principle as an alternative approach for satisfying the requisite

---

551 See *Criminal Code*, RSC 1985, c C-46, s 462.31(1) ("Laundering the Proceeds of Crime"). See also *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* SC 2000, c. 17 (PCMLTFA) and associated Regulations.

552 R v Briscoe, 2010 SCC 13, [2010] 1 S.C.R. 411, at para 21.

553 *Id.*

554 Leonardo Borlini, The Economics of Money Laundering" supra note 547 at 238.

555 Proceeds of Crime Act 2002 (c.29) (POCA), s 340

556 Westminster City Council v Croyalgrange Ltd [1986] UKHL 9 at para 359.

557 See 18 U.S. Code § 1956 - Laundering of Monetary Instruments and 18 USC § 1956(c)(1).

mens rea, finding that if the actor purposely avoids clarification of the origin of the funds so that he can never be accused of subjective knowledge of the illicit nature of the funds, knowledge may be imputed.[558] The court in that case held that actual knowledge is satisfied if the prosecutors can show that the actor intentionally closed his or her eyes to the obvious and in doing so maintained willful blindness of the origin of the funds.[559] Given that the international AML instruments are implemented through domestic legislation, the above approach could be the basis for fulling the knowledge requirement for objective factual circumstances.

Furthermore, one view in existing literature is that in the absence of actual knowledge, intent could be established by "constructive intention" as opposed to "reckless knowledge". This view stresses that since money laundering is a conduct crime, its *mens rea* should refer to intention to perform the conduct.[560] From this, if an alleged launderer (the financial professional described above) in this instance is uncertain as to the origin of the funds but intends to and indeed proceeds to perform the conduct, then an offence of money laundering is established.

The alternative view is that for an offence of money laundering to be established, the offender must be certain of the illicit nature of the funds.[561] Given the difficulties in proving subjective intent in this context, my view is that the former perspective is consistent with the requirements set out in the international AML instruments. AML requirements in the form of CDD serve to put financial operators on notice. The CDD provisions also offer a means of avoiding culpability for money laundering. Consequently, where there are uncertainties surrounding the source of funds,

---

558 US v Campbell, 977 F.2d 854, 857 (4th Cir. 1992), paras 12-16, 24. In the case, the court examined the *mens rea* of a realtor engaging in a transaction with a drug dealer. While the drug dealer never told Campbell of the illicit nature of his work, the prosecution argued that she made concerted efforts to remain wilfully blind as the clues that should prompt her to perform due diligence were there. For instance, the drug dealer only drove luxury cars, paid for half of the purchase price in cash and put the property in his parents' name. Therefore, the drug dealer's actions spoke as loudly as any express statement. See Fletcher N. Baldwin, "The financing of terror in the age of the Internet: wilful blindness, greed or a political statement?" (2005) 8:2 Journal of Money Laundering Control 157 at 148-149. Pursuant to US law, the requirement is that the person conducting the financial transaction does know with knowledge that the property represents the proceeds of crime. This provision is explained as knowledge that the property involved proceeds from some form of criminal activity even though the individual may not know which specific form of criminal activity is involved. See 18 U.S. Code § 1956 - Laundering of Monetary Instruments and 18 USC § 1956(c)(1).

559 Id.

560 Leonardo Borlini, The Economics of Money Laundering" supra note 547 at 238. This is in keeping with the requirements of the UNCTOC article 6(2)(f) mentioned above.

561 *Id.*

this should trigger due diligence on the part of the financial professional in order to meet the burden placed on him by virtue of his position. As part of its mandate as Canada's financial intelligence unit, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) provides extensive guidance for individuals and entities on the compliance requirements as provided for in the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations.[562] FINTRAC notes that "establishing and implementing a comprehensive and effective compliance program is the basis for meeting all of your reporting, record keeping, client identification and know-your-client requirements under the PCMLTFA and associated Regulations."[563] This clarification is in keeping with the principle of willful blindness referred to above.

In a similar manner to the challenges with traditional money laundering, establishing intent in the context of money laundering using cryptocurrencies is likely to encounter problems. This is especially so, given that there is no express regulation of cryptocurrency networks and exchanges. For cryptocurrency transactions, only minimal information is disclosed on the blockchain ledger. Additionally, for transactions with a bitcoin exchange, for instance, the empirical studies evaluated for this thesis suggest that the information given by clients may not enable an exchange operator determine whether or not a suspicious transaction is taking place. This in turn highlights the significance of CDD procedure for exchange operators. It also suggests that the principle of willful blindness may be crucial for establishing liability of any exchanges that allegedly facilitate money laundering. Applying this principle could enable the courts draw inference from objective facts towards establishing *mens* rea. Furthermore, where the responsibility to comply with preventive CDD measures are applied to cryptocurrency exchange, such exchanges would be less likely to claim ignorance of suspicious transactions. Such responsibility could also be buttressed by supervisory guidance on the requirements of CDD for cryptocurrency exchanges. This could come in the form of the guidance provided by FINTRAC, as discussed in the previous paragraph. Where the cryptocurrency exchanges consequently fail to perform the requisite CDD, knowledge may be

562 FINTRAC was established by the PCMLTFA and acts as its administrative body.

563 FINTRAC, "Compliance program requirements under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations" online: <http://www.fintrac.gc.ca/guidance-directives/compliance-conformite/Guide4/4-eng.asp>.

imputed and willful blindness established pursuant to the international AML requirement of inferring intent or knowledge from objective factual circumstances.

5.6.2 Jurisdiction

The questions and challenges associated with jurisdiction are heightened by the involvement of cryptocurrencies. Jurisdictional principles recognize the sovereignty of states and the importance of mutual recognition, by states, of said sovereignty. Whereas cryptocurrencies are by their nature transnational, domestic authorities – on whom the burden of implementing and enforcing the requirements of the international AML regime rest – are limited by the boundaries of their domestic jurisdiction. For instance, where evidence of transnational money laundering using bitcoin is suspected, how could a domestic law enforcement authority exercise its jurisdiction to investigate or prosecute the crime? What would happen when the alleged illicit activity touches on the jurisdiction of more than one country?

If one country claims jurisdiction, the relevant authorities are likely to encounter jurisdictional challenges if the alleged offender or proceeds of crime are located outside their jurisdiction. These issues may be barriers to investigation and prosecution in the context of cryptocurrencies due to their nascent existence. For instance, where one country criminalizes its use or existence and another does not or even legalize its use, the different legislative approaches would be significant for obtaining assistance. At present the answer to these questions appears to lie in the cooperation provisions of the international AML regime, for instance through MLA and recovery of assets. MLA requires double criminality in order to extend the requisite assistance. However, state awareness or appreciation of the challenges posed by cryptocurrencies is at present varied, and ranges from outright prohibition of the use of cryptocurrencies to varying degrees of acceptance.[564]

564 Algeria, Bolivia, Morocco, Nepal, Pakistan, and Vietnam ban all activities involving cryptocurrencies. Canada permits the use of cryptocurrencies although it is not considered legal tender instead, a commodity. Spain, Belarus, the Cayman Islands, and Luxemburg see the potential in the cryptocurrency technology and are developing crypto-friendly regulations to attract investment in their technology sector. Venezuela, the Eastern Caribbean Central Bank (ECCB) member states, and Lithuania are attempting to develop their own system of cryptocurrencies. Belgium, South Africa, and the United Kingdom have issued public warnings on the pitfalls of investing in cryptocurrencies but at the same time determine that the size of the crypto-market is not sufficient to require regulation or ban. See Publication by The Law Library of Congress: Global Legal Research Directorate, Regulation of Cryptocurrency Around the World (June 2018) online: <http://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf>.

The diverse state positions is likely to impact the willingness of states to comply with a request for MLA (at least in the short-run) for a money laundering investigation where it has to do with cryptocurrencies. This is especially so, given that there is no international consensus at present on regulating cryptocurrencies.

While these challenges have an effect on the powers of law enforcement agencies with regards to cryptocurrency-assisted money laundering, the challenges inadvertently create a breeding ground for criminally-minded actors who capitalize on differences in domestic laws, globalization and the borderless nature of cryptocurrencies to advance their illicit purposes.[565]

5.6.3 Bitcoin exchanges, Mixers, and Anonymizers

Bitcoin exchanges, mixers and anonymizers constitute an added layer of difficulty for law enforcement. First, exchanges do not necessarily comply with AML instruments. Secondly, mixers and anonymizers facilitate anonymity of bitcoin transactions. International AML actors (UNODC and FATF amongst others) are finally starting to consider the role of cryptocurrencies in facilitating money laundering and other transnational crimes. However, it is also necessary to reflect on this component of cryptocurrency-based money laundering i.e. the use of exchanges, mixers, and anonymizers within the extant legislative instruments. One way of recognizing their role in money laundering could be to adopt the approach of the FATF in developing its Recommendations. In Chapter 3, this work explains that the initial Recommendations focused solely on money laundering and predicate transnational crimes. When money laundering was subsequently found to facilitate terrorist financing, the substantive Recommendations were modified accordingly. The Recommendations could therefore be further modified to recognize these emerging techniques of money laundering using cryptocurrency exchanges and other obfuscating tools.

565 While the question of how the principle of jurisdiction should be reconceptualized is beyond the scope of this work, suffice to observe that the initial recognition of sovereignty and jurisdiction (that states are the exclusive actors in international law) continues to be impacted by these developments i.e. globalization, technology, and the consequent rise of powerful non-state actors. See for instance Alex Mills, "Rethinking Jurisdiction in International Law" (2014) 84:1 British Yearbook of International Law 187.

5.6.4 Identifying Suspicious Transactions

Another limitation to bringing cryptocurrencies within existing AML rules concerns the implementation of CDD in order to investigate suspicious transactions. The challenge in this context has to do with recognizing suspicious transactions when they take place. This is because, the information revealed in the context of such transactions is minimal and may not be sufficient to enable law enforcement officials detects suspicious activity. Law enforcement officials now require specialist technological knowledge in order to keep up with methods and techniques of criminal activity facilitated by technology.[566] The operators of bitcoin exchanges may equally find themselves in the same situation of being legally required to identify suspicious uses of cryptocurrencies without a baseline knowledge of what such transactions look like. In such a situation, it may prove even more challenging for AML officials to establish that an apparently legitimate bitcoin operator has the requisite intent to facilitate an illicit transaction.

5.7 Conclusion

This chapter demonstrates some of the possible options for incorporating cryptocurrencies within the existing international AML regime. While this may not be the most effective approach, the suggestions constitute a potential starting point to achieve cohesive state response to an emerging technique for carrying out transnational crimes.

First, categorizing cryptocurrencies as assets demonstrates that their operations could fall under the extant AML provisions. The AML provisions referred to above criminalize the act of knowingly laundering property constituting the proceeds of crime. A determination that cryptocurrencies fall within the category of property means that the provisions of the AML regime could be interpreted as applicable to cryptocurrency-assisted money laundering.

Having clarified that the operations of the Bitcoin network and bitcoin exchanges are distinct, this chapter also argued that cryptocurrency exchanges could be considered informal institutions in the context of the AML provisions. This approach is significant for prevention, prosecution, and

566 Interpol is making efforts to assist law enforcement agencies in this regard as mentioned earlier in this chapter.

international cooperation in the context of cryptocurrency-facilitated money laundering. It is also important in the context of transnational crimes as due diligence measures, for instance, become applicable to the operation of bitcoin exchanges.

This approach is not without its challenges and obstacles. The challenges to the proposed interpretations become apparent in part due to the nascent nature of cryptocurrencies. For instance, the quasi-anonymous and decentralized nature of cryptocurrencies present problems of identifying offenders. The use of mixers and anonymizers obfuscate cryptocurrency transactions. In turn, they require that law enforcement authorities develop a great deal of technological expertise in order to identify illicit transactions and apprehend criminal actors. By obscuring cryptocurrency transactions, the mixers and anonymizers also raise related problems of obtaining evidence and apprehending offenders operating within, but domiciled beyond, the investigating jurisdiction. This is especially so where extradition may not be possible. Moreover, all these obstacles occur within the context of rapid financial transactions and technological evolution.

It may be that an interpretive approach as suggested in this chapter is a necessary first step towards AML regulation of cryptocurrencies. However, as cryptocurrencies grow and gain momentum (and existing literature suggests this is already happening), it would be more effective to expressly regulate them in an AML context. Adopting express AML provisions on cryptocurrencies could produce greater certainty on this subject. Such provisions could also provide law enforcement authorities with well-defined options when it comes to investigating and prosecuting suspected perpetrators. For instance, the express categorization (through legislation) of cryptocurrencies as assets, and exchanges as financial institutions, could eliminate any uncertainty with respect to the application of the AML regime to their operations. Doing so would also counteract the perception of exchanges, such as Bitstamp, that AML provisions as inapplicable to their operations.

So far, governments are at various stages of regulating cryptocurrencies from the standpoint of generating public revenue in the form of taxation. As the use of cryptocurrencies moves from a subculture phenomenon to a tangible alternative to mainstream financial institutions, it remains to be seen whether there is political will to also contemplate its use for money laundering. In the

meantime, focusing on bitcoin exchanges in the first instance could activate the existing AML provisions in the realm of cryptocurrency operations.

Chapter 6: Conclusion

6.1 Findings and Recommendation

Society constantly has to contend with new dimensions to transnational criminality. The arrival of new technologies has enabled criminal actors to modify their criminal techniques and given them another way through which to evade the reach of law enforcement. Transnational crime groups rely on various techniques for money laundering to obscure links between themselves and their illicit proceeds. In doing so, they are able to 'profit' from their crimes to continue in the cycle of illicit activity. The money laundering process also enables such criminal actors introduce illicit funds into mainstream society as well as the international financial system. Therefore, the role of money laundering in facilitating transnational crimes cannot be overstated. Heightened by factors such as corruption, globalization, technological advancements, loopholes in state sovereignty, and the third world dimension, transnational crime continues to evolve. As a consequence, societies are brought together and the reach of illicit markets are enlarged.

In presenting an overview of money laundering in the context of transnational crimes, chapter 2 demonstrates that the enormity of funds laundered across the globe has thus far eluded accurate quantification. This work also finds that empirical studies seeking to quantify the value of money laundering are limited by extensive lengths that money launderers would go to in order to ensure their activities remain undetected. Additionally, new schemes for placement, layering, and integrating illicit funds into the global financing system continue to emerge. Hence, the role of cryptocurrencies in facilitating money laundering and other transnational crimes is considered in this thesis.

The global Anti-Money Laundering (AML) regime has experienced some success in curtailing avenues for money laundering. The AML regime, though initially developed in response to drug trafficking, now demonstrates that the predicate crimes for money laundering exceed the parameters of drug trafficking as conceptualized by the United Nations Convention on United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances.[567]

567 Vienna Convention, *supra* note 38.

Thus, chapter 3 examined the present international AML regime on the basis of three thematic areas: prevention, prosecution, and international cooperation. To do this, it focused on the approaches of the Vienna Convention, United Nations Convention on Transnational Organized Crime (UNCTOC), United Nations Convention Against Corruption (UNCAC), the International Convention for the Suppression of the Financing of Terrorism (the CFT Convention), and the Financial Actions Task Force (FATF) Recommendations.[568]

Elements of the thematic areas identified are present in the AML instruments with different degrees of emphasis. In recognition of the import of technology in the context of transnational crimes, the UNCTOC, for instance, requires the training of law enforcement personnel on organized crime committed using modern forms of technology.[569] The AML instruments additionally recognize (to various degrees) that informal services are also used in facilitating money laundering.[570] The AML framework also emphasizes the responsibility of financial institutions as 'gatekeepers' of the international financial system, placing them at the forefront in the prevention of money laundering.[571] Financial institutions are required, for instance, to investigate customer identities, report suspicious transactions, and other relevant information to supervisory AML institutions within their jurisdictions. Furthermore, where financial institutions fail to comply with the AML provisions, sanctions are imposed accordingly. Thus, international law continues to move beyond the traditional range of actors in (mainly states), to administer rules that apply to the activities of non-state actors.

The provisions of the international AML regime also highlight the importance of international cooperation in combatting money laundering and transnational crimes. Mutual legal assistance and

---

568 Vienna Convention, supra note 38; UNCTOC, *supra* note 34. The UNCTOC enjoys relatively wide acceptance with 147 signatories and 189 ratifications. UNCAC, *supra* note 38. The UNCAC currently has 140 signatories and 186 ratifications. The CFT Convention, *supra* note 34; The FATF Recommendations, *supra* note 38. FATF membership comprises 37 countries, 2 regional institutions (European Commission and the Gulf Cooperation Council), 3 observer countries, associate members (regional organizations) and observer organisations (made up of various international and regional financial and security minded institutions such as African Development Banks, Basel Committee on Banking, and the International Monetary Fund (IMF). The level of involvement in the FATF by other established international institutions is a credit to its influence since from the time of its inception. FATF, "Members and Observers" online: < http://www.fatf-gafi.org/about/membersandobservers/>.

569 See UNCTOC article 29(1)(h).

570 See UNCAC, article 14; CFT Convention, article 18(2)(a) &(b); FATF r26-28.

571 See Bruce Zagaris, "Gatekeepers Initiative", *supra* note 471. Duncan E. Alford, "Anti-Money Laundering Regulations: A Burden on Financial Institutions" *supra* note 206 at 471.

information sharing amongst AML stakeholders, for instance, reveals a recognition that the phenomenon of money laundering and transnational crimes cannot be effectively addressed by a singular state. Such cooperation is even more essential with developments in Internet technology, globalization, transportation, and communication technology. These advances enable transactions and interactions that transcend domestic borders and consequently proliferate opportunities for transnational crime.

Emerging in the wake of the global economic downturn, cryptocurrencies continue to gain momentum in the face of skepticism from the mainstream financial sector (amongst others) and extreme volatility in terms of its value. In contemplating the emergence of cryptocurrencies and their growing popularity, this thesis determines that domestic authorities so far appear to contend with cryptocurrencies from the standpoint of generating public revenue than with its use for illicit purposes.

Cryptocurrencies offer some benefits to society. For instance, accessing the bitcoin network simply requires the use of an Internet-enabled device. However, the emergence of cryptocurrencies is also concerning with regards to its role in facilitating the laundering of proceeds of transnational crimes. Although attractiveness in this regard stems from the purported anonymity of cryptocurrencies, this thesis demonstrates that true anonymity does not exist within the bitcoin network. Owing to tools and techniques of 'deanonymization' identified by various empirical research efforts,[572] what exists can at best be considered 'pseudo-anonymity'.

However, opportunities remain within the bitcoin ecosystem for concealing user identities using bitcoin exchanges, mixers, and anonymizers (TOR).[573] These obscuring techniques may contribute to bitcoin's attractiveness for criminal actors. Although cryptocurrencies as a financial mechanism are in their relative infancy, actual incidents of money laundering using cryptocurrencies have been identified and such illicit use has the potential to grow if cryptocurrencies remain unregulated.

---

572 Sarah Meiklejohn et al, "A fistful of Bitcoins," *supra* note 382. Fergal Reid and Martin Harrigan, "An Analysis of Anonymity in the Bitcoin System" supra at note 410 at 15. Philip Koshy, Diana Koshy, and Patrick McDaniel, "An analysis of anonymity in Bitcoin using P2P network traffic" *supra* note 410.

573 Arvind Narayanan & Malte Möser, "Obfuscation in Bitcoin" *supra* note 425.

Empirical studies seeking to understand the potential of cryptocurrencies as a tool for money laundering remain somewhat speculative.[574] This is understandable given that the phenomenon of illicit use of cryptocurrencies is still incipient. It is also the case that due to the design of cryptocurrencies, identifying illicit use on the blockchain is impracticable. The public ledger (blockchain) contains minimal information concerning cryptocurrency transactions such as the time and the amount of the transaction. Such information does not reveal details that could enable identification of illicit transactions. The blockchain importantly does not record the identities of parties to a transaction.

In chapter 4, I determined that the distinction between the Bitcoin network and bitcoin exchanges is significant. In doing so, I established that the potential for money laundering is greater within the context of bitcoin exchanges than in the Bitcoin network. This is because bitcoin exchanges function as a type of intermediary between the Bitcoin network and customers, essentially operating as cryptocurrency-based financial institutions.[575] This suggests that regulating the operation of exchanges may be the first step towards inhibiting money laundering using cryptocurrencies. Bitcoin exchanges themselves already recognize the import of AML within their operations, as seen in self-regulatory efforts by cryptocurrency industry stakeholders including under the umbrella of the Digital Asset Transfer Authority (DATA). Similarly, the cryptocurrency exchange Bitstamp disclaims the applicability of AML initiatives while at the same time formulating its own AML policy. Chapter 4 also detailed the case of Silk Road, the bitcoin-based darknet merchant whose owner, Ross Ulbricht, was found guilty of facilitating money laundering and the perpetration of various transnational crimes. The Silk Road case is one of actual knowledge and admission by Ross Ulbricht of facilitating money laundering and other illicit activities through cryptocurrencies. Thus, the above considerations point to recognition within the cryptocurrency industry of the potential of cryptocurrencies for illicit use.

---

574 Perri Reynolds and Angela S.M. Irwin “Tracking Digital Footprints: anonymity within the bitcoin system” supra note 52. Angela S.M. Irwin, *et al*, "Are the financial transactions conducted inside virtual environments truly anonymous?” *supra* note 16.

575 An FATF policy research paper makes a similar finding. See FATF, *Guidance for a Risk-Based Approach to Virtual Currencies* (Paris: FATF, 2015), online: < http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>.

In exploring the potential for illicit use of cryptocurrencies, this thesis draws on certain criminological theories: environmental criminology, rational choice, routine activity; and the situational crime prevention (SCP) approach. The SCP approach adopts criminological theories such as those just mentioned towards formulating policies that disincentivize as well as thwart opportunities for money laundering. By arguing for the applicability of the existing AML regime to cryptocurrencies as a first step towards comprehensive regulation of cryptocurrencies, the approach of this thesis aligns with the SCP.

Having ascertained that cryptocurrencies have potential as a tool for facilitating transnational crimes, chapter 5 envisaged how cryptocurrencies could be brought within the existing international AML regime. In doing so, chapter 5 determined that the international AML regime definition of assets/funds which constitute the proceeds of crime is broad enough to extend to cryptocurrencies. Chapter 5 also demonstrated that the definition of financial institutions within these instruments is broad enough to apply to bitcoin exchanges.

Though not an express incorporation of cryptocurrencies into existing AML initiatives, this measured approach is appropriate given that the extent to which cryptocurrency facilitated money laundering occurs remains uncertain for the moment. Furthermore, it could be that the existing AML provisions are sufficient to tackle the instances where cryptocurrencies are used for laundering proceeds of transnational crimes without any need for express provisions. However, the suggested approach achieves the three thematic aims of AML identified in chapter 3. First, the AML responsibilities currently imposed on traditional banking and financial institutions would be extended to bitcoin exchanges. Adopting this approach would limit loopholes that enable cryptocurrency-assisted money laundering. For instance, should they be seen as falling under the authority of the international AML regime, bitcoin exchanges would be required to perform customer due diligence in facilitating financial transactions. Secondly, this approach could enable AML investigation and prosecution where money laundering using cryptocurrencies is alleged. Finally, in the context of international cooperation, law enforcement agencies would able to implement mutual legal assistance, if under the international AML regime, where cryptocurrencies are involved. Having demonstrated that cryptocurrencies such as bitcoin constitute assets within the definition of the AML instruments, such officials seeking to apprehend suspected launderers

or confiscate cryptocurrency assets used for illicit purposes, can rely on instruments providing for MLA, international cooperation in tracing and confiscation of proceeds of crime. For instance, Interpol's initiative in the context of cryptocurrencies (its Darknet and Cryptocurrencies working group) has created a platform for law enforcement cooperation in the context of cryptocurrencies.[576]

This method is consistent with the SCP approach in that it is aimed at disincentivizing the use of cryptocurrencies as a tool for money laundering and for facilitating transnational crimes. However, as demonstrated in chapter 5, there are challenges to this approach. First, the decentralized nature of cryptocurrencies and their pseudo-anonymous design compounds existing challenges in identifying and tracing illicit transactions. The nascent nature of cryptocurrencies also means that any efforts taken to overcome these challenges are somewhat speculative as cryptocurrencies continue to develop. Mixers and anonymizers are tools for obfuscating the identity of users. They continue to proliferate, adding to the existing complexity of cryptocurrencies. These tools present additional challenges with respect to obtaining evidence and apprehending offenders. Such additional challenges would be evident where cryptocurrencies and their associated tools are not the subject of regulation in the jurisdiction from which assistance is sought. Consequently, criminal actors are able to exploit the absence of regulation (or weak regulations) in some jurisdictions in order to avoid the reach of law enforcement in other (more robustly regulated) jurisdictions where they operate. This challenge is similar to that which necessitated international cooperation for transnational crimes, and could constitute a setback to many of the strides made so far in tackling money laundering. Challenges also emerge in satisfying requirements for knowledge requirements of the AML instruments. While the Silk Road case involved an admission of intention on the part of the marketplace's operators, this will not necessarily be the case with other cryptocurrency exchanges. That said, the challenge of meeting the knowledge requirements is somewhat minimized as the AML instruments provide for the inference of knowledge from objective

576 See 6(2)(f) of the UNCTOC.

circumstances.[577] Nevertheless, it may fall on the court in any given case to determine whether objective circumstances necessitate a finding that the knowledge requirement is satisfied.

As argued in this thesis, cryptocurrencies present a challenge to the existing international AML regime, and may inadvertently facilitate its circumvention. However, this work has demonstrated that careful interpretation of the existing international AML regime is a first step towards AML regulation of cryptocurrencies. In carrying out such an interpretation, this thesis demonstrates that the present AML regime is able to encompass cryptocurrencies. However, as cryptocurrencies go beyond a subculture phenomenon and achieve mainstream acceptance, express provisions such as a protocol to the UNCTOC or even a standalone international AML instrument are desirable for regulating cryptocurrencies in an AML context. Express provisions could produce greater certainty for AML stakeholders and create further options for enforcement authorities in the prevention, investigation, and prosecution of cryptocurrency-facilitated money laundering.

6.2 Limitations of Research

Certain components that could have otherwise enriched this emerging research area were not considered. For instance, this research could have been enriched by primary empirical studies involving interviews with cryptocurrency experts, operators, and users. Such studies could shed light on a number of issues including the perception of the frequency of money laundering within cryptocurrency ecosystems. With respect to bitcoin exchanges, it would be interesting to obtain the perspective of operators both concerning money laundering and whether the international AML regime should be applicable to their operations. Such insight would be meaningful especially so in light of Bitstamp's exclusion of AML from their operations.[578]

Although alluded to in some parts, a consideration of domestic approaches to cryptocurrency regulation was also not feasible as part of my research. However, by focusing on a select few instruments in the international AML regime, the findings of this research could be slightly limited.

---

577 See UNCTOC, article 6(2)(f).

578 Bitstamp, Bitstamp Limited Anti Money Laundering ("AML") and Counter Terrorist Financing ("CFT") Policy, *supra* note 353.

Nevertheless, in the course of researching this subject, I discovered that scholars are starting to contend with the domestic approach to cryptocurrency-facilitated money laundering.

6.3 Areas for Future Research

This thesis has demonstrated that cryptocurrencies continue to establish themselves to be more than a passing fad. In the course of this research, I have identified three areas that could benefit from further research. First, this work has identified that the cost of using cryptocurrencies may be affected by the implementation of AML policies in that context. Consequently, research adopting an economic analysis of law could shed light on the cost of cryptocurrency transactions and how such costs are determined. Doing so may necessitate an examination of the cost implications for traditional financial institutions in fulfilling their AML requirements. This could be a method for assessing the costs to cryptocurrencies where they are also required to do the same. Engaging in this research focus could also clarify factors that motivate cryptocurrency users to choose to conduct their financial transactions using this mechanism. The results could also help determine whether AML requirements would disincentivize criminally-minded users from utilizing cryptocurrencies.

Secondly, in the context of AML, the ability to freeze or confiscate assets that constitute the proceeds of crimes is an important part of the international AML instruments. At present, it is unknown whether cryptocurrency assets that constitute the proceeds of crimes can similarly be frozen or confiscated under the existing AML regime or domestic legislation. If it is not possible to confiscate cryptocurrency assets where they are used to facilitate money laundering. Within this context, then the reality of combatting cryptocurrency-facilitated money laundering becomes more theoretical. Existing research on the apprehension of the proceeds of crime demonstrates that in many instances, organized crime actors would rather serve a prison sentence than have their funds

confiscated.[579] This finding highlights the importance of seizing funds constituting the proceeds of crime as a means of curbing money laundering, including in the cryptocurrency context.

Further research that delves into state approaches to the regulation of cryptocurrencies is also necessary. While an international approach is identified as the pragmatic first step to addressing this problem pursuant to the new legal realism approach, it is also important to compare existing state practices. This is because current state practice on cryptocurrencies could determine their attitude towards further responsibility in this context. Understanding a state's stance with regards to cryptocurrencies (and its use for transnational crimes) could be significant for determining the extent to which any given state is willing to cooperate with others to combat cryptocurrency-facilitated money laundering. Furthermore, the instruments in the international AML regime are framed in a manner that places the responsibility on states to act in combatting money laundering. The aim of this approach is to ensure that no state becomes a safe haven for perpetrators of money laundering and its predicate/postdicate crimes.

6.4 Contributions to the Literature

This thesis is an important contribution to the emerging area of research on cryptocurrencies. The use of cryptocurrencies for illicit purposes has been identified as a problem by a number of scholars including Perri Reynolds and Angela Irwin, as well as Malcolm Campbell-Verduyn. Relying on a number of criminological theories, this thesis builds on the work of these scholars by demonstrating the importance of regulating cryptocurrencies while the problem of its illicit use is still at a nascent stage. This work also illustrates, through interpretation of the international AML regime, how cryptocurrencies could be brought within the application of the existing AML regime as it is. In doing so, it identifies a solution to the problem in its embryonic stage. Just as the existing AML regime recognizes the benefits of traditional financial benefits while seeking to curtail its

579 Katalin Ligeti and Michele Simonato, "Asset Recovery in the EU" *supra* note 268 at 1. This assumption is the subject of some contention. See for instance Criticism to such an assumption has been expressed, for example, by Hans Nelen, "Hit Them Where It Hurts Most?" *supra* note 268.

illicit use, so also will cryptocurrencies continue to serve its beneficial purposes while its drawbacks are curtailed pursuant to the AML framework.

Bibliography

Legislation

18 U.S.C. § 1956 - U.S. Code - Unannotated Title 18. Crimes and Criminal Procedure § 1956. *Laundering of monetary instruments.*

Criminal Code, RSC 1985, c C-46.

New York State Department of Financial Services, New York Codes, Rules, and Regulations, *Title 23 Department of Financial Services, Chapter 1 Regulations of the Superintendent of Financial Services, Part 200 Virtual Currencies* (2014), available at http://www.dfs.ny.gov/legal/regulations /adoptions/dfsp200t.pdf

Proceeds of Crime (Money Laundering) and Terrorist Financing Act SC 2000, *c. 17.*

Proceeds of Crime Act (UK) 2002.

Jurisprudence

R v Briscoe, 2010 SCC 13, [2010] 1 S.C.R. 411.

US v Campbell, 977 F.2d 854, 857 (4th Cir. 1992).

Westminster City Council v Croyalgrange Ltd [1986] UKHL 9.

Secondary Materials: Monographs

Beaudry, Jeffery S. and Lynne Miller, *Research Literacy: A Primer for Understanding and Using Research* (New York: Guilford Publications, 2016).

Black's Law Dictionary, 10th ed., *sub verbo "*Bank Secrecy."

Boon, Kristen E., Aziz Huq, and Douglas C. Lovelace, *Terrorism: Commentary on Security Documents* vol. 106 (Terrorist Financing and Money-laundering) (Oxford: Oxford University Press, 2010).

Bossard, Andre, *Transnational Crime and Criminal Law* (Chicago: University of Chicago, Office of International Criminal Justice, 1990).

Crawford, James, *Brownlie's Principles of Public International Law*, 8th ed. (Oxford: Oxford University Press, 2012).

Currie, Robert and Dr. Joseph Rikhof, *International and Transnational Criminal Law*, 2nd ed. (Toronto: Irwin Law, 2013).

Gates, Mark, *Blockchain: The Ultimate Guide to Understanding Blockchain, Bitcoin, Cryptocurrencies, Smart Contracts and the Future of Money* (2017).

Gayard, Laurent, *Darknet: Geopolitics and Uses* (Hoboken: John Wiley & Sons, 2018).

Gilmore, William C. ed., *Mutual Assistance in Criminal and Business Regulatory Matters* (New York: Cambridge University Press, 1995).

Hinterseer, Kris, *Criminal finance: The political economy of money laundering in a comparative legal context* (The Hague: Kluwer Law International, 2002).

Hopton, Doug, *Money Laundering: A concise Guide for all Businesses* (London: Gower, 2009).

Kahneman, Daniel, Paul Slovic, and Amos Tversky eds., *Judgment Under Uncertainty: heuristics and biases* (Cambridge: Cambridge University Press, 1982).

Leslie, Daniel Adeoye, *Legal Principles for Combatting Cyberlaundering* (Basel: Springer, 2014).

Perrin, Benjamin, *Social Media Crime in Canada: Annotated Criminal Code* (Ottawa: Canadian Bar Association Law for the Future Fund, 2017).

Reichel, Philip, ed. *Handbook of Transnational Crime & Justice* (Thousand Oaks: Sage Publishing, 2005).

Reuter, Peter and Edwin M. Truman, *Chasing Dirty Money: the Fight Against Money Laundering* (Washington DC: Institute for International Economics, 2004).

Richardson, Louise, *What Terrorists Want* (London: John Murray, 2006).

Shaw, Malcom, *International Law,* 6th ed. (Cambridge: Cambridge University Press, 2008).

Wortley, Richard and Lorraine Mazerolle, *Environmental Criminology and Crime Analysis* (London: Willan, 2008).

Secondary Materials: Articles and Edited Collections

Albanese, Jay, "Transnational Organized Crime," in Mangai Natarajan (ed.) *International Criminal Justice* (New York: Cambridge University Press, 2010) 231.

Alford, Duncan E., "Anti-Money Laundering Regulations: A Burden on Financial Institutions" (1994) 19:*3 N.C. J. Int'l L. & Com. Reg*. 437.

Allum, Felia and Stan Gilmour, “Introduction” in Felia Allum and Stan Gilmour (eds.) *Routledge Handbook of Transnational Organized Crime* (Oxon: Routledge, 2011).

Androulaki, Elli, Ghassan O. Karame, Marc Roeschlin, Tobias Scherer, Srdjan Capkun “Evaluating user privacy in bitcoin” in Ahmad-Reza Sadeghi. (ed.) *Financial Cryptography and Data Security FC 2013 Lecture Notes in Computer Science* Vol. 7859 (Berlin: Springer, 2013).

Angela S.M. Irwin and George Milad "The use of crypto-currencies in funding violent jihad"(2016) 19:4 *Journal of Money Laundering Control*, 407.

Arnone, Marco, & Leonardo Borlini, “International anti-money laundering programs: Empirical assessment and issues in criminal regulation" (2010) 13:3 *Journal of Money Laundering Control* 226.

Aust, Anthony, *Modern Treaty Law and Practice*, 3rd ed. (Cambridge: Cambridge University Press, 2013).

Baldwin, Fletcher N., "The financing of terror in the age of the Internet: wilful blindness, greed or a political statement?" (2005) 8:2 *Journal of Money Laundering Control* 157.

Barthe, Emmanuel P., "Situational Crime Prevention" in Kenneth J. Peak, *Encyclopedia of Community Policing and Problem Solving* (Thousand Oaks: SAGE Publications, 2013) 387.

Bassiouni, M. Cherif, "The Source and Content of International Criminal Law: A Theoretical Framework", in M. Cherif Bassiouni ed., *International Criminal Law Vol. I: Crimes* (2nd ed.) (New York: Transnational Publishers, 1999), 4.

Baur, Aaron W., Julian Bühler, Markus Bick & Charlotte S. Bonorden “Cryptocurrencies as a Disruption? Empirical Findings on User Adoption and Future Potential of Bitcoin and Co” in Marijn Janssen, et al, (eds.), *Open and Big Data Management and Innovation: 14th IFIP WG Conference on e-Business, e-Services, and e-Society*, I3E 2015, Delft, The Netherlands, October 13-15, 2015, Proceedings (Basel: Springer International Publishing) 63.

Beare, Margaret, “Responding to Transnational Organized Crime: Follow the Money” in Felia Allum & Stan Gilmour, eds., *Routledge Handbook of Transnational Organized Crime* (Abingdon: Routledge, 2011) 274.

Bjerg, Ole, “How is Bitcoin Money?” (2015) 33:1 *Theory, Culture & Society* 53.

Boister, Neil, “Further reflections on the concept of transnational criminal law” (2015) 6:1 *Transnational Legal Theory* 9.

Boister, Neil, “Human Rights Protections in the Suppression Conventions” (2002) 2:2 *Human Rights L Rev*, 199.

Boister, Neil, “Transnational Criminal Law?” (2003) 14:5 *EJIL* 953.

Borlini, Leonardo, The Economics of Money Laundering" in Philip Reichel & Jay Albanese, *Handbook of Transnational Crime and Justice* (Thousand Oaks: Sage Publications, 2014) 227.

Bower, Joseph L., and Clayton M. Christensen, “Disruptive Technologies: Catching the Wave” (1995) 73:1 *Harvard Business Review* 43

Brenig, Christian, Rafael Accorsi, Rafael & Günter Müller, "Economic Analysis of Cryptocurrency Backed Money Laundering" (2015) 20 ECIS Completed Research Papers, online: < https://aisel.aisnet.org/ecis2015_cr/20/>.

Bruinsma, Gerben J.N., Lieven J.R. Pauwels, Frank M. Weerman, Wim Bernasco, “Situational Action Theory: Cross-Sectional and Cross-Lagged Tests of Its Core Propositions” (2015) 57:*3 Canadian Journal of Criminology and Criminal Justice*, 363.

Brummer, Chris, “How International Financial Law Works (and How it Doesn’t)” 99 (2011) *Georgetown Law Journal* 257.

Campbell-Verduyn, Malcom, “Bitcoin, crypto-coins, and global anti-money laundering governance” (2018) 69 *Crime Law and Social Change* 283.

Clarke, Ronald V., ‘‘Technology, Criminology and Crime Science’’ (2004) 10 *European J Criminal Policy & Research* 55.

Clarke, Ronald V., “Situational Crime Prevention: Theory and Practice (1980) 20:2 *Brit J Crim.* 136.

Clarke, Ronald V., “Situational crime prevention” (1995) 19 *Crime and Justice* 91.

Clarke, Ronald V., and Derek B. Cornish. “Modelling Offenders' Decisions: A Framework for Research and Policy.” (1985) 6 *Crime and Justice*, 147.

Clarke, Ronald V., Situational Crime Prevention: Its Theoretical Basis and Practical Scope (1983) 4 *Crime and Justice* 225.

Clifford, William, “New dimensions in criminality: National and Transnational” (1975) 8:2 Australian and New Zealand Journal of Criminology 67.

Cohen, Lawrence E. and Marcus Felson. "Social Change and Crime Rate Trends: A Routine Activity Approach." (1979) 44:4 *American Sociological Review* 588.

Cornish Cornish, Derek B., and Ronald V. Clarke, “Understanding Crime Displacement: An Application of Rational Choice Theory” (1987) 25:4 *Criminology* 933.

Cornish, Derek B., "The procedural analysis of offending and its relevance for situational prevention" in Ronald V. Clarke (ed.) *Crime Prevention Studies* (Vol. 3) (Monsey: Criminal Justice Press, 1994).

Cornish, Derek B., and Ronald V. Clarke, "Analyzing Organized Crimes" in Alex R. Piquero & Stephen G. Tibbetts (eds.) *Rational Choice and Criminal Behavior: Recent Research and Future Challenges* (New York: Routledge, 2002).

Cuccuru, Pierluigi, "Beyond bitcoin: an early overview on smart contracts" (2017) 25 *International Journal of Law and Information Technology* 179.

David Lee Kuo Chuen (ed.) *Handbook of Digital Currency: bitcoin, innovation, financial instruments, and big data* (London: Academic Press, 2015).

De Filippi, Primavera, "Bitcoin: A Regulatory Nightmare to a Libertarian Dream" (2014) 3:2 *Internet Policy Review* online (pdf): <https://policyreview.info/node/286/pdf>.

Descoteaux, David, "Bitcoin: More Than a Currency: a Potential for Innovation" (2014) *Montreal Economic Institute* (Regulation Series: Economic Note) online (pdf): <http://www.iedm.org/sites/default/files/pub_files/note0114_en.pdf>.

Descôteaux, David, "How should Bitcoin be regulated?" (2014) *Montreal Economic Institute* (Regulation Series: Economic Note) online (pdf): <http://www.iedm.org/files/note0114_en.pdf>.

Dostov, Victor & Pavel Shust, "Cryptocurrencies: an unconventional challenge to the AML/CFT regulators?" (2014) 21:3 *Journal of Financial Crime* 249.

Doughty, Caroline, "Know your customer: Automation is key to comply with legislation" (2005) 22:4 *Business Information Review* 248.

Elliott, Samuel, "Bitcoin: The First Self-Regulating Currency?" (2018) 3, *LSE Law Review* 57.

Farah, Douglas, "Money Laundering and Bulk Cash smuggling: challenges for the Mérida Initiative" in *Working Paper Series on U.S.-Mexico Security Cooperation Woodrow Wilson Centre for International Scholars/Trans-Border Institute*, 2010.

FIjnaut, Cyrille "Transnational Crime and the Role of the United Nations in Its Containment through International Cooperation: A Challenge for the 21st Century" (2000) 8:2 *European Journal of Crime, Criminal Law and Criminal Justice* 119.

Friedrich, Carl J., "Political Pathology" (1966) 37(1) *The Political Quarterly* 70.

Friedrichs, David O., "Transnational Crime and Global Criminology: Definitional, Typological, and Contextual Conundrums." (2007) 34:2 *Social Justice* 4.

Gallagher, Anne T., *The International Law of Human Trafficking*, (ed.) (Cambridge: Cambridge University Press, 2010).

Gilmour, Nicholas, "Preventing money laundering: a test of situational crime prevention theory" (2016) 19:4 *J Money Laundering Control* 376.

Gilmour, Nicholas, "Understanding the practices behind money laundering: A rational choice interpretation" (2015) 44 *Intl JL Crime & Practice* 1.

Godlove, Nicholas, "Regulatory Overview of Virtual Currency" (2014) 10 *Oklahoma Journal of Law and Technology* 1.

Gross, Ralph and Alessandro Acquisti, "Information revelation and privacy in online social net- works" in *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, Alexandria, VA, 7-10 November 2005, 71-80, online (pdf): <https://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf>.

Gruber, Sarah, "Trust, Identity and Disclosure: Are Bitcoin Exchanges the Next Virtual Havens for Money Laundering and Tax Evasion (2013) 32 *Quinnipiac Law Review* 135.

Guex, Sebastien, "The Origins of the Swiss Banking Secrecy Law and its Repercussions for Swiss Federal Policy" (2000) 74:2 *The Business History Review* 237.

Hicks, David C., "Money Laundering: Vulnerable Commodities and Services" in Margaret E. Beare (ed.) *Encyclopedia of Transnational Crime & Justice* (Thousand Oaks: Sage Publications, 2012).

Hicks, David, & Adam Graycar "Money Laundering" in Mangai Natarajan, ed., *International Crime and Justice* (Cambridge: Cambridge University Press, 2010) 171.

Hileman, Garrick, and Michel Rauchs, "Global Cryptocurrency Benchmarking Study", *Cambridge Judge Business School [Cambridge Centre for Alternative Finance]*, University of Cambridge, online (pdf) <https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf>

Innes, Martin and Michael Levi, "Terrorism and Counter-Terrorism" in Rod Morgan, Mike Maguire & Robert Reiner (eds.) *The Oxford Handbook of Criminology*, 5th ed. (Oxford: Oxford University Press, 2012) at 665.

Irwin, Angela S.M., Jill Slay, Ki-Kwang Raymond Choo, and Lui Liu, "Are the financial transactions conducted inside virtual environments truly anonymous? An experimental research from an Australian perspective," (2013) 16:*1 J Money Laundering Control* 6.

Joyce, Elizabeth, "Expanding the International Regime on Money Laundering in Response to Transnational Organized Crime, Terrorism, and Corruption" in Philip Reichel (ed.) *Handbook of Transnational Crime & Justice* (Thousand Oaks: Sage Publishing, 2005) 79.

Klaveren, Jacob V., 'The Concept of Corruption' in Heidenheimer, Arnold J., et al, (eds.), *Political Corruption: A Handbook* (Transaction Publishers 1989) 25–6.

Koley, Tapomoy, "End of Duopoly in Credit Card Payment Scheme Industry" (2014) 4:1 *IOSR Journal of Economics and Finance* 67.

Koshy, Philip, Diana Koshy, and Patrick McDaniel, "An analysis of anonymity in Bitcoin using P2P network traffic" (2014) *Financial Cryptography and Data Security*, 469.

Kriz, George J., "International Co-operation to Combat Money Laundering: The Nature and Role of Mutual Legal Assistance Treaties" (1992) 18:2 *Commw. L. Bull.* 723.

Kte'pi, Bill, "Money Laundering: Methods" in Margaret E. Beare (ed.) *Encyclopedia of Transnational Crime & Justice* (Thousand Oaks: Sage Publications, 2012) 262.

Lee, Judith, Arthur Long, Marcellus McRae, Jeff Steiner, Stephanie Gosnell Handler, "Bitcoin Basics: A Primer on Virtual Currencies" (2015) 16:1 *Business Law International* 2.

Ligeti, Katalin and Michele Simonato, "Asset Recovery in the EU: Towards a Comprehensive Enforcement Model beyond Confiscation? An Introduction." in Katalin Ligeti and Michele Simonato (eds.) *Chasing Criminal Money: Challenges and Perspectives on Asset Recovery* (Oxford: Hart Publishing, 2017).

Maïga, Aïssata and Elizabeth Tompkins, "West Africa's New Drug of Choice: The Rise of Methamphetamine" (Stockholm: *Institute for Security and Development Policy*, June 12, 2014).

Maras, Marie-Helen, "Inside Darknet: the takedown of Silk Road" (2014) 98 *Centre for Crime and Justice Studies* 22.

Mills, Alex, "Rethinking Jurisdiction in International Law" (2014) 84:1 *British Yearbook of International Law* 187.

Möser, Malte, and Rainer Böhme, "The price of anonymity: empirical evidence from a market for Bitcoin anonymization" (2017) 3:2 Journal of Cybersecurity 127.

Mueller, Gerhart, "Transnational crime: Definitions and Concepts" in Philip Williams and Dmitri Vlassis, eds., *Combating Transnational Crime: Concepts, Activities, and Responses* (Abingdon: Frank Cass, 2001).

Narayanan, Arvind and Malte Möser, "Obfuscation in Bitcoin: Techniques and Politics" presented at the I*nternational Workshop on Obfuscation: Science, Technology, and Theory, New York University*, April 7-8, 2017, online (pdf): <https://arxiv.org/pdf/1706.05432.pdf>.

Narayanan, Arvind, "What Happened to the Crypto Dream? Part 1" (2013) 11:2 *IEEE Security & Privacy* 75.

Narayanan, Arvind, et al, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction* (New Jersey: Princeton University Press, 2016).

Naylor, Thomas R.T., "The International Anti-Money Laundering Regime: A Bankrupt Policy Desperate for a New Raison D'être" in Georgios Antonopoulos, et al (eds.), *Usual and Unusual Organising Criminals in Europe and Beyond: Profitable Crimes, from Underworld to Upperworld* (Antwerp: Maklu, 2011).

Nelen, Hans, "Hit Them Where It Hurts Most?" (2004) 41 *Crime, Law & Social Change* 517.

Nian, Lam Pak and David Lee Kuo Chen, "Introduction to Bitcoin" in David Lee Kuo Chuen (ed.), *Handbook of Digital Currencies: Bitcoin, Innovation, Financial Instruments, and Big Data* (London: Academic Press, 2015).

Nuth, Maryke Silalahi, "Taking Advantage of New Technologies: For and Against Crime", (2008) 24:5 *Computer L & Security Rev* 437.

Nye, Joseph S., 'Corruption and Political Development: A Cost-Benefit Analysis' (1967) 61 *American Political Science Review*, 419.

Pflaum, Isaac and Emmeline Hateley, "A bit of a problem: national and extraterritorial regulation of virtual currency in the age of financial disintermediation" (2014) 45:4 *Georgetown Journal of International Law*, 1169.

Plassaras, Nicholas, "Regulating digital currencies: Bringing Bitcoin within the reach of the IMF" (2013) 14:1 *Chicago Journal of International Law* 377.

Plouffe Jr., William C., "Transnational Crime: Defined" in Margaret E. Beare (ed.) (2012) *Encyclopedia of Transnational Crime & Justice* (Thousand Oaks: SAGE Publications Ltd, 2012).

Porter, Tony, "Technical Collaboration and Political Conflict in the Emerging Regime for International Financial Regulation" (2003) 10:3 *Review of International Political Economy* 520.

Reid, Fergal and Martin Harrigan, "An Analysis of Anonymity in the Bitcoin System" in Yaniv Altshuler, et al, (eds.) *Security and Privacy in Social Networks* (New York: Springer, 2013).

Reynolds, Perri and Angela S.M. Irwin "Tracking Digital Footprints: anonymity within the bitcoin system" (2017) 20:2 *Journal of Money Laundering Control* 172.

Rutherford, Donald, *Routledge Dictionary of Economics* (3rd ed.) (London: Routledge, 2013) sub verbo "assets".

Schneider, Stephen, "The Incorporation and Operation of Criminally Controlled Companies in Canada (2013) 7:2 *Journal of Money Laundering Control* 126.

Shaffer, Gregory, "New Legal Realism in International Law" in Heinz Klug, Elizabeth Mertz, & Sally Engle Merry (eds.) *Studying Law Globally: New Legal Realist Perspectives* Vol. II (Cambridge: Cambridge University Press, 2015).

Shaffer, Gregory, "The New Legal Realist Approach to International Law" (2015) 28:2 *Leiden J Intl L* (Symposium on New Legal Realism) 189, online: <https://ssrn.com/abstract=2605198>.

Shelley, Louise I. (ed.), *Dirty Entanglements: Corruption, Crime, and Terrorism* (Cambridge: Cambridge University Press, 2014).

Shelley, Louise I., "The Globalization of Crime," in Mangai Natarajan (ed.) *International Criminal Justice* (New York: Cambridge University Press, 2011).

Shelley, Louise I., and John T. Picarelli, "Methods and Motives: Exploring Links between Transnational Organized Crime and International Terrorism" (2005) 9:2 *Trends in Organized Crime* 52.

Stamp, John, and John Walker, "Money laundering in and through Australia" (2004) 342 *Trends & issues in crime and criminal justice* (Canberra: Australian Institute of Criminology) online: <https://aic.gov.au/publications/tandi/tandi342>.

Tamanaha, Brian Z., "The Third Pillar of Jurisprudence: Social Legal Theory," (2015) 56:6 *Wm. & Mary L. Rev*. 2235.

Tobin, James, "A Proposal for International Monetary Reform" (1978) 4:3-4 *Eastern Economic J* 153.

Vlasic, Mark V., and Gregory Cooper, "Recovery of Stolen Assets" in Margaret E. Beare (ed.), *Encyclopedia of Transnational Crime & Justice* (Thousand Oaks: SAGE, 2012) online (pdf): <http://sk.sagepub.com/reference/download/transntlcrime-justice/n138.pdf>.

von Lampe, Klaus, "The Practice of Transnational Organized Crime" in Felia Allum & Stan Gilmour (ed.) *Routledge Handbook of Transnational Organized Crime* (Oxon: Routledge) 186.

Walker, John, "Estimates of the extent of money laundering in and through Australia," for *Australian Transaction Reports and Analysis Centre*, (Queanbeyan: John Walker Consulting Services, 1995).

Walker, John, and Brigitte Unger, "Measuring Global Money Laundering: the Walker gravity model" (2009) 5 *Review of Law and Economics,* 821.

Walsh, Anthony and Craig Hemmens, *Introduction to Criminology: A Text/Reader*, 3rd ed. (Thousand Oaks: Sage, 2014).

Young, Ian, "Banks and Tax" in Sajid M. Chaudhry & Andrew W. Mullineux, eds., *Taxing Banks Fairly* (Cheltnam: Edward Elgar Publishing Limited, 2014) 90.

Zagaris, Bruce, "Gatekeepers Initiative: Seeking Middle Ground between Client and Government" (2002) 16 *Criminal Justice* 26.

Zagaris, Bruce, "Money Laundering and Counterterrorism Financial Enforcement" in Bruce Zagaris, *International White-Collar Crime: Cases and Materials*, ed. (Cambridge: Cambridge University Press, 2010) 56.

Zagaris, Bruce, "Transnational Organized Crime" in Bruce Zagaris, (ed.), *International White Collar Crime: Cases and Materials* (Cambridge: Cambridge University Press, 2010) 168.

Secondary Materials: International Law Documents

Council of Europe Directive 2005/60/EC, European Parliament and Council Directive on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.

Council of Europe, Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, May 16, 2005.

Council of Europe, Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, November 8, 1990.

Demirgüç-Kunt, Asli, Leora Klapper, Dorothe Singer, Saniya Ansar & Jake Hess, The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution (Washington DC: World Bank, 2017).

European Banking Authority, "EBA Opinion on 'Virtual Currencies'" (European Banking Authority: London, 2014) at para 46 online (pdf): <https://www.eba.europa.eu/documents/10180/657547/EBA-Op-201408+Opinion+on+Virtual+Currencies.pdf>. (last accessed 9 September 2018).

The European Union Agency for Law Enforcement Cooperation (Europol), Press Release,

"Money Laundering with Digital Currencies: Working Group Established" (9 September2016), online <https://www.europol.europa.eu/newsroom/news/money-laundering-digital-currencies-working-group-established09Sep2016>.

Europol, European Union Serious and Organised Crime Threat Assessment (SOCTA) (Hague: European Police Office, 2013).

Europol, The Internet Organised Crime Threat Assessment (iOCTA) (Hague: European Police Office, 2014).

Financial Action Task Force "Combatting the Abuse of Alternative Remittance Systems: International Best Practices," Special Recommendation VI (SR VI) (Paris, France: FATF/GAFI, 2003), online (pdf): <http://www.oecd.org/fatf/pdf/SR6-BPP_en.pdf>.

Financial Action Task Force, Press Release, "FATF Clarifies Risk-Based Approach: case by case not wholesale de-risking" October 23, 2014, online: < http://www.fatf-gafi.org/publications/?hf=10&b=0&s=desc(fatf_releasedate)>.

Financial Action Task Force Report, "Emerging Terrorist Financing Risks", online (pdf): <http://www.fatfgafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf>.

Financial Action Task Force, "What is Money Laundering? Basic Facts About Money Laundering", online: <http://www.fatf-gafi.org/MLaundering_en.htm>.

Financial Action Task Force, *FATF Report to G20 Finance Ministers and Central Bank* Governors (Paris: FATF, July 2018) available online: www.fatf-gafi.org/publications/fatfgeneral/documents/report-g20-fm-cbg-july-2018.html>.

Financial Action Task Force, FATF Report: Laundering the Proceeds of Corruption (Paris: FATF, 2011).

Financial Action Task Force, FATF Report: Virtual Currencies - Key Definitions and Potential AML/CFT Risks (Paris: FATF/OECD, June 2014), online: <http://www.fatf-gafi.org/topics/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html>.

Financial Action Task Force, FATF Report. Emerging Terrorist Financing Risks, (2015) online (pdf): <http://www.fatfgafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf>.

Financial Action Task Force, *Guidance for a Risk-Based Approach to Virtual Currencies* (Paris: FATF, 2015), online (pdf): <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>.

Financial Action Task Force, International Standards on Combatting Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations (Paris: FATF, 2012) online (pdf): <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>.

Information on the Law Enforcement, Organized Crime and Anti-Money-Laundering Unit of UNODC online (pdf): <https://www.unodc.org/documents/money-laundering/GPML-Mandate.pdf>.

International Convention Against the Taking of Hostages, New York, 17 December 1979, 1316 UNTS 205.

International Convention for the Suppression of the Financing of Terrorism 9 December 1999, 2178 UNTS at 197 (entered into force 10 April 2002).

International Monetary Fund, Factsheet: The IMF and the Fight Against Money Laundering and the Financing of Terrorism (2018) online: <http://www.imf.org/en/About/Factsheets/Sheets/2016/08/01/16/31/Fight-Against-Money-Laundering-the-Financing-of-Terrorism>.

Kristina M. Gjerde *et al*, *Regulatory and Governance Gaps in the International Regime for the Conservation and Sustainable Use of Marine Biodiversity in Areas beyond National Jurisdiction* (Gland: IUCN, 2008), online (pdf): <https://portals.iucn.org/library/sites/library/files/documents/EPLP-MS-1.pdf>.

Paul Alan Schott, Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism (World Bank Publications, 2006), online: <https://elibrary.worldbank.org/doi/abs/10.1596/978-0-8213-6513-7>.

Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition, supplementing the United Nations Convention against Transnational Organized Crime 31 May 2001, 2326 at UNTS 208 (entered into force 3 July 2005)

Protocol against the Smuggling of Migrants by Land, Sea and Air, supplementing the United Nations Convention against Transnational Organized Crime 15 November 2000, 2241 UNTS at 480 (entered into force on 28 January 2004)

Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the UNCTOC 15 November 2000, 2237 UNTS at 319 (entered into force on 28 January 2004).

Rome Statute of the International Criminal Court, UN Doc. A/CONF. 183/9.

The Commonwealth, Commonwealth Working Group on Virtual Currencies: Working Group Report (London: Commonwealth, 2015).

The International Convention for the Suppression of the Financing of Terrorism, 9 December 1999, 2178 UNTS 197.

UN Security Council Resolution 1373 adopted by the Security Council at its 4385th meeting, on 28 September 2001 (S/RES/1373 (2001).

United Nations Convention Against Corruption, 31 October 2003, 2225 UNTS 209 (entered into force 29 September 2003 [UNCAC].

United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (20 December 1988), 1582 UNTS 95; in force 11 November 1990.

United Nations Convention Against Transnational Organised Crime and its Protocols thereto, 15 November 2000, 2225 UNTS 209 (entered into force 29 September 2003) [UNCTOC].

United Nations Economic and Social Council Commission on Crime Prevention and Criminal Justice, "World Crime Trends and Emerging Issues and Responses in the Field of Crime Prevention and Criminal Justice" Twenty-sixth Session Vienna, 22-26 May 2017, at 14; online (pdf): <https://www.unodc.org/documents/data-and-analysis/statistics/crime/ccpj/World_crime_trends_emerging_issues_E.pdf> accessed November 10, 2018.

United Nations Economic Commission for Africa, Draft Report on Blockchain Technology in Africa (2017), online (pdf): <https://www.uneca.org/sites/default/files/images/blockchain_technology_in_africa_draft_report_19-nov-2017-final_edited.pdf>.

United Nations Office on Drugs and Crime, "World Drug Report 2005, accessed September 27, 2018, <http://www.unodc.org/pdf/ WDR_2005/volume_1_web.pdf>.

United Nations Office on Drugs and Crime, "World Drug Report 2017" online (pdf): https://www.unodc.org/wdr2017/field/Booklet_1_EXSUM.pdf>.

United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, February 2013, online (pdf): <http://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf>.

United Nations Office on Drugs and Crime, Drug Money: The Illicit Proceeds of Opiates Trafficked on the Balkan Route (Vienna: United Nations Office on Drugs and Crime, 2015) online (pdf): <http://www.unodc.org/documents/data-and-analysis/Studies/IFF_report_2015_final_web.pdf>.

United Nations Office on Drugs and Crime, Legislative Guides for the Implementation of the United Nations Convention Against Transnational Organized Crime and the Protocols Thereto (New York: United Nations, 2004).

United Nations Office on Drugs and Crime, The Globalization of Crime: A Transnational Organized Crime Threat Assessment (Vienna: UNODC, 2010).

United Nations Office on Drugs and Crime, Transnational Organized Crime in West Africa: A Threat Assessment (Vienna: UNODC, 2013) online (pdf): http://www.unodc.org/documents/data-and-analysis/tocta/West_Africa_TOCTA_2013_EN.pdf.

United Nations Office on Drugs and Crime, Travaux Préparatoires of the Negotiations for the Elaboration of the United Nations Convention Against Transnational Organized Crime and the Protocols Thereto United Nations Office on Drugs and Crime. (New York: United Nations, 2006).

United Nations Security Council (UNSC) Resolution 1373 (2001) Adopted by the Security Council at its 4385th meeting, on 28 September (2001 S/RES/1373 (2001)).

World Bank, Global Financial Development Report 2014, (Washington: World Bank, 2014).

Secondary Materials: Online Sources

Asian Development Bank, Anticorruption: Our Framework and Strategies, 1998, online: <http://www.adb.org/documents/anticorruption-policy>.

Baker, Raymond, John Christensen, and Nicholas Shaxson, "Catching Up with Corruption," The American Interest (September/October 2008), http://www.the-american-interest.com/article-bd.cfm?piece=466>.

Bambrough, Billy, "Binance CEO Predicts A Bitcoin and Crypto 'Bull Run'" Forbes November 12, 2018, online: <https://www.forbes.com/sites/billybambrough/2018/11/12/binance-ceo-predicts-a-bitcoin-and-crypto-bull-run/#67e6a0a63921>.

Bitcoin.org

Bitstamp, "Bitstamp Limited Anti Money Laundering ("AML") and Counter Terrorist Financing ("CTF") Policy" online: < https://www.bitstamp.net/aml-policy/>.

Blockchain, online: <https://www.blockchain.com/en/charts/total-bitcoins>.

Breslow, Jason M., "The Staggering Death Toll of Mexico's Drug War," FRONTLINE, July 27, 2015, <https://www.pbs.org/wgbh/frontline/article/the-staggering-death-toll-of-mexicos-drug-war/>.

Brown, Aaron, “Bitcoin Billionaires May Have Found a Way to Cash Out” Bloomberg (December 21, 2017) online: <https://www.bloomberg.com/view/articles/2017-12-21/bitcoin-billionaires-may-have-found-a-way-to-cash-out#footnote-1513870741754>.

Buck, John, “Julian Assange Urges Donors to Use Cryptocurrencies, Thwart Government” Coin Telegraph (December 20, 2017) online: <https://cointelegraph.com/news/julian-assange-urges-donors-to-use-cryptocurrencies-thwart-government>.

Casey, Michael J., “NY Financial Regulator Lawsky Releases Final BitLicense Rules for Bitcoin Firms: Rules to Only Regulate Intermediaries with Custody of Customer Funds, not Software Developers” updated June 3, 2015, online: <https://www.wsj.com/articles/ny-financial-regulator-lawsky-releases-final-bitlicense-rules-for-bitcoin-firms-1433345396>.

CBC News, “World’s first bitcoin ATM opens in Vancouver” October 29, 2013, online: < https://www.cbc.ca/news/technology/world-s-first-bitcoin-atm-opens-in-vancouver-1.2286877>.

Centre for Strategic and International Studies, Net Losses: Estimating the Global Cost of Cybercrime: Economic Impact of Cybercrime II (Washington, DC, 2014) online (pdf): <http://www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf>.

Chanjaroen, Chanyaporn, Andrea Tan & Haslinda Amin, “Singapore Won't Regulate Cryptocurrencies, Central Bank Chief Says” (24 October 2017) Bloomberg (blog), online: <https://www.bloomberg.com/news/articles/2017-10-24/singapore-won-t-regulate-cryptocurrencies-remains-alert-to-risk>.

Chavez-Dreyfuss, Gertrude, “Bitcoin hits another record high in march towards $20,000” (December 12 2017) Reuters, online <https://www.reuters.com/article/uk-markets-bitcoin/bitcoin-hits-another-record-high-in-march-towards-20000-idUSKBN1E60PE>.

Chohan, Usman W., ‘The Double-Spending Problem and Cryptocurrencies’ (2017) University of NSW Discussion Papers Series, online: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3090174>.

Church, Zach, “Blockchain Explained: An MIT Expert on Why Distributed Ledgers and Cryptocurrencies Have the Potential to Affect Every Industry” (25 May 2017), MIT Sloan School of Management, online <http://mitsloan.mit.edu/newsroom/articles/blockchain-explained/>.

CoinMarketCap, “Top 100 Cryptocurrencies by Market Capitalization” online: <https://coinmarketcap.com>, last visited March 11 2019.

Cuthbertson, Anthony and Andrew Griffin, “Bitcoin Price - Latest Updates: Cryptocurrency Recovers from Eight-Month Low”, The Independent (6 July 2018) online:

<https://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-price-live-updates-latest-value-exchange-rate-digital-cryptocurrency-futures-investment-a8203081.html>.

DATA, Anti-Money Laundering Guidelines (2014), online: <http://datauthority.org/blog/2015/07/01/global-aml-kyc-guidelines-data/>.

Davis, Joshua, "The crypto-currency", The New Yorker, October 10 2011.

The Egmont Group, Revised Statement of Purpose (June 23, 2004), <http://www.egmontgroup.org/>.

Ek, Veronica, and Johan Carlstrom, 'Bitcoin turns into art as Sweden rejects creative currency', Bloomberg, 23 January 2014.

Ethereum.org

Faife, Colin, "Live Free or Mine: How Libertarians Fell in Love with Bitcoin" (10 October 2016) Coindesk (blog), online: <https://www.coindesk.com/live-free-or-mine-how-libertarians-fell-in-love-with-bitcoin/>

Fedotov, Yury, "In Just Two Decades, Technology Has Become a Cornerstone of Criminality (23 October 2017), The Huffington Post (blog) online <http://www.unodc.org/unodc/en/frontpage/2017/October/in-just-two-decades--technology-has-become-a-cornerstone-of-criminality.html>

FINTRAC, "Compliance program requirements under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations" online: <http://www.fintrac.gc.ca/guidance-directives/compliance-conformite/Guide4/4-eng.asp>.

Frank Etto, "Know Your Coins: Public vs. Private Cryptocurrencies" September 22, 2017 Nasdaq online: <https://www.nasdaq.com/article/know-your-coins-public-vs-private-cryptocurrencies-cm849588>.

George-Cosh, David, "Canada says Bitcoin isn't legal tender" Wall Street Journal, 16 January 2014.

German, Peter M., An Independent Review of Money Laundering in Lower Mainland Casinos Conducted for the Attorney General of British Colombia (2018), online: <https://news.gov.bc.ca/files/German_Gaming_Final_Report.pdf>.

Globalization.org, online: < http://www.globalization.org/ What_is_Globalization.html>.

Hanning, James and David Connet, "London is now the global money-laundering centre for the drug trade, says crime expert" July 4, 2015 Independent, online:

<https://www.independent.co.uk/news/uk/crime/london-is-now-the-global-money-laundering-centre-for-the-drug-trade-says-crime-expert-10366262.html>.

https://z.cash

Interpol "International Global Complex for Innovation" online: <https://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation>.

Interpol, Press Release, "Project to Prevent Criminal Use of Blockchain Technology Launched by International Consortium" (24 May 2017) INTERPOL, online: <https://www.interpol.int/News-and-media/News/2017/N2017-069>.

Interpol, "INTERPOL holds first DarkNet and Cryptocurrencies Working Group: Altcoins identified as serious law enforcement challenge" April 3, 2018, online: <https://www.interpol.int/en/News-and-media/News/2018/N2018-022>.

Joffe-Block, Jude, "Banamex USA Bank to Pay $140 Million Fine and Shut Down," KJZZ (July 23, 2015), http://kjzz.org/content/169775/banamex-usa-bank- pay-140-million-fine-and-shut-down.>.

Kharif, Olga, "Bitcoin's Use in Commerce Keeps Falling Even as Volatility Eases" August 1, 2018, Bloomberg, online: <https://www.bloomberg.com/news/articles/2018-08-01/bitcoin-s-use-in-commerce-keeps-falling-even-as-volatility-eases?srnd=cryptocurriences>.

Kollewe, Julia, "Bitcoin: UK and EU Plan Crackdown Amid Crime and Tax Evasion Fears" (4 December 2017), The Guardian, Online <https://www.theguardian.com/technology/2017/dec/04/bitcoin-uk-eu-plan-cryptocurrency-price-traders-anonymity>.

Leal, Roman, "Is Bitcoin the Future of Payments?" (2014) 21 Goldman Sachs Global Investment Research Paper 18.

Litecoin.com

Luther, William J. and Lawrence H. White, "Can Bitcoin Become a Major Currency?" (5 June 2014), GMU Working Paper in Economics No. 14-17, Available at SSRN, online <https://ssrn.com/abstract=2446604>.

Matonis, Jon, "First Bitcoin Hedge Fund Launches from Malta" FORBES (March 8 2013) online: <https://www.forbes.com/sites/jonmatonis/2013/03/08/first-bitcoin-hedge-fund-launches-from-malta/#404a78193e1e> (last accessed October 5, 2018).

Matonis, Jon, "WikiLeaks bypasses financial blockade with bitcoin." http://www.forbes.com/sites/jonmatonis/2012/08/20/wikileaks-bypasses-financial-blockade-with-bitcoin/> Forbes. Accessed 20 Aug 2018.

McElroy, Justin, "B.C. to ask Ottawa for more tools to fight money laundering" CBC News Mar 26, 2018 online: <http://www.cbc.ca/news/canada/british-columbia/bc-ottawa-eby-trip-march-2018-1.4593444>.

McGuire, Mike, and Samantha Dowling, Cybercrime: A review of the evidence Research Report 7 (2013) (UK: Home Office, 2013).

Meek, Jessica, "Bitcoin regulation challenges and complexities. Operational Risk & Regulation" (2014) risk.net online: <http://www.risk.net/operational-risk-andregulation/feature/2328022/bitcoin-regulation-challenges-and-complexities>.

Meiklejohn, Sarah, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoyy, Geoffrey M. Voelker & Stefan Savage "A fistful of Bitcoins: characterizing payments among men with no names" (2013), IMC, online: https://cseweb.ucsd.edu/_smeiklejohn/files/imc13.pdf> (accessed August 23 2018).

Monero.org

Ozsoy, Tugce and Jeremy Herron, "Bitcoin Rebounds to Surpass $16,000 as Five-Day Selloff Ends" Bloomberg (December 26, 2017) online: <https://www.bloomberg.com/news/articles/2017-12-26/is-bitcoin-back-cryptocurrency-passes-15-000-as-rebound-begins>.

Pohjanpalo, Kati, "Bitcoin judged commodity in Finland after failing money test", Bloomberg, 20 January 2014 online: <https://www.bloomberg.com/news/articles/2014-01-19/bitcoin-becomes-commodity-in-finland-after-failing-currency-test>.

Press Release, Citigroup, Citigroup Statement on Banamex USA (July 22, 2015), online: <http://www.citigroup.com/citi/news/2015/150722a.htm.>.

Reinares, Fernando and Carlos Resa. "Transnational organized crime as an increasing threat to the national security of democratic regimes: assessing political impacts and evaluating state responses." (1999) NATO online (pdf): <http://www. nato.int/acad/fellow/97-99/reinares.pdf>.

Russollilo, Steven, "Bitcoin Goes to the Big Four: PwC Accepts First Digital-Currency Payment" (30 November 2017), The Wall Street Journal, online <https://www.wsj.com/articles/pricewaterhousecoopers-accepts-fee-in-bitcoin-1512036992>.

Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2012) Bitcoin.org online (pdf): <https://bitcoin.org/bitcoin.pdf

Securities and Exchange Commission, “Self-Regulatory Organizations; Cboe BZX Exchange, Inc.; Notice of Filing of Proposed Rule Change to List and Trade Shares of SolidX Bitcoin Shares Issued by the VanEck SolidX Bitcoin Trust” June 26, 2018, online: <https://www.sec.gov/rules/sro/cboebzx/2018/34-83520.pdf>.

Tasca, Paolo, “Digital Currencies: Principles, Trends, Opportunities, and Risks” (7 September 2015) Social Sciences Research Network (SSRN), online <https://ssrn.com/abstract=2657598>.

The Law Library of Congress: Global Legal Research Directorate, Regulation of Cryptocurrency Around the World (June 2018) online (pdf): <http://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf>.

The United States Attorney’s Office Southern District of New York, Press Release, “Liberty Reserve Founder Arthur Budovsky Sentenced in Manhattan Federal Court To 20 Years for Laundering Hundreds of Millions of Dollars Through His Global Digital Currency Business” (9 May 2016), The U.S. Attorney’s Office Southern District of New York, online: <https://www.justice.gov/usao-sdny/pr/liberty-reserve-founder-arthur-budovsky-sentenced-manhattan-federal-court-20-years>.

Transparency International, “Frequently Asked Questions About Corruption” Retrieved June 30, 2018, from <www.transparency.org/news_room/faq/corruption_faq#faqcorr1>

U.S. General Accounting Office (GAO), Terrorist Financing: U.S. Agencies Should Systematically Assess Terrorists' Use of Alternative Financing Mechanisms (Washington, DC: U.S. GAO, 2003) at 19, online (pdf): <http://www.gao.gov/new.items/d04163.pdf>.

United Kingdom Home Office, “UK National Risk Assessment of Money Laundering and Terrorist Financing: Policy Paper” (October 2015) GOV>UK, online (pdf): <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/655198/National_risk_assessment_of_money_laundering_and_terrorist_financing_2017_pdf_web.pdf>.

United States Department of Justice, Press Release, “Ross Ulbricht, The Creator and Owner of the “Silk Road” Website, Found Guilty in Manhattan Federal Court on All Counts” U.S. Attorney’s Office Southern District of New York (February 5, 2015) online: <https://www.justice.gov/usao-sdny/pr/ross-ulbricht-creator-and-owner-silk-road-website-found-guilty-manhattan-federal-court>.

United States v Ross William Ulbricht, Superseding Indictment, In the United States District Court for the District of Maryland, October 1, 2013, online (pdf): <https://www.ice.gov/doclib/news/releases/2013/131002baltimore.pdf>.

Vallentyne, Peter and Bas van der Vossen, "Libertarianism" in Edward N. Zalta, ed., *The Stanford Encyclopedia of Philosophy* (Fall 2014 Edition), online: <https://plato.stanford.edu/archives/fall2014/entries/libertarianism/>

Velde, François R., "Bitcoin: A primer" (2013) 317 *Federal Reserve Bank of Chicago Essays on Issues*, online: <https://www.chicagofed.org/publications/chicago-fed-letter/2013/december-317>.

Volcker, Paul A., Richard J. Goldstone, & Pieth, "Manipulation of the Oil-For-Food Programme by the Iraqi Regime Oil Transactions and Illicit Payments Humanitarian Goods Transactions and Illicit Payments The Escrow Bank and the Inspection Companies Other UN-Related Issues" (Independent Inquiry Committee into the United Nations Oil-For-Food Programme, October 27, 2005) www.iic-offp.org (website not found) but document obtained online (pdf): <https://www.files.ethz.ch/isn/13894/ManipulationReport.pdf>.

Written Agreement Between Standard Chartered Bank and New York State Department of Financial Services, Consent Order Under New York Banking Law §§ 39 and 44 (Aug. 19, 2014), online (pdf): <http://www.dfs.ny.gov/about/ea/ea140819.pdf>.