Pure

Bond University

DOCTORAL THESIS

Money Laundering: Facets associated with detection and magnitude of the problem.

Tiwari, Milind

Award date:
2021

Link to publication

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal.

Money Laundering:
Facets associated with detection and magnitude of the problem

Milind Tiwari

Submitted in total fulfilment of the requirements of the degree of Doctor of Philosophy

November 2021

Bond Business School

Professor Kuldeep Kumar and Associate Professor Adrian Gepp

This research was supported by an Australian Government Research Training Program Scholarship.

Abstract

The rise in financial crimes has resulted in a wide range of regulatory reforms to combat the problem. The failure of regulations to accomplish the desired objectives has brought regulators under pressure to justify their actions concerning political, executive and judicial scrutiny. One example of non-compliant behaviour subjected to extensive debate among practitioners, academics and regulators has been money laundering, an act of giving dirty money a legitimate appearance. In 2020, the amount of money being laundered after five rounds of international flows for the year of 2014 was estimated to be three percent of global Gross Domestic Product (GDP) or USD 2.3 trillion. The seriousness of the problem has increased over time, as indicated by the uncovering of the "Troika Laundromat" by the Organised Crime and Corruption Reporting Project (OCCRP), which involved moving billions of dollars of illicit Russian funds through the use of secretive offshore companies. On similar lines, shell companies incorporated in the U.K. alone were identified to be involved in laundering 80 billion pounds of stolen money between 2010 and 2014.

As a result, an emerging interest from both researchers and practitioners has surrounded money laundering. In the current economic environment, regulators are struggling to stay ahead of fraudulent schemes, and financial institutions are being challenged to ensure that they identify and stop criminal activities while serving legitimate customers effectively and efficiently. Consequently, it is necessary to improve understanding and come up with mechanisms to detect money laundering. This thesis contributes to this by: exploring the literature in the field; synthesising existing knowledge to develop a framework for explaining techniques adopted to launder funds; developing a model for detecting shell companies being used to launder illicit proceeds of crime using publicly available information; assessing an opportunity created by technological innovation to commit fraud and money laundering; assessing the implication of cannabis regulations on money laundering; and, finally, developing a money-laundering attractiveness index.

This dissertation first conducts a thematically systematised literature review to identify the extent of research conducted on money laundering. The complexity of techniques adopted to launder funds may vary depending upon the situation, with new typologies being created in response to changes in technology and regulations. However, no attempt is made in the literature to explain a launderer's choice of techniques. This research develops the new APPT framework of money laundering to explain the interrelated factors influencing the choice of

laundering techniques used to accomplish the objective. The new APPT framework is named according to four factors that each play a role in explaining the choice of techniques: the Actors involved, Predicate crime, the Purpose for laundering, and Technological innovations. The framework would assist in acknowledging the continuously evolving regulatory landscape and would direct attention towards the need for better mechanisms in combatting money-laundering activities.

Amongst the various techniques to launder funds, the review of existing literature identified the use of shell companies to be an under-researched technique to launder funds. Consequently, to address this need, the focus shifts towards developing a model for detecting shell companies being used to launder illicit proceeds of crime. The opportunity to detect illicit shell companies rested in using the networks prevalent among entities in a corrupt network and analysing the links and similarities. The analysis would facilitate scores of links and similarities that could be useful in distinguishing corrupt entities from non-fraudulent ones. Facilitating models to detect illicit shell companies using publicly available information quantitatively is under-researched.

The use of data science techniques in coming up with new detection mechanisms is worth appreciating. However, as depicted in the APPT framework, the importance of technological innovation in undertaking illicit acts of fraud and money laundering must not be undermined. The thesis takes a step in this direction by exploring an opportunity, initial coin offerings (ICOs), created by technological innovation to give rise to a predicate crime that may subsequently lead to money laundering.

To further understand the need for the APPT framework, detection mechanisms and being aware of new technological innovations capable of paving the way for illicit acts such as money laundering, it becomes critical to be aware of the magnitude of the problem. The review of existing literature identified a stream of research focusing on estimating the magnitude of money laundering. Among a range of illicit activities, the money from drug trafficking is the most prominent for immediate money laundering, and research work on money laundering would be incomplete without incorporating the contribution of drug trafficking to the amount of funds laundered. Considering the case of Australia, this thesis extends the literature by estimating the magnitude of money laundering by quantifying the amount of funds being laundered through cannabis trafficking.

Finally, acknowledging the debate in literature on lack of consensus on generated estimates of the magnitude of money laundering and the need to find countries attractive to launder funds, this thesis proceeds to construct a reliable and robust index for measuring a country's appeal as a destination for money laundering. It uses the Principal Component Analysis (PCA) to come up with a Money-Laundering Appeal Index (MLAI), thus avoiding the difficulty of precisely calculating illicit financial flows.

The key stakeholders to benefit from such research would be legal and compliance professionals and government officials, especially tax officials and anti-corruption NGOs. Among experienced practitioners, the knowledge of the APPT framework would aid in exercising professional judgement to come up with appropriate detection and deterrence mechanisms. In educational institutions, such a framework would suggest a move towards the incorporation of pedagogical techniques aimed at improving the content value and encouraging the development of skills valued by academics and practitioners.

The models developed to detect illicit shell entities could be of use to investigators, regulatory agencies and banks with access to transaction information. They could use the models alongside suspicious transaction analysis to increase the accuracy of entities they term as suspicious. The models developed as part of this research would assess the risk of a company being involved in illicit activities and whether there is a need to investigate further.

The work around Initial Coin Offerings (ICOs) would raise awareness around a possible opportunity to commit fraud as well as launder funds. Similarly, the work surrounding money laundered through cannabis trafficking could play a vital role in the debate around the legalisation of cannabis by providing an additional component for depicting harms from illegal markets. It may have implications for economies attempting to tackle the problem of money laundering by providing an avenue to consider the cannabis angle. Finally, the complex phenomenon of money laundering appeal can be placed into a single composite indicator and this might not only inform national strategies to prevent money laundering but provide an opportunity to use a similar approach to develop more localized hotspot maps that could move analysis at the sub-national level.

Key words

Money laundering; Shell companies; Detection; Illicit Activities; Graph Analytics; Cannabis Trafficking; Principal Component Analysis; Initial Coin Offerings (ICOs); Walker Gravity Model.

Declaration by author

This thesis is submitted to Bond University in fulfilment of the requirements of the degree of Doctor of Philosophy. This thesis represents my original work towards this research degree and contains no material which has been previously submitted for a degree or diploma at this University or any other institution, except where due acknowledgement is made.

Milind Tiwari

2nd November 2021

Declaration of Author Contributions

Publication Co-authored	Statement of Contribution
Tiwari, M., Gepp, A., & Kumar, K. (2021). Global money laundering appeal index: application of principal component analysis. *Journal of Money Laundering Control*. https://doi.org/10.1108/JMLC-10-2021-0108	MT 80%, KK 10%, AG 10%
Tiwari, M., Gepp, A., & Kumar, K. (2020). A Review of Money Laundering Literature: The State of Research in Key Areas. *Pacific Accounting Review*, *32*(2), 271-303. https://doi.org/10.1108/PAR-06-2019-0065	MT 80%, KK 10%, AG 10%
Tiwari, M., Gepp, A. & Kumar, K. The future of raising finance - a new opportunity to commit fraud: a review of initial coin offering (ICOs) scams. *Crime Law Soc Change* 73,417–441 (2020). https://doi.org/10.1007/s10611-019-09873-2	MT 80%, KK 10%, AG 10%
Tiwari, M. 2018. Shell companies – Identification of an instrument used for illicit purposes: A Pitch. *Journal of Accounting and Management Information Systems* 17 (4):685-692.	MT 100%

Research Outputs and Publications During Candidature

Peer- reviewed publications

1. **Tiwari, M.**, A. Gepp, and K. Kumar. 2020. Global money laundering appeal index: application of principal component analysis. *Journal of Money Laundering Control*. https://doi.org/10.1108/JMLC-10-2021-0108
2. **Tiwari, M.**, A. Gepp, and K. Kumar. 2020. A review of money laundering literature: the state of research in key areas. *Pacific Accounting Review* 32 (2):271-303.
3. **Tiwari, M.**, A. Gepp, and K. Kumar. 2019. The future of raising finance – a new opportunity to commit fraud: a review of initial coin offering (ICOs) scams. *Crime, Law and Social Change*.
4. **Tiwari, M.** 2018. Shell companies – Identification of an instrument used for illicit purposes: A Pitch. *Journal of Accounting and Management Information Systems* 17 (4):685-692.

Other publication

1. **Tiwari, M.**, A. Gepp, and K. Kumar. 2019. Case of Empty Crates: Finding a solution to letter-of-credit fraud. *Fraud Magazine*, 36(6).
2. **Tiwari, M.**, A. Gepp, and K. Kumar. 2019. Can economic sanctions lead to fraud?: Nations might turn to virtual currencies if slapped with restrictions. *Fraud Magazine*, 34(3).

Conference presentations

1. **Tiwari, M.**, A. Gepp, and K. Kumar. 2021. Shell Companies: Using a hybrid technique to detect illicit activities. In *2021 AFAANZ Virtual Conference.*

2. **Tiwari, M.**, A. Gepp, and K. Kumar. 2021. Shell Companies: Using a hybrid technique to detect illicit activities. In *2021 NODES Virtual Conference.*

3. **Tiwari, M.**, A. Gepp, and K. Kumar. 2020. Money Laundering: Using a hybrid approach to detect illicit shell companies. In *International Online Conference in Applied Statistics 2020: Application of Statistics in Sciences, Social Sciences, Commerce, Humanities and Management.*

4. **Tiwari, M.** 2020. Money Laundering: Ranking the countries attractive for money laundering to India. In *Online International Conference on 'Emerging Opportunities and Challenges in Indian Economy: An Interdisciplinary Approach.*

Working papers and papers in the publication process

1. **Tiwari, M.**, Gepp, A., & Kumar, K. (2021). The Evolution of Cannabis Regulation in Australia and the Overlooked Link with Money Laundering. *(Targeting journal: Criminal Justice Policy Review) (Rank: Q1)*

2. **Tiwari, M.**, Gepp, A., & Kumar, K. (2021). Factors influencing the choice of technique to launder funds: The APPT Frameworks. (*Targeting journal: Crime Science) (Rank: Q1)*

Ethics Declaration

"The research associated with this thesis received ethics approval from the Bond University Human Research Ethics Committee. Ethics Application number MT03540."

Copyright Declaration

Parts of Chapter 2 and Chapter 5 contain some material of mine already published in peer-reviewed journals. They have been published in journals, namely, *Crime, Law and Social Change* and *Pacific Accounting Review* and are reproduced with permission from *Springer Link* and *Emerald Publishing*. The citations for the papers are as follows:

Tiwari, M., Gepp, A. & Kumar, K. (2021). The future of raising finance - a new opportunity to commit fraud: a review of initial coin offering (ICOs) scams. *Crime Law Soc Change* 73, 417–441 (2020). https://doi.org/10.1007/s10611-019-09873-2

Tiwari, M., Gepp, A., & Kumar, K. (2020). A Review of Money Laundering Literature: The State of Research in Key Areas. *Pacific Accounting Review*, *32*(2), 271-303. https://doi.org/10.1108/PAR-06-2019-0065

Acknowledgements

I would first like to take this opportunity to thank my supervisors Professor Kuldeep Kumar and Associate Professor Dr Adrian Gepp for their ongoing advice, guidance and support, all of which has been extremely helpful throughout my PhD studies. Thanks to both of you for being a constant source of motivation and support in my academic research. Thank you for being the perfect role models and words are not enough to express my gratitude towards you both.

I would like to thank the Australian Government for funding this research ever since May 2019, through the Research Training Program Scholarship. I am particularly grateful to Professor Bruce Vanstone for his support and for providing me with many opportunities to grow as a professional, through attending industry conferences.

Thank you to Aaron, Junior, Kairi, Kristine, Lynna, Rafael and Viktoria for being such understanding and wonderful friends throughout this adventure. And to you Susan – thanks for the past, present and the future. I also want to acknowledge and thank the numerous other people who have greatly influenced who I am today and will become tomorrow; James and Tom, you are at the top of that list.

To Ahmad, Dipa, Rui, Vishal, Nicco, Robyn and Tahera, no words can accurately express my gratitude for the advice, friendship and support that you have given, and continue to give me.

To my family, thank you, now and always, for your unconditional love, honest advice and your unwavering belief in me. Most importantly, for being patient with me.

Last, but not the least, to Bond University and its people, for making me feel believe in myself and giving me a place to call home away from home.

When you want something, all the universe conspires in helping you to achieve it.

– Paul Coelho, *The Alchemist*

Table of Contents

List of Tables

List of Figures

List of Abbreviations/Acronyms

Active learning sequential design:	ALSD
Advocacy Coalition Framework:	ACF
All Pairs Shortest Path:	APSP
Amazon Web Services:	AWS
Anti-money laundering:	AML
Application Programming Interface:	API
Association of Chartered Certified Accountants:	ACCA
Australian Capital Territory:	ACT
Australian Crime Commission:	ACC
Australian Criminal Intelligence Commission:	ACIC
Australian Financial Services:	AFS
Australian Institute of Health and Welfare:	AIHW
Australian Securities and Investments Commission:	ASIC
Australian Transaction Reports and Analysis Centre:	AUSTRAC
Autorité des Marchés Financiers:	AMF
Banking Secrecy:	BS
Cannabis Expiation Notice:	CEN
Cannabis Intervention Requirement:	CIR
Classification and Regression Trees:	CART
Combating the Financing of Terrorism:	CFT
Commercial Affairs Department:	CAD
Commodity Futures Trading Commission:	CFTC
Conflict:	CF
Controlled Access Scheme:	CAS
Corruption:	CR
Crime and Misconduct Commission:	CMC
Diamond Reserve Club:	DRC
Diffusion Theory:	DT
Distributed Ledger technologies:	DLT
Dun and Bradstreet:	D&B
Egmont Group:	EG

European Economic Area:	EEA
European Securities and Markets Authority:	ESMA
Federal Deposit Insurance Corporation:	FDIC
Financial Action Task Force:	FATF
Financial Conduct Authority:	FCA
Financial Deposits:	FD
Financial Market Supervisory Authority: ..	FINMA
Financial Secrecy Index:	FSI
Financial Services Commission:	FSC
Financial Supervisory Services:	FSS
Fiscal Information and Investigation Service:	FIOD
Foreign Direct Investment:	FDI
General Refine Expression Language:	GREL
Government Attitude:	GA
Gross Domestic Product:	GDP
Hong Kong Monetary Authority:	HKMA
Hong Kong Securities and Futures Commission:	SFC
Hub Promoted Index:	HPI
Illicit Drug Data Report:	IDDR
Initial Coin Offering:	ICO
Initial Membership Offer:	IMO
Initial Public Offering:	IPO
Initial Token Sales:	ITS
Internal Determinants Models:	IDM
International Monetary Fund:	IMF
Investigative Consortium of Investigative Journalists:	ICIJ
Japan Cryptocurrency Business Association:	JCBA
Japan’s Financial Services Agency:	JFSA
Javascript Object Notation:	JSON
Kaiser-Meyer-Olkin Measure of Sampling Adequacy:	KMO
Limited Liability Partnership:	LLP
Limited Partnership:	LP
Link Discovery method based on Correlation Analysis:	LDCA
Monetary Authority of Singapore:	MAS

Money Laundering Appeal Index:	MLAI
Multiple Streams Approach:	MSA
Online Transaction Processing:	OLTP
Organisation for Economic Co-operation and Development:	OECD
Organized Crime and Corruption Reporting Project:	OCCRP
Persons with Significant Control:	PSC
Principal Component Analysis:	PCA
Punctuated Equilibrium Theory:	PET
Relational Database Management System:	RDBMS
Securities and Futures Act:	SFA
Securitites and Exchange Commission:	SEC
Society for Worldwide Interbank Financial Telecommunication:	SWIFT
Strongly Connected Component:	SCC
The Onion Router:	TOR
Transparency International, UK:	TIUK
United Nations Office on Drugs and Crime….	UNODC
Universal Node to ICO Research and Network:	UNICORN

Chapter 1 Introduction

As per the most recent estimates of International Monetary Fund (IMF), the level of money laundering ranges between 2% and 5% of the world's annual gross domestic product or approximately 1.5 trillion US dollars (FATF, 2012). As per the Australian Transaction Reports and Analysis Centre (AUSTRAC), the reported figure of money laundering ranges between $10 and $15 billion per annum in 2011 (Singh & Best, 2019). In 2020, the amount of money being laundered after five rounds of international flows for the year of 2014 was estimated to be three percent of global Gross Domestic Product (GDP) or USD 2.3 trillion (Ferwerda et al., 2020). The magnitude of the problem is also demonstrated by the "Troika Laundromat", uncovered by the Organized Crime and Corruption Reporting Project (OCCRP), that involved secretly moving billions of dollars of illicit Russian funds to offshore companies (OCCRP, 2019). Similarly, shell companies incorporated in the United Kingdom alone were identified to be associated with laundering 80 billion pounds of stolen money between 2010 and 2014 (Cowdock, 2017). Money laundering activities are a prominent threat to the global economy as proceeds of these activities may be used to fund further criminal activities and to undermine the integrity of financial systems worldwide.

The Financial Action Task Force (FATF) was formed in 1989 by The Group of Seven (G7) to further combat the growing problem. The FATF expanded the scope of money laundering by criminalising proceeds derived from other illicit sources such as illegal arms sales, insider trading, embezzlement, bribery and fraud. Since then, in an attempt to curb this growing problem, the scope of money-laundering regulation has been regularly widened further, such as to include activities financing the act of terrorism (Unger, 2013). The FATF serves as a vanguard in combatting money laundering by providing guidance to governmental bodies globally.

Money laundering attempts to wash dirty money to give it a legitimate appearance. According to the United Nations Office on Drugs and Crime (UNODC) 2000 Convention

(UNODC, 2004), money laundering involves converting or transferring an asset with knowledge of its being derived from a criminal source, concealing the criminal source or helping the criminal involved in committing the crime. The objective is to disguise the nature and origin of the illicit income generated and integrate it into the financial system without drawing tax authorities or law enforcement agencies' attention (Compin, 2008). Apart from the more usual underground activities such as cybercrime, corruption and drug trafficking, there are quasi-legal activities involving the concealment of income from public authorities. Such activities produce the shadow economy (Schneider, 2010; Schneider & Windischbauer, 2008). They contribute to money laundering as well. Buchanan (2004) categorises the process of money laundering into three stages, namely, placement, layering and integration. The first stage, that is, placement, involves introduction of the cash generated from illicit sources into the financial system. It is at this stage that the criminal proceeds are vulnerable to detection. The sources to introduce these funds into the financial system may comprise financial institutions, businesses and casinos. Generally, the amount of money to be laundered is deposited into bank accounts in smaller amounts or by purchasing goods which could be easily resold. Once the placement of the illicit proceeds takes place, the next step, layering, involves concealing and disguising the origin of such illicit funds. The illicit proceeds are separated from their source through a web of transactions. These are accomplished by the transfer of funds in related accounts or across jurisdictions, conversion of cash into other monetary instruments, investment in real estate or other such legitimate business, or into financial securities. The final stage in the process, that is integration, aims at manifesting the money (into cash) through normal business operations or personal transactions. The purpose is to make it difficult to distinguish between the legitimately derived and the laundered income.

Money laundering exploits a web of disguised relationships and unravelling this complex network of connections is challenging and time-consuming. These relationships include the adoption of different methods of placing money, its movement between actors in the financial system, and the organisational entities and their owners involved in the process. Furthermore, specific entities, most often shell companies, may play a transitory role within the network used to receive and distribute money.

Shell companies have legitimate uses such as facilitating reverse mergers, being used as holding companies or for protecting small entrepreneurs from bankruptcy risks. However, these entities have also become instruments for laundering the dirty money to make it appear legitimate and hide information about the actual beneficial owners. Illicit arms dealers, drug

cartels, corrupt politicians, terrorists and cyber-criminals have become some of the frequent users of these shell companies. The ease of setting up companies, trans-nationality involved and low-level of compliance towards the Financial Action Task Force (FATF) standards have posed a challenge for law enforcement authorities in countering crime and corruption (Martini et al., 2019). In 2002, an anonymous shell corporation called "Anglo-Leasing" was used to launder €24 million of the total €30 million as part of the contract awarded to the firm to update the passport system in Kenya. The information about the beneficial owners could not be identified because of the anonymity such form of entities provides (Allred et al., 2017; Findley et al., 2015). Other such instances involving the use of shell companies are that of China ZTE using shell companies to evade US sanctions, and SBM Offshore N.V., a Dutch-based group, paying bribes to shell companies owned by government officials (Hubbs, 2018).

Shell companies, with no physical presence and economic value, have legitimate purposes such as use in reverse merger thus providing access to formal economy and protecting small entrepreneurs from bankruptcy risks. However, they may be used for illicit purposes such as bribery, corruption, money laundering, terrorist financing by acting as a corporate veil to hide ultimate beneficial owner information. Therefore, it becomes essential to detect shell companies being used to launder the proceeds of illicit activities. Cowdock and Simeone (2019) conducted a forensic analysis of over 400 cases and interviews with academics and experts in the domain. They pointed to the need for further corporate transparency reforms to prevent abuse of companies in the UK and offshore financial centres.

It is necessary for jurisdictions such as the UK and Singapore, responsible for supplying opaque offshore structures and thereby reducing the effectiveness of the efforts of transparency and integrity, to take up more responsibility (Lasslett, 2019). Nougayrède (2019) believes appropriate steps need to be taken to combat the illicit use of shell companies. The steps include acceleration of intergovernmental measures to prevent tax evasion, money laundering and corruption through the exchange of financial information across borders, and by increasing corporate transparency. The empirical effect of these measures is yet to be ascertained; however, there do exist potential limitations for effective implementation of them. The limitation of their implementation may be attributed to resistance from jurisdictions such as the USA, proactiveness of national regulators and enforcement agencies and on the quality of information maintained by local service agents. A significant literature exists on enhancing regulations regarding beneficial ownership of shell companies and regulating CSPs. However,

no prior study exists on coming up with a model to detect shell companies being used to hide and transfer illicit proceeds.

In the current economic environment, regulators are struggling to stay ahead of fraudulent schemes, and financial institutions are being challenged to ensure that they identify and stop criminal activities while serving legitimate customers effectively and efficiently. Effective technological solutions are an essential element in the fight against money laundering. The continuously evolving regulatory landscape, in combination with recent instances of money laundering violations, has highlighted the need for better technology in managing anti-money laundering activities (Ray, 2015). An improvement in data and analytics would be essential in assisting investigators to focus more on suspicious activities and less on false positives (Newman, 2007). The representation of data in the form of graphs would establish the presence, if any, of a relational structure, and graph computations can provide a stronger relational inductive bias. Graph analysis may enable investigators to effortlessly infer ownership and relationships, such as common or joint ownership of businesses; this may mean prompt detection of illicit shells.

1.1 Aim of research

The research aims to advance the field of money laundering in terms of:

- Reviewing the literature around money laundering and identifying key research gaps
- Developing an understanding of the reasons behind the choice of using a particular technique to launder funds
- Developing an appropriate schema of relationships to identify hidden patterns and relationships among entities, if any;
- Using graph analytics and supervised learning methods to detect illicit shell companies using publicly available data for the UK incorporated private-limited companies
- Identifying the emergence of a new opportunity to commit fraud and launder funds by means of technological innovations, in particular, Initial Coin Offerings (ICOs) as it depicts how FinTech innovation like cryptocurrencies is being used as means to commit fraud;
- Assessing the magnitude of money laundering subject to cannabis trafficking given drug trafficking constitutes the major portion of laundered money and cannabis is one of the largest consumed drugs;
- Identifying factors making a country an appealing destination to launder funds

The main objective of this research is to improve knowledge around money laundering, and to develop models for the identification of shell companies being used to launder illicit proceeds of crime. The central hypothesis is that a useful model for detecting illicit shell companies can be built by analysing such entities identified in the past to be associated with various illicit activities. It attempts to produce findings that are widely applicable to regulators, investigators and other stakeholders.

The main research questions that this study addresses are introduced below.

Research Question 1 (RQ1): What factors may influence a launderer's choice of technique to launder funds?

Research Question 2 (RQ2): Does the presence of data related to entities on a graph database platform aid in revealing hidden patterns and relationships?

Research Question 3 (RQ3): Are combinations of graph analysis algorithms and supervised-learning modelling techniques successful in detecting illicit shell companies?

Research Question 4 (RQ4): How have the changes in technology enhanced the opportunity to commit fraudulent acts?

Research Question 5 (RQ5): How do the changes in cannabis regulations affect money laundering in Australia?

Research Question 6 (RQ6): What factors may make a country attractive for a money launderer to launder funds?

1.2 Main contributions of this research

This research is first in coming up with a framework to determine a launderer's choice of techniques to launder funds. Among a range of illicit activities, the money from drug trafficking is the most demanding for immediate money laundering, and research work on money laundering would be incomplete without incorporating the contribution of drug trafficking on the amount of funds laundered. Consequently, there is an assessment of the effects of cannabis regulations in Australia on money laundering. Such an understanding may help in being proactive to assess the effects of regulatory changes on money laundering and come up with suitable detection mechanisms. This research utilises a comprehensive range of material to develop a property graph database (a graph model representation where nodes, apart from connections between them, have properties associated with it) using publicly available information. Further to this, the data used in the analysis are not synthetically generated and comprise entities identified in actual cases of corruption. Consequently, findings from this research contribute to a better understanding of money laundering and the use of graph database models in detecting money laundering through illicit shell companies. Some of these findings include:

- A framework for the choice of technique adopted to launder funds is provided
- Empirical support for the use of multi-relational property graph databases platforms that detect money laundering
- Empirical support for retrieval of hidden patterns and relationships using traversal queries
- Identification of the fraudulent opportunities arising through ICOs
- An empirical assessment of the magnitude of money laundering through cannabis trafficking; and,
- Identification of factors resulting in development of the Money-Laundering Appeal Index (MLAI)

This research also makes a contribution to the literature on money laundering. It is further identified that the detection of money laundering through shell companies had received limited attention. The existing literature on shell companies is focused on regulations related to international standards aiming to achieve transparency. Additionally, the focus has been on implementation of these regulations on CSPs.

Consequently, results from this research make an important contribution to a better understanding of the use of graph database platforms to traverse through networks of illicit shell companies and employ additional graph analytics to develop detection models. Some of the results are briefly mentioned below.

The graph database of corporate entities shows that only 51 companies in the dataset had an ultimate beneficial owner and 16 companies were located at the same postal address. Furthermore, in the graph database of corporate entities, two individuals had executive appointments in 139 and 610 entities, respectively. No studies in the past have considered companies from multiple illicit corruption cases in the same graph network and attempted to investigate the links between them, and then gone on to propose a need to adopt a graph database structure for storing information related to corporate entities. Additionally, several graph algorithms were performed, mainly related to determining similarities, communities and node importance. One of the underlying rationales was to establish a base for the interaction between network structure and node attributes, rather than just considering the importance of nodes in a network. Such a step would permit advantage to be taken of both network structure and node attributes (Backstrom & Leskovec, 2011). The scores were the results of these graph analytics and were further exported to decision-tree software called CART (Classification and Regression Trees) provided exclusively by Salford Systems. The results showed that on using three classification algorithms, namely Decision Trees, TreeNet and Random Forests, for the combination of a variety of graph algorithms, the classification accuracy achieved was within the range of 88.17 % and 97.85 % respectively. It is important to note that variables that are difficult to obtain are not likely to be used in a practical context; therefore, all explanatory variables used in this research are publicly available (Perols, 2011a).

Overall, new contributions are made to the current body of research on money laundering. A framework of money laundering, informed by several theories, is proposed to explain the choice of a particular technique to launder funds. This information can be used to improve early detection, which would mitigate cost to society and help deter occurrence. There

are also specific beneficiaries of this information such as regulators, company service providers, corporate registries and investigators who can use detection models to assist them in better assessing the risk of an entity involved in illicit activity and whether there is a need to investigate further. Additionally, financial institutions can use detection models to help them avoid prolonged association with fraudulent companies.

1.3 Dissertation structure

The next chapter (Chapter 2) introduces and provides a brief overview of the concept of money laundering. It includes a review of literature related to money laundering and its related aspects. This information is followed by the identification of the research gap in the literature.

Following this overview of money laundering, Chapter 3 focuses on attempting to explain the factors influencing the choice of techniques adopted to launder funds. The idea is to propose an interrelated framework for money laundering. Such a multi-dimensional model of money laundering complements the knowledge about various techniques available to launder funds gained in Chapter 2, and it helps to provide a better detection mechanism.

Based on the review of money-laundering literature and identification of the research gap, Chapter 4 lays down the foundation for the development of a model for the detection of illicit shell companies. It provides an overview of data used, data collection methodology and the development of graph database schema. Such a schema allows for identification of patterns using traversal queries. The chapter then presents a discussion of the results and the potential implications of a graph database platforms for stakeholders. The chapter then concludes with an overview of the modelling techniques used, analysis of data and results.

In continuation, to emphasise the importance of technological innovations, Chapter 5 presents an examination of a new opportunity to commit fraud and money-laundering crimes through Initial Coin Offerings (ICOs). It includes the use of case-study analysis to determine characteristics of fraudulent schemes, regulatory changes to combat such an illicit act, and the potential takeaways for investors, issuers and regulators.

To justify the seriousness of the problem of money laundering, Chapter 6 focuses on the effects of cannabis regulations on money laundering in the context of Australia. Illicit drug trafficking provides a major portion of funds available for laundering and consequently it

becomes important to assess whether regulatory changes pertaining to drugs such as cannabis, so often a topic of debate, have an influence on money laundering.

Chapter 7, deviating from literature on money-laundering estimation magnitude, directs attention to factors that may increase the appeal of a country as a destination for laundering funds. As established in the literature, weaker AML regulations do not necessarily make a country an appealing destination for money laundering.

Chapter 8 presents the overall conclusion and suggested future work. The thesis structure is exhibited by Figure 1.

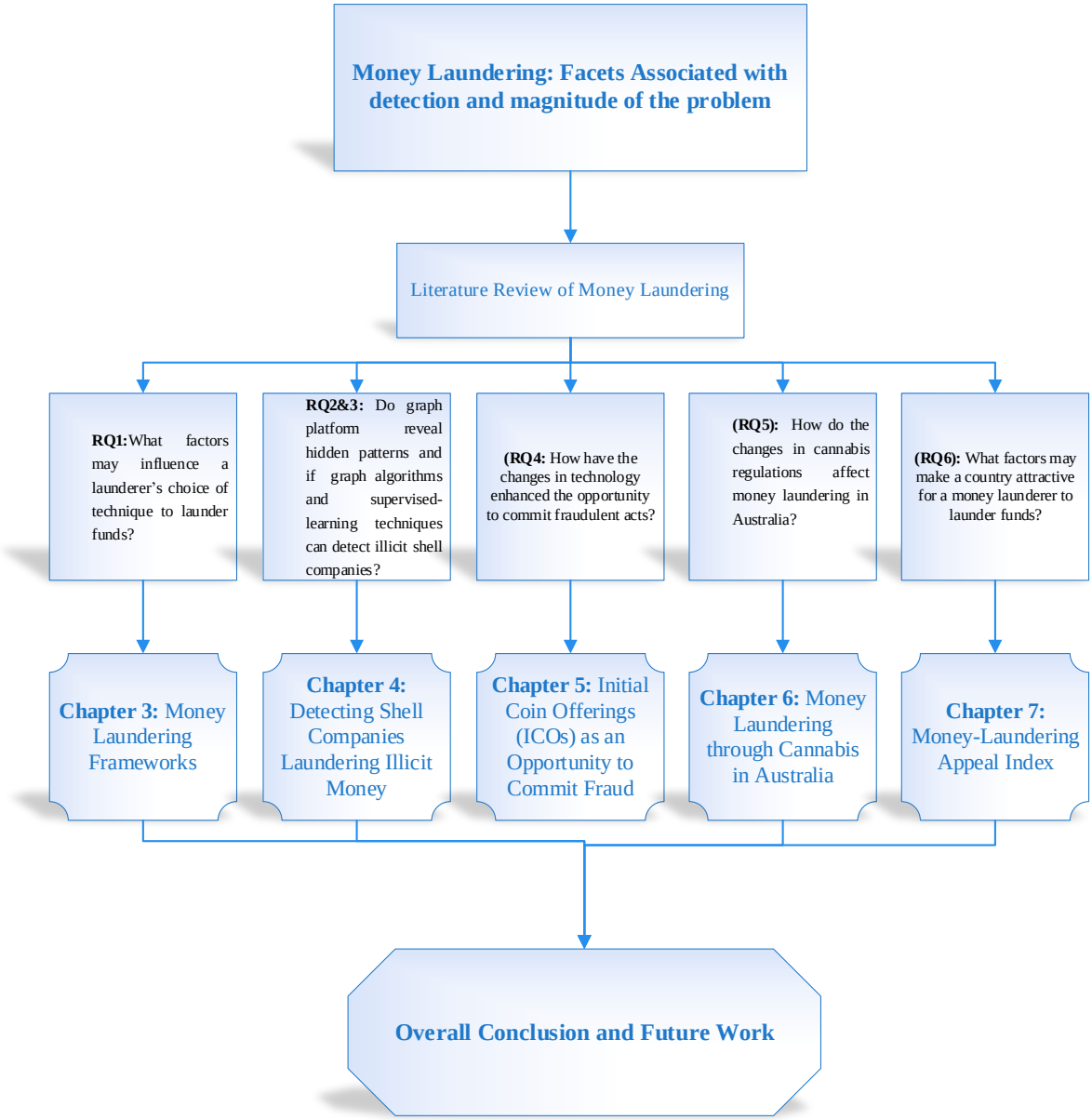

Figure 1: Thesis Map

Chapter 2 Literature Review of Money Laundering

* This chapter is based on a published paper in a peer-reviewed journal, namely: Tiwari, M., A. Gepp, and K. Kumar. 2020. A review of money-laundering literature: the state of research in key areas. *Pacific Accounting Review* 32 (2):271-303.

Money laundering makes dirty money appear legitimate. The United Nations Office on Drugs and Crime (UNODC) 2000 Convention (UNODC, 2004) says that money laundering involves converting or transferring an asset with knowledge of its being derived from a criminal source, concealing the criminal source or helping the criminal involved in committing the crime. The objective is to disguise the nature and origin of the illicit income generated and integrate it into the financial system without drawing the attention of tax authorities or law enforcement agencies (Compin, 2008). Apart from underground activities such as cybercrime, corruption and drug-trafficking, there are other quasi-legal activities concealing income from public authorities. Such activities produce the shadow economy (Schneider, 2010; Schneider & Windischbauer, 2008). They also contribute to money laundering. Buchanan (2004) divides the process of money laundering into three stages, namely, placement, layering and integration.

The first stage, placement, involves the introduction into the financial system of the cash generated from illicit sources. It is at this stage that the criminal proceeds are vulnerable to detection. The sources to introduce these funds comprise financial institutions, businesses and casinos among others. Generally, the amount of money to be laundered is deposited into bank accounts in smaller amounts or by purchasing goods which could be easily resold. Once the placement of the illicit proceeds takes place, the next step, layering, involves concealing and disguising the origin of such illicit funds. The separation of illicit proceeds from their source takes place through a web of transactions. It is accomplished by the transfer of funds in related accounts or across jurisdictions, conversion of cash into other monetary instruments, investment in real estate or other such legitimate business or financial securities among others.

The final stage in the process that is integration aims at returning or converting the money (into cash) through normal business operations or personal transactions. The purpose is to make it difficult to distinguish between legitimately derived income and laundered income.

Identified instances such as the Danske Bank scandal (Bjerregaard & Kirchmaier, 2019), Panama Papers (Harding, 2016), the Paradise Papers, and the Offshore Leaks (International Consortium of Investigative Journalists) have brought to light the scale and effect of money-laundering activities at a global level. As a result, it becomes critical to understand the work done around money-laundering activities globally. Additionally, the use of shell companies to accomplish laundering of illicit proceeds as observed in laundromat schemes such as the Troika Laundromat and the Azerbaijani Laundromat gives rise to the need to review the literature on shell companies.

To better understand the concept of money laundering and the availability of a wide range of methods to accomplish it, this chapter begins with a brief introduction. It is followed by a review of the multi-faceted literature on money laundering and its related areas to lay down the foundation for discussion of the detection of such activities undertaken through shell companies.

2.1 Brief introduction to money laundering

In 1998, the then-director of the International Monetary Fund (IMF) highlighted the problem by estimating the amount of money being laundered to be between two and five percent of global Gross Domestic Product (GDP) (Camdessus, 1998). The Organized Crime and Corruption Reporting Project (OCCRP) highlighted schemes such as the "Troika Laundromat", involving movement of billions of dollars of illicit Russian funds using offshore companies (OCCRP, 2019). Similarly, shell companies incorporated in the United Kingdom alone were identified as being associated with laundering 80 billion pounds of stolen money between 2010 and 2014 (Cowdock, 2017).

The term "laundering" was named after the gangster Al Capone's use of launderettes for disguising illegal revenues from an alcohol business in the United States. The launderettes, one of the most cash-intensive businesses during the 1930s, served as an ideal location for washing the dirty money. However, the activities which in today's time would be defined as money laundering have been in use for a long time. For instance, in earlier times, the use of a variety of methods by money lenders to conceal and move the overcharged amount of interest collected on loans, or merchants purchasing assets to hide their wealth, would be viewed as money-laundering activities.

The necessity to monitor money-laundering activities has gained prominence with growing concerns in the USA regarding the movements of funds across borders for tax evasion or the use of cash-intensive businesses such as casinos to conceal the origin of funds (Levi & Reuter, 2009; Van Duyne, 2003). However, money laundering was criminalised as far back as 1986. The Money Laundering Control Act of that year in the USA was an attempt to tackle the illicit proceeds from acts of bribery, drug trafficking, extortion and fraud. The motive was to aid in the war against drugs by reducing the profitability of organised crime from criminal activities. Additionally, a prevailing global belief was that to conceal the illicit funds, they were being moved to offshore jurisdictions and tax havens. Subsequently, the phenomenon of money laundering garnered attention as a threat to legitimacy and stability of financial systems and a source of reputational risk (Van Duyne & Levi, 2005). All these factors paved the way for the emergence of a consensus among global economic powers to develop and initiate a coordinated response to tackle the money-laundering problem.

The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances was held in Vienna from November 25 to December 20, 1988. It

was the first global step to address the problem of money laundering. The convention made offenders subject to money laundering prosecution if found trying to launder illicit wealth earned from production and sales of narcotics. The Financial Action Task Force (FATF) was formed in 1989 by The Group of Seven (G7) to further combat the growing problem. The FATF expanded the scope of money laundering by criminalising proceeds derived from other illicit sources such as illegal arms sales, insider trading, embezzlement, bribery and fraud. Since then, in an attempt to curb this growing problem, the scope of money-laundering regulation has been regularly widened further, such as to include activities financing the act of terrorism (Unger, 2013).

The next section in this chapter provides a brief overview of research on money laundering and its related aspects. Following this, current works investigating shell companies are discussed to highlight the gaps in the literature.

2.2 Review of money-laundering literature

A systematic approach was used to investigate the current literature on money laundering and shell companies. First, Pro-Quest, Scopus and Science-Direct were searched for papers that contained the keywords “money launder*” in the title, abstract or keywords. Additional articles were obtained by investigating cited references and conducting Google Scholar searches. After an initial review of these papers, additional searches were conducted using keywords found in those articles. The additional search keywords were “shell compan*”,“shell firm*”, “anonymous compan*”, “front compan*”, “phantom firm*”, “dormant compan*”, and “sham corporation*” as documented in Table 1.

S. No	Database	Search String	Date Access	Results
1	Pro-Quest	"Money Laundering"	15-05-21	14,623
2	Scopus	"Money Laundering"	15-05-21	2,806
3	ScienceDirect	"Money Laundering"	15-05-21	3,794
4	Google Scholar	"Money Laundering"	15-05-21	30,700
5	Pro-Quest	"Online Money Laundering"	14-01-21	10
6	ScienceDirect	"Money Laundering" AND "Australia"	13-04-21	690
7	Pro-Quest	"Money Launderer"	28-02-21	309
8	Scopus	"Money Launderer"	12-05-21	104
9	ScienceDirect	"Money Launderer"	04-05-21	3,794

S. No	Database	Search String	Date Access	Results
10	ScienceDirect	“Shell Firms” AND “Money Laundering”	09-04-21	3
11	ScienceDirect	“Shell Companies” AND “Money Laundering”	09-04-21	66
12	Scopus	“Shell Companies” AND “Money Laundering”	09-04-21	18
13	Scopus	“Shell Firms” AND “Money Laundering”	09-04-21	4
14	Scopus	“Shell Firms” AND “Fraud”	09-04-21	3
15	Scopus	“Shell Companies” AND “Fraud”	09-04-21	14
16	ScienceDirect	“Shell Companies” AND “Fraud”	09-04-21	117
17	ScienceDirect	“Shell Firms” AND “Fraud”	09-04-21	8
18	ProQuest	“Shell Companies” AND “Money Laundering”	11-05-21	390
19	ProQuest	“Shell Firms” AND “Money Laundering”	11-05-21	4
20	ProQuest	“Dormant Firms”	20-04-21	111
21	ProQuest	“Dormant Firms” AND “Money Laundering”	20-04-21	15
22	Google Scholar	“Shell Firms” AND “Money Laundering”	11-05-21	53
23	Google Scholar	“Dormant Firms” AND “Money Laundering”	11-05-21	4
24	ProQuest Dissertation	“Shell Firms”	20-04-21	21
24	ProQuest Dissertation	“Shell Firms” OR “Shell Companies” OR “Dormant Firms” AND “Money Laundering”	12-05-21	789
25	ScienceDirect	"Shell firms" OR "Shell Companies" OR "Dormant Firms"	12-05-21	1155
26	EBSCO Business Host	"Shell firms" OR "Shell Companies" OR "Dormant Firms" AND “Money Laundering”	13-05-21	392
27	ScienceDirect	"Shell firms" OR "Shell Companies" OR "Dormant Firms" AND “Money Laundering”	20-05-21	1142

S. No	Database	Search String	Date Access	Results
28	SAGE Journals	"Shell firms" OR "Shell Companies" OR "Dormant Firms" AND “Money Laundering”	20-05-21	169
29	Scopus	"Shell firms" OR "Shell Companies" OR "Dormant Firms" AND “Money Laundering”	20-05-21	14
30	Google Scholar	"shell compan*" OR "anonymous compan*" OR "transit firm*" OR "taxhole compan*" OR "Front compan*" OR “front compan*” OR “mailbox compan*” OR “sham corporation*” OR “shelf compan*” OR “paper firm*” OR "paper compan*" OR “phantom firm*” OR “phantom compan*"	27-03-21	34
31	ProQuest	"shell compan*" OR "anonymous compan*" OR "transit firm*" OR "taxhole compan*" OR "Front compan*" OR “front compan*” OR “mailbox compan*” OR “sham corporation*” OR “shelf compan*” OR “paper firm*” OR "paper compan*" OR “phantom firm*” OR “phantom compan*"	17-02-21	8,252
32	ScienceDirect	"shell compan*" OR "anonymous compan*" OR "transit firm*" OR "taxhole compan*" OR "Front compan*" OR “front compan*” OR “mailbox compan*” OR “sham corporation*” OR “shelf compan*” OR “paper firm*” OR "paper compan*" OR “phantom firm*” OR “phantom compan*"	17-02-21	173

Table 1. Search log with keywords

Table 1 lists the database search strings that formed the basis of this review. The review of relevant studies led to a thematic categorisation of the literature on money laundering and shell companies. The categorisation foregrounds different aspects of the money-laundering process. Money laundering can be multi-faceted; for instance, the use of shell companies to launder funds does not rule out the use of banks in aiding the illicit activity. In such cases, only the most prominent part of the laundering technique is used for categorisation purposes. Additionally, the focus on money laundering literature is derived from the fact that shell companies are used to launder the proceeds of illicit activities such as drug-trafficking, robberies, smuggling, tax evasion, terrorism, bootlegging, art theft, vehicle theft, fraud and so forth (Mitchell et al., 1998a, 1998b). As a result, it becomes imperative to understand the work done around money laundering before focusing explicitly on shell companies and its uses in undertaking illicit activities.

The review of money-laundering literature led to categorisation of the literature on money laundering into six broad categories as exhibited in Figure 2, namely, anti-money laundering (AML hereafter) framework and its effectiveness, the effect of money laundering on other fields and the economy, the role of actors and their relative importance, the magnitude of money laundering, and new opportunities for money laundering and its detection. The classification of the literature into those broad but overlapping categories above is to showcase the volume of work being undertaken concerning different aspects of money laundering. Such a cross-horizon review helps to identify areas that might have been overlooked or that have not been extensively researched. The following sub-sections provide an analysis of the critical research in each of these categories.

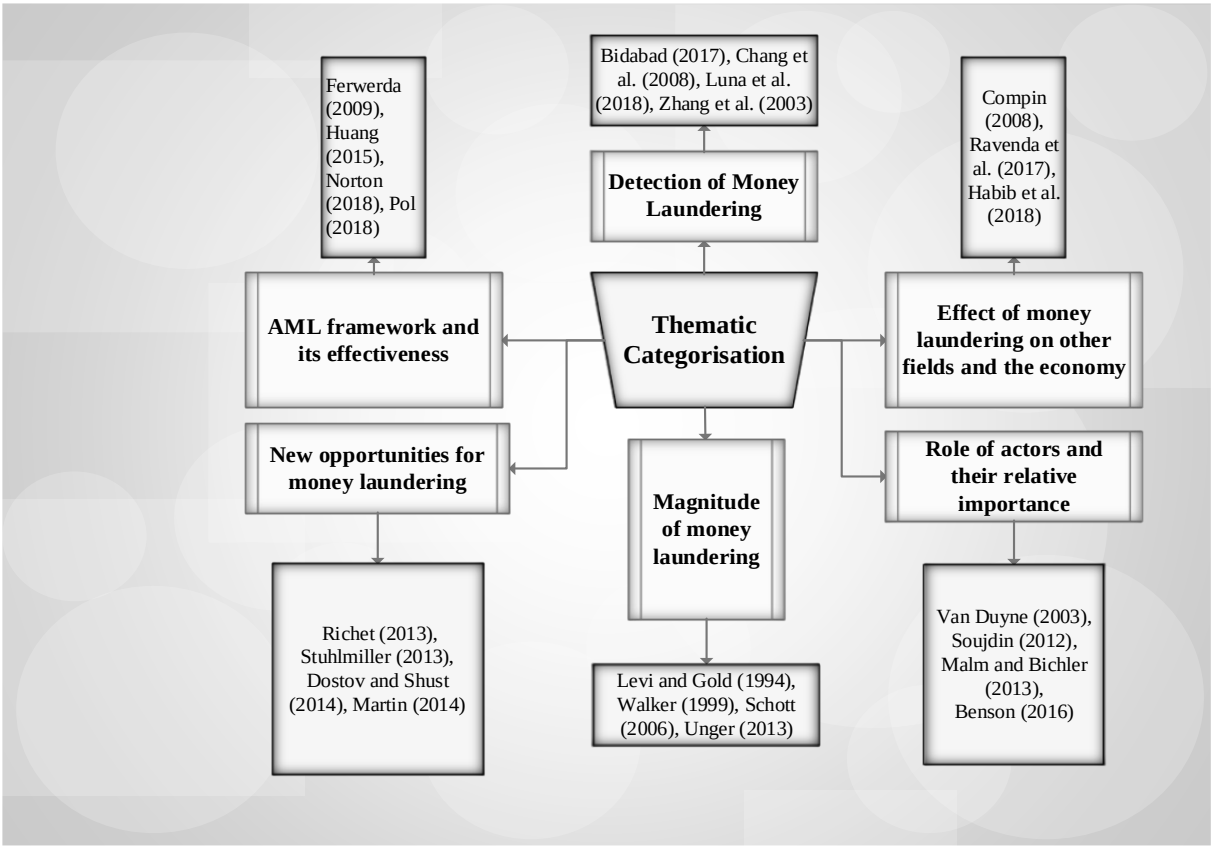

Figure 2: Classification of literature on money laundering

2.2.1 AML framework and its effectiveness

A fast-growing body of literature exists on AML and counter-financing of terrorism (CFT hereafter) framework and regulations. The effectiveness of the AML regime and its effect on illicit activities such as money laundering, terrorism, financing of crime and crime prevention and detection have been of interest to scholars (Anand, 2011; Barone & Masciandaro, 2011; Brzoska, 2016; Chaikin, 2009; Ferwerda, 2009; Harvey, 2008; Huang, 2015; Masciandaro, 1998; Masciandaro & Portolano, 2003; Pellegrina & Masciandaro, 2009; Unger et al., 2014). The interest arises out of the need to provide sufficient justification for the cost incurred in implementing these regulations and their effectiveness in achieving the desired objectives.

Masciandaro (1998) and Masciandaro and Portolano (2003) termed AML legislation to be costly because of its negative effect on the efficiency of domestic and international banking.

Huang (2015) provided a macro-level analysis of the AML legislation present in the USA, including the reasons underlying its effective implementation. The study examined the effectiveness of the American AML regime on the banking sector and observed it has adverse socio-economic effects, in terms of fear of compliance and violation of regulations. Other jurisdictions have also been studied. Alberto (2016) examined the effectiveness of a new Spanish Act of financial ownership to combat money laundering and financing of terrorism by comparing it with models of France and Germany. He found the Act to have shortcomings in terms of data protection, automation in processing of personal data, and access to information by third parties without consent. Aurasu and Aspalella (2018) conducted a comparative analysis of Money Laundering Acts between the United Kingdom and Malaysia in terms of their forfeiture regime. These two countries share a similar legislative structure which facilitated comparison. It was concluded that the United Kingdom's money laundering Act is more comprehensive than the Malaysian Act in terms of offences covered and the standard of proof. However, Norton (2018) critiqued the United Kingdom's AML legislative changes and highlighted its failure to clearly define "suspicious activity", thus leading to a low threshold to report. As a result, there was a notable increase in the volume of reporting by auditors.

Jakobi (2018) examined the global AML regime from a security governance perspective and concluded that AML represents the elements of security governance. Pol (2018a) extended this literature by focusing on AML practices and their effectiveness as a policy against defined outcomes as set by FATF. He found that FATF methodologies are not sufficient and a better implementation is required to achieve effective results. Pol (2018b) further questioned the other assumptions upon which the global AML/CFT framework is based, that is, whether forfeiture of criminal assets is a good measure of evaluating the success of AML policies and whether their extension as an obligation for new sectors will have an effect.

Pellegrina and Masciandaro (2009) highlight the differences that exist between countries' national legislation about the criminalisation of money-laundering activities. They suggest that eliminating the possibility of exploiting the differences between regulations across countries may help in increasing the effectiveness of the AML regulations. The need for international cooperation to bolster the AML regime is supported by Ferwerda (2009). On the lines of assessing the AML effectiveness, Barone and Masciandaro (2011) estimated the public benefit for Europe from a drastic reduction in the money-laundering multiplier effect. They found the cost of AML regulations would increase to achieve a reduction in the multiplier effect and this would result in increased public benefits. Similarly, Barone and Schneider (2018) are of the

view that a causal link exists such that effective AML regulations increase the costs for criminal organisations. They describe this as an efficient way to reduce money laundering.

The debate around the AML framework and its effectiveness has led to the rapidly changing regulatory landscape to combat the problem of illicit activities including money laundering. It is demonstrated by the proposed changes made to the reforms to address the loopholes and effectively address the problem of money laundering (AUSTRAC, 2018; Bozhilova, 2018). For instance, a list of proposed changes has been suggested to the existing European Union's Fifth Anti-Money Laundering Directive to address the loopholes in regulation. The proposed changes address aspects related to exchange and use of information and to the operational cooperation between financial intelligence units (FIUs) of the member states, as well as between FIUs and competent authorities within the member states. The goal is to reduce opportunities for illicit actors to take advantage of national differences in the definition, scope and sanctioning of money-laundering offences which result in sub-optimal cooperation between concerned authorities of member states. The proposals seek to incorporate changes in line with other policies pursued by the EU, such as the reformed data protection regime (Bozhilova, 2018).

Prominent Work	Key Objective	Key Findings
Ferwerda (2009)	Assess the role of AML policies in deterring criminals from illegal activities	• Improved AML policy was associated with lower crime rates
Barone and Masciandaro (2011)	Estimate the public benefit of reducing money laundering	• In Europe, an estimated public benefit of USD 7.71 billion for an increase of USD 5.45 billion in the cost of AML regulations
Unger et al. (2014)	Analyse the AML/CFT regimes of EU member states	• Effectiveness of AML policy was dependent upon national institutions in member states
Huang et al. (2015)	Analyse US AML legislation to determine its effectiveness	• The US AML legislation was found to be comprehensive • This legislation is enforced diligently, which has an adverse socio-economic impact on financial

		institutions in terms of adherence, and thus undermining their effectiveness
Pol (2018)	Analyse the effectiveness of the AML regime against FATF defined outcomes	• AML policies were determined to be ineffective and considered as a waste of resources and efforts • The need was proposed for development of a new set of strategies
Manning et al. (2020)	Investigate relationship between FATF recommendation compliance, regulatory affiliations and Basel AML Index	• Irregularity in guidelines used by countries to develop AML regulatory policy undermines AML security • Need to maintain continuing and consistent compliance standards across all affiliation groups, and facilitate cross-jurisdictional cooperation among financial intelligence agencies

Table 2. Overview of research on the effectiveness of AML

2.2.2 Effect of money laundering on other fields and the economy

Apart from critiquing the AML framework, researchers have also focused on the relation of money laundering with various other fields and its effect on the overall economy. The effect of money laundering and tax havens on each other has been examined by many scholars (Dharmapala & Hines, 2009; Masciandaro, 2008; Rose & Spiegel, 2007). Schwarz (2011) extended this literature by determining the incentives for tax havens to maintain low regulatory standards for attracting dirty money and thus provide money-laundering services. Picard and Pieretti (2011) aimed at observing the effect of pressure policies such as blacklisting and sanctions on offshore financial centres (OFCs hereafter) and their ability to ensure compliance with AML regulations. Instead of analysing the desirability or harm of tax havens (Alstadsæter et al., 2018; Christensen, 2012; Chu et al., 2015), Picard and Pieretti focused on the incentives for offshore governments and banks to comply with AML regulations. They found that offshore banks would comply under pressure policies, provided the pressure had the potential to harm the reputation of investors.

Knowledge of accounting has always been essential and used by various stakeholders in promoting their respective interests (Kenno & Free, 2018); with the advent of technological innovations, the importance of accounting has only increased (Hoiberg, 1999). Compin (2008)

assessed the importance of accounting knowledge in undertaking money-laundering and terror-financing activities by using a theoretical approach. He concluded that money laundering and terror financing differ concerning financial sophistication and psychological profile. Irwin et al. (2012) also found that money launderers and terrorist financiers exhibit different laundering techniques and launder different amounts; the techniques involved in money laundering are sophisticated, and the asset value involved is higher, as compared with terrorist financing.

The importance of accounting practices in undertaking illicit activities such as money laundering and corruption, and facilitating a criminal network between the perpetuators, was supported by Mitchell et al. (1998b) and Neu et al. (2013). A large sum of money cannot be laundered without the help of accountants and other professionals who use their expertise to obscure and conceal the illicit source of funds. Mitchell et al. (1998a; 1998b) used case studies to examine the role of accountants in undertaking illicit activities. Before this study, the scrutiny of links between white-collar crimes and accountants was limited only to social scientists and was neglected by accounting academics. The study emphasised the involvement of accountants in money laundering and the unwillingness of regulators to investigate them. Ravenda et al. (2017) contributed to this by extending the literature on the use of accounting practices for undertaking money-laundering activities to Italian Mafia firms. Further to this, the need to focus on the use of forensic accounting and its knowledge to combat illicit activities has been emphasised by Botes and Saadeh (2018).

The effect of money laundering on the economy and vice versa has also been examined. According to Dowers and Palmreuther (2003) and Drayton (2002), money laundering harms the economy by causing monetary and socio-economic instability and economic distortions; it promotes corruption and a more vulnerable financial system. Stack (2015b) examined the role of money-laundering organisations in Ukraine to facilitate tax evasion and corruption. He found that a massive amount of dirty money is generated and used to satisfy the greed of state actors. Similarly, Hendriyetty and Grewal (2017) found that money laundering increases criminal activities and the shadow economy, and also reduces tax collections. On the other hand, Barone et al. (2018) analysed the effect of macroeconomic cycles on illicit capital and money-laundering activities to determine whether business cycles can influence trends and activities in illegal markets and money laundering. They found that during different economic cycles, the capacity of illegal capital that the market can sustain varies.

Prominent Work	Key Objective	Key Findings

Schwarz (2011)	Analyse the relationship between money laundering and tax havens	• They coincide within the same country • Poorer countries are more inclined towards providing money-laundering services
Balakina et al. (2017)	Empirically evaluate whether there is a stigma from FATF blacklisting about banking secrecy	• No stigma effect is found • Change in demand for banking secrecy is due to a change in incentives rather than blacklisting • Incentives may be economic, political or criminal
Barone et al. (2018)	Determine the effect of business cycles on money laundering	• Illegal markets grow at rates that depend upon the condition of the legal economy • The pass-through effect exists since the business cycle influences legal markets that are used by illegal operators to reinvest their profits
Mitchell et al. (1998)	Investigate the relationship between accountants and regulators, and any protection of illicit professionals.	• The reluctance of regulators to pursue accountants and larger accounting firms suggests the presence of a regulatory apparatus to shield the activities of accountancy firms from critical scrutiny
Ravenda et al. (2017)	Examine the use of accounting practices on money-laundering activities	• Empirical evidence suggests that strategic management of accounting transactions is occurring to assist money-laundering activities within Mafia-controlled firms
Habib et al. (2018)	Investigate the relationship between money laundering and audit fees	• A positive association exists between money laundering and audit fees • Money laundering raises audit fees by increasing the overall business risk unrelated to financial reporting quality
Loayza et al. (2019)	Provide an economic analysis of illicit activities and money laundering	• Presents measures to assess the effects of changes in government efficiency, licit sector productivity, and the demand for illegal drugs • Monitors changes in trends in volume of laundered assets

Table 3. Overview of research on the effect of money laundering on other fields and the economy

2.2.3 The role of actors and their relative importance

Prior literature has studied the role of actors involved in money-laundering activities, those laundering for themselves, laundering on behalf of others and even those trying to prevent it.

It becomes quite vital to determine the importance of money launderers in undertaking such an illicit activity. Furthermore, it is critical to understand their source of motivation (Barone et al., 2018; Barone & Masciandaro, 2011; Barone & Schneider, 2018). Van Duyne (2003) and Reuter and Truman (2004) found that criminals generally laundered money themselves rather than hiring professionals to do it. On the contrary, Soudijn (2012) reported that professionals are an essential part of criminal networks, but he did not specify their involvement in drug markets.

Malm and Bichler (2013) tried to address the question of who launders money and their respective roles in the criminal network. The authors found the importance of money launderers to be higher in drug markets than any other illicit market and found support for the notion of a social snowball effect whereby the social circle of a person played an important role in entering the illicit drug market. This notion was reiterated by Gilmour (2015) who characterised the importance of the social and cultural context of a person in influencing his decisions to commit an offence or not. On examining the importance of legal and finance professionals in money-laundering activities, Benson (2016) found that the decision to launder criminal proceeds is influenced by the nature of the occupational role, social relationships and dynamics, and also by the circumstances leading up to and surrounding the point at which the decision is made. Other research supports the importance of organisational climate and financial incentives in influencing actions of the concerned stakeholders (Andon et al., 2018; Kumar et al., 2018; Murphy & Free, 2016).

The decision to undertake a criminal activity can be attributed to cost-benefit analysis (Becker, 1968). McCarthy et al. (2015) attempted to address the effect of the kind of financial benefits being offered. The authors found that the payoff to the launderer increases when his legal wage rate increases, when a criminal's legal wage rate decreases, and when the probability of detection increases.

The literature has also focused on actors responsible for curbing financial crimes such as money laundering. On analysing the extent of auditors' compliance concerning legislative changes in the United Kingdom's AML, Norton (2018) found the level of suspicious activity reporting by auditors to be relatively low in comparison with professionals from other sectors. He attributed it to having a standardised format for reporting suspicious activity and the nature of the occupation whereby adverse audit reports can result in auditors losing clients. While Liss and Sharman (2015) emphasised the growing importance of private actors to combat money

laundering through the concept of global governmentality, K. Murray (2018) and Howieson (2018) stressed the need to address wilful blindness and a lack of epistemic virtues in professionals' codes of conduct to minimise the opportunities for fraud and money laundering.

2.2.4 Magnitude of money laundering

Understanding the magnitude of any problem is a key aspect of solving it. In the case of money laundering, this would imply first determining its seriousness and its effect on the macroeconomy, and then evaluating the effectiveness of countermeasures over time. The same holds for money laundering. Researchers have long attempted to quantify the extent to which money is being laundered (Quirk, 1997; Tanzi, 1996). One of the most notable works in this area is by Walker (1999). The study presented what has come to be known as the "Walker model of global money laundering", and it relies upon a wide range of publicly available databases. The model suggested that the global amount of money subject to laundering was USD 2.85 billion per year in 1999 with the most flows in Europe and North America.

Numerous researchers have since focused on quantifying the amount of money being laundered and by what means (Ardizzi et al., 2014; Argentiero et al., 2008; Barone & Masciandaro, 2011; Barone & Schneider, 2018; Biagioli, 2008; Ferwerda et al., 2013; Hassan & Schneider, 2016a, 2016b; Medina & Schneider, 2018; Schneider, 2010; Schneider & Enste, 2000b; Schott, 2006; Unger, 2013; Unger & Hertog, 2012; Walker & Unger, 2009; Zdanowicz, 2004b, 2009). Researchers have used a variety of methods including case studies, proxy variables and economic models. Unger (2013) classified ways of measuring money laundering into two categories, namely, using proxies (such as GDP, world-wide proceeds of crime and balance of payments discrepancies) and through the use of economic models (such as the dynamic two-sector model and Walker-Gravity model).

Prominent Work	Key Objective	Key Findings
Walker (1999)	Develop a crime-economic model from public data to determine and monitor the size of global money laundering	• USD 2.85 billion is laundered globally per year • The United States was the most frequent origin and destination of laundered money
Argentiero et al. (2008)	Measure money laundering for the Italian economy	• Money laundering accounted for 12% of GDP • Money laundering is more volatile than GDP and is negatively correlated with it

Walker and Unger (2009)	Develop a model for measuring money laundering	• A gravity model was presented estimating the flows of illicit funds from and to each jurisdiction in the world
Zdanowicz (2009)	Measure, detect and monitor trade-based money laundering	• Anomalies were identified in trade transaction data which act as a mean of monitoring, detecting and prosecuting trade-based money-laundering activities • The variables considered were country, customs district, product and transaction price risk
Schneider (2010)	Estimate the turnover of organised crime from 1995 to 2006 for 20 OECD countries.	• Turnover of organised crime activities increased from USD 270 billion in 1995 to USD 614 billion in 2006
Barone and Masciandaro (2011)	Measure the role of money laundering in organised crime in the European legal economy through the measurement of ownership of legal assets	• Money laundering by criminals facilitates their investing cash in legal and illegal sectors • Money laundering to clean illicit funds in Eastern Europe resulted in legal assets amounting to 0.67% of EU GDP in 2009
Unger and Hertog (2012)	Determine whether money laundering has decreased over time	• There was no substantial decline in proceeds of crime and therefore no decline in money laundering • A combination of economic information and criminological data was proposed, to develop a new tool for identifying money laundering in sectors such as trade and real estate
Ferwerda et al. (2013)	Develop a model for trade-based money laundering	• Countries with strict AML regulation experience more trade-related money laundering
Unger (2013)	Determine whether money laundering has decreased over time	• Money laundering did not decrease over the last two decades • This was attributed to broadening of the concept of money laundering to include other predicate crimes such as tax evasion
Ardizzi et al. (2014)	Ascertain the proportion of cash from criminal activities deposited in financial institutions in Italy	• Dirty money accounted for 7.5% of GDP in North Italy and 5.1% of GDP in the South.
Collin (2019)	Summarise empirical work in area of illegal and harmful cross-border financial flows	• Literature on illicit financial flows (IFFs) can be categorised into methods of measuring IFFs, constructed risk indicators. and forensic studies that aim to uncover instances where illicit flows have occurred.

Table 4. Overview of research on the magnitude of money laundering

However, there exists a school of thought that criticises these estimates and deems them to be inaccurate and misleading in estimating the correct amount of funds being laundered (Levi & Reuter, 2006; Pol, 2018b; Reuter & Greenfield, 2001; Reuter & Truman, 2004; Thoumi, 2005). Unger (2013) attributed the lack of a precise estimate of the size of money laundering to the concealed nature of the underlying crime and the amount of proceeds generated.

2.2.5 New opportunities for money laundering

Speer (2000) deemed the threat of cybercrime to be substantial, and correctly predicted that it would grow with increases in knowledge about computers and other technologies. This new form of criminal activity mainly comprises a computer, a network and a human interface that allows the perpetrators to steal money using the network (Sood et al., 2013). Researchers have recently directed attention towards understanding the costs and proceeds of cybercrimes (Anderson et al., 2013; Levi et al., 2016; Levi et al., 2017; Schneider, 2017a, 2017b; Schneider & Linsbauer, 2016). With a rapid transformation in crimes, it becomes imperative to distinguish between new cybercrimes and those that are e-enabled. Cybercrimes by definition do not exist outside of the cyber domain; such effects as they may have spilling over are also relatively low. E-enabled crimes, on the other hand, are existing criminal acts that have flourished through easier use of technology (Burden & Palmer, 2003). Consequently, criminal activities such as hacking and malware attacks are examples of cybercrimes whereas activities such as money laundering and phishing are e-enabled crimes. The online platform is an enabling factor in overcoming the constraints of a social network such as geographical or social barriers, and it facilitates collaboration with perpetrators across the globe, substantially increasing the opportunity to commit illicit acts (Leukfeldt, 2014).

There has also been growth in the literature based on the new opportunities for illicit money-laundering activities. These have come about because of rapid advances in technology. Barone and Schneider (2018) view as a growing threat cyberlaundering and money laundering accomplished through the use of automatic electronic devices.

Irwin et al. (2012) proposed that an understanding of the modus operandi for money laundering and terror financing could be used to develop typologies for the virtual world. Further, Richet (2013) made use of an online ethnography approach to determine new cyber-

methods for laundering funds. He found two fundamental forces providing opportunities for money laundering: online gaming, and micro-laundering, which involves moving a small amount of funds over a large number of transactions. He concluded that traditional methods of laundering funds have evolved through the online medium and an understanding of the modus operandi of such new methods would enable better detection. It has led to some work being undertaken to monitor new opportunities that may have become available to launder funds.

By analysing E-Gold and Liberty Reserve fraud cases, Stuhlmiller (2013) found that the anonymity of virtual currency transactions and lack of regulatory oversight were prominent catalysts for their use as new laundering methods. On the contrary, Dostov and Shust (2014), on investigating cryptocurrencies such as Digicash and Bitcoin and the threats they pose in money laundering and financing of terrorism, found that the feature of anonymity is unlikely to make them popular among its users. According to them, cryptocurrencies have limitations in terms of negotiability, risk and the need for specialised training. In other words, as there is no universal acceptability for cryptocurrencies, the need to exchange them for fiat money arises at some point. Secondly, cryptocurrencies such as Bitcoins are unequally distributed and are highly volatile, which makes them unattractive. Dostov and Shust also stressed the importance of examining each cryptocurrency and its characteristics separately to develop an appropriate regulatory framework. The need to have a regulatory framework in place to combat the threats posed by cryptocurrencies towards money laundering and financing of terrorism is supported by Choo (2015).

To address the problem of anonymity and untraceable nature of cryptocurrency transactions, Turner and Irwin (2018) attempted to de-anonymise Bitcoin transactions using a variety of software tools. The authors found that while it was possible to follow a transaction across the blockchain, the anonymity feature inherent in the system was not overcome. The technological innovations have paved new ways to perpetuate organised crimes. Silk Road is one such example that has drawn attention from academics and enforcement agencies alike (Barratt, 2012; Bright et al., 2012; Christin, 2012; Hout & Bingham, 2013).

2.2.6 Detection of money laundering

With the growing focus on illicit activities, the academic literature has emphasised coming up with a wide variety of automated detection systems to detect such illicit activities (Baader & Krcmar, 2018; Battaglia et al., 2018; Chang et al., 2008; Gepp, 2015, 2016; Gepp et al., 2018; Khaled et al., 2018; Ngai et al., 2011; Perols, 2011b; Phua et al., 2010; Ravenda

et al., 2015; Sahin et al., 2013; Singh & Best, 2019; Song et al., 2014; Van Vlasselaer et al., 2017; Wedge et al., 2017). As per Ngai et al. (2011), although the application of data mining techniques has been extended towards the detection of insurance fraud, there existed a distinct lack of research on mortgage fraud, money laundering and securities and commodities fraud.

Since then researchers have investigated both machine-learning and traditional statistical approaches to detect money laundering (Bidabad, 2017; Chang et al., 2008; Colladon & Remondi, 2017; Deng et al., 2009; Drezewski et al., 2012; Gao, 2009; Gao & Ye, 2007; Gilmour, 2017; Irwin et al., 2012; Ju & Zheng, 2009; Ngai et al., 2011; Perols, 2011b; Regan et al., 2017; Savage, 2017; Savage et al., 2016; Turner & Irwin, 2018; Unger et al., 2011; Wang et al., 2007; Zdanowicz, 2004a, 2009; Zhang et al., 2003). Zhang et al. (2003) on using the Link Discovery method based on Correlation Analysis (LDCA) suggested that the possibility of being associated with a money-laundering scheme would depend upon the correlation between financial transaction patterns of two persons. Zdanowicz (2004a, 2009) proposed the use of statistical analysis to monitor and detect trade-based money laundering. He extended upon the already-existing empirical evidence of trade-based money laundering to be found in academic and professional literature. He stated that detection of trade-price manipulations by identifying anomalies in trade data might help in detecting money laundering of funds derived from activities such as for financing the acts of terrorism, tax avoidance or evasion, dumping of goods, concealment of illegal commission and so forth, by focusing on country, customs district, product and transaction price risk characteristics.

Chang et al. (2008) highlighted the use of a set of coordinated visualisations based upon keywords identification in wire transactions to detect fraudulent transactions. The authors on depicting the relationship between keywords and accounts over time were able to detect transactions and accounts exhibiting suspicious behaviours. Similarly, Deng et al. (2009) came up with an active learning sequential design (ALSD) approach to detect instances of money laundering. The study was motivated by the need to identify and prioritise relevant suspicious transactions among the large volume of financial transactions that occur daily. The idea was to help investigators focus attention and direct resources to accounts which are suspicious and improve money-laundering detection with minimal time and effort. The authors found the model to outperform stochastic approximations in detecting money-laundering transactions. Savage et al. (2016) presented a system for detection of money-laundering activities through the use of a combination of network analysis and supervised learning. The authors on using the

system on real-world data found that the system was able to detect suspicious activity with a low rate of false positives.

Prominent Work	Key Objective	Key Findings
Gao et al. (2007)	Develop a framework for data-mining based on AML research	• Pattern discovery techniques can deal with complex non-numeric evidence and involve structured objects, text and a variety of discrete and continuous data • Link discovery, social network analysis and graph theory can be used as money-laundering detection tools
Deng et al. (2009)	Develop an active learning sequential design approach (ALSD) to detect money-laundering transactions	• The model outperformed stochastic approximations in detecting money-laundering transactions.
Ngai et al. (2011)	Review literature about using data mining to detect money laundering	• A distinct lack of research exists on mortgage fraud and money laundering
Ravenda et al. (2015)	Develop a model for detecting legally registered mafia firms	• The developed model correctly classified 76.41% of firms within a matched sample of 853 firm-year observations.
Wedge et al. (2017)	Use an automated approach to reduce false positives in fraud detection.	• False positives could be reduced by 54% on holdout data of 1.852 million transactions
Van Vlasselaer et al. (2017)	Examine the effect of network information for social security fraud detection	• Domain-driven network variables have a substantial effect on fraud detection • Improves rate of fraudulent detection by 55%
Baader et al. (2018)	Determine whether a combination of red flags and process mining techniques reduces false positives in fraud detection	• The authors found the false positive rate to be 0.37%, which was lower than rates reported in other research
Singh and Best (2019)	Use visualisation techniques to efficiently identify patterns of money laundering	• Banking transactions can be visualised using link analysis • Subtle indications of suspicious behaviour were identified; for example, transactions of more than $10,000, and multiple transactions below $10,000

Table 5. Overview of research on the detection of money laundering and other illicit activities

Overall, the literature has focused on attempting to detect money laundering being undertaken through the use of real estate, international trade and high-value portable goods

among others as exhibited by Figure 3. Ferwerda et al. (2013); Zdanowicz (2009) and Unger (2013) directed attention towards the detection of money laundering being undertaken through real estate and trade. Turner and Irwin (2018) found technological innovations such as bitcoin provided opportunities to launder money and suggested means of detection. Gilmour (2017) studied the use of high-value portable commodities being used to launder funds in the United Kingdom and abroad. Bidabad (2017) suggested mechanisms to detect money laundering being undertaken through the use of banking transactions.

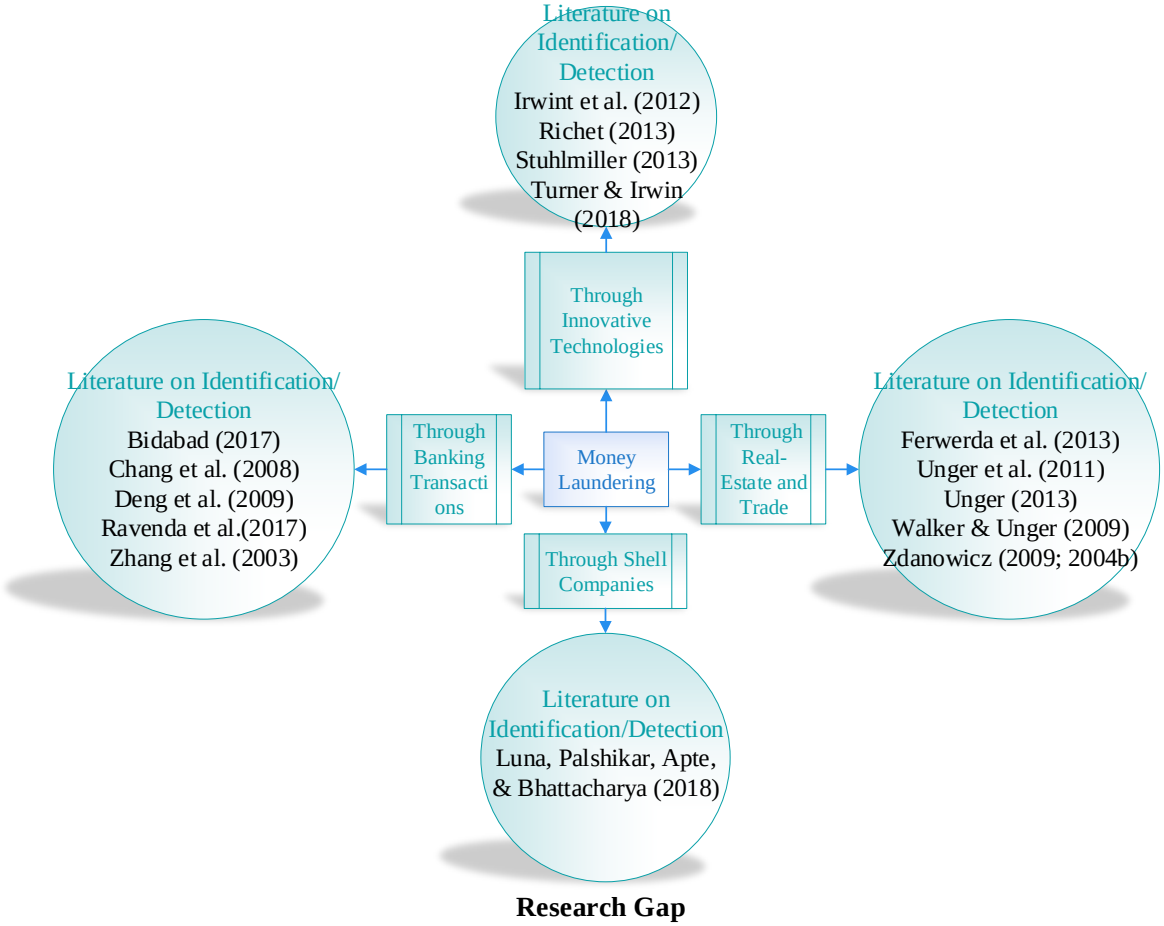

Figure 3: Literature on detection of money laundering

However, the detection of money laundering through shell companies has received limited attention. In other words, attempts are in the nascent stage towards identifying shell companies being used for illicit activities such as bribery, corruption and money laundering. The next sub-section will provide an overview of shell companies and the limited work that has been undertaken concerning them.

2.3 Review of literature around shell companies

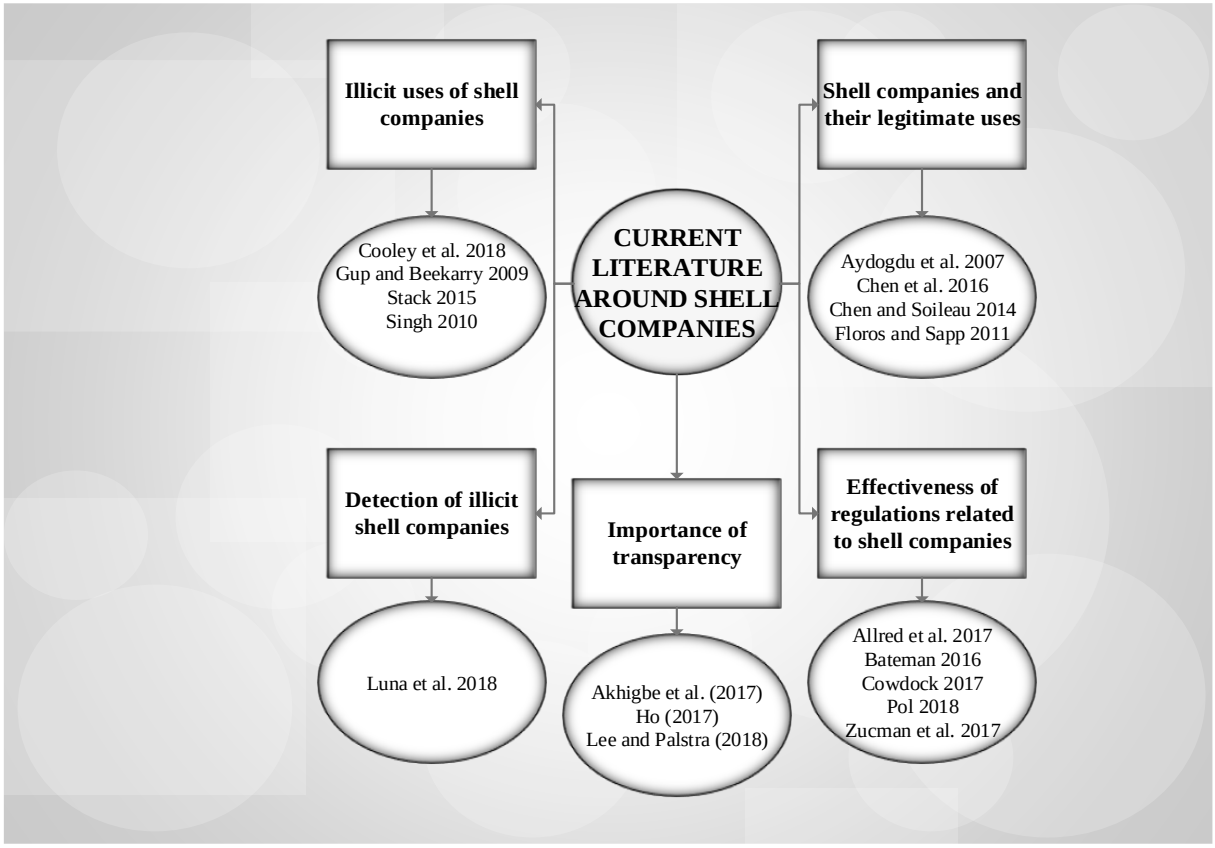

Figure 4: Current literature around shell companies

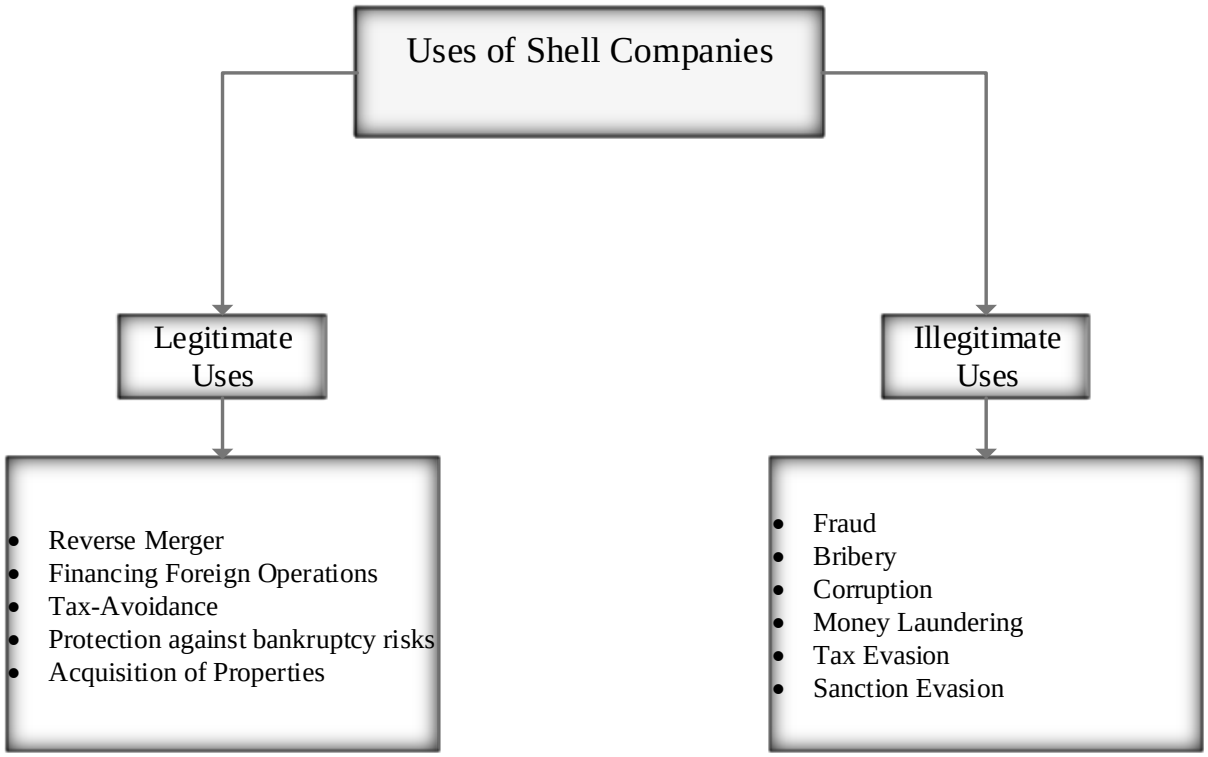

Figure 5: Uses of shell companies

A review of the literature on shell companies led to classification into five broad categories as exhibited in Figure 4: namely, shell companies and its legitimate uses; illicit uses of shell companies (as exhibited in Figure 5); the effectiveness of regulations related to shell companies; the importance of transparency; and the detection of illicit shell companies. The following sub-sections provide a brief overview through key papers in each of these categories.

2.3.1 Shell companies and their legitimate uses

Shell Companies, also known as front companies or anonymous companies, are entities with no to minimal operations and assets, and generally do not exhibit a physical presence. Private companies to become publicly listed may use shell companies (Aydogdu et al., 2007). According to Floros and Sapp (2011), the purpose of shell firms may range from gaining a tax advantage, avoiding legal liability, facilitating collection of income from patents and other such intangible assets, but the majority of these entities aim to be acquired or merge with another firm.

The use of publicly-listed shell companies by private companies to go public is called reverse mergers. A substantial amount of literature exists examining the use of shell companies for reverse mergers, and the benefits as well as the associated disadvantages (Aydogdu et al.,

2007; Chen et al., 2016; Chen & Soileau, 2014; Floros & Sapp, 2011; Gleason et al., 2005; Lee et al., 2015; Poulsen & Stegemoller, 2008; Semenenko, 2011; Sjostrom, 2008).

Prominent Work	Key Objective	Key Findings
Gleason et al. (2005)	Examine reverse takeovers to determine the generation of long-term wealth	• A small improvement in operations and profitability was found after reverse takeover; only 46% of the sample survived for two years • Reverse takeovers may provide an alternative means of going public, but are often risky and may fail to generate long-term wealth
Sjostrom (2008)	Examine reverse mergers as a method of going public	• Reverse mergers are often termed cheaper and quicker than traditional initial public offers, but this is not the case for many companies
Floros and Sapp (2011)	Investigate the value of shell companies for private firms	• The performance of shell companies is irrelevant to a private firm. They seek a shell company with a clean history and a quick path to a merger • The expected reward to investors from a shell reverse merger is justified by the growth of shell firms for a reverse merger
Chen and Soileau (2014)	Examine the earnings quality of US domestic firms that access capital markets via a reverse merger compared to those via initial public offers	• Reverse merger firms have lower earnings quality compared to US initial public offer firms • Investors, regulators, auditors and other stakeholders should consider the method that firms use to access capital markets in their investment decision-making process
Lee et al. (2015)	Compare the after-merger performance of Chinese reverse mergers with control firms rather than initial public offer firms	• Chinese reverse mergers outperformed control firms • Chinese reverse mergers are not toxic investments

Table 6. Overview of research on shell companies and their legitimate uses

Aydogdu et al. (2007) deemed reverse mergers efficient and cost-effective as several requirements associated with an Initial Public Offering (IPO) can be avoided. They examined the trading activity around reverse mergers to search for market-wide stock price manipulation and did not find any evidence of such manipulation. They observed that merger announcements

are considered positive as reflected by increasing stock prices and statistically significant positive returns. However, the results were inconclusive as to whether reverse mergers are value-increasing events for shell companies.

Chen and Soileau (2014), on comparing the earnings quality of US-based domestic firms, extended the literature on reverse mergers by finding that reverse-merger firms had lower earnings quality compared with IPO firms during the period from 1997 to 2011. Lee et al. (2015) added to the knowledge of performance, financial health, benefits and disadvantages of reverse mergers by comparing the after-merger return performance of US control firms with that of Chinese reverse mergers.

2.3.2 Illicit uses of shell companies

Apart from being used in reverse mergers, shell companies are used as holding companies or for protecting small entrepreneurs from bankruptcy risks. They are also referred to as fictitious entities, sham companies, front companies, pass-throughs and anonymous companies, and are often used for a wide range of illicit activities such as bribery, corruption, financial statement fraud, tax evasion, terrorist financing, money laundering, sanction evasion and cybercrimes (Findley et al., 2013; Hubbs, 2018). The literature, both professional and academic, available on shell companies has focused on its illicit uses (Cooley et al., 2018; Cowdock, 2017; Does de Willebois et al., 2011; Findley et al., 2013, 2015; Gup & Beekarry, 2009; Harding, 2016; Hubbs, 2018; Jancsics, 2017; Stack, 2015b, 2015c).

Prominent Work	Key Objective	Key Findings
Christensen (2011)	Investigate the role of tax havens in facilitating offshore shell companies used to hide and disguise illicit financial flows	• Tax havens have become a prominent part of globalised capital markets, and their activities create a criminal environment where illicit financial flows can be disguised as legitimate transactions
Stack (2015b)	Examine the role of shell companies in Ukraine in facilitating tax evasion and corruption	• Shell companies generate a considerable international flow of dirty money and within Ukraine as well. State actors utilise these organisations.
Jancsics (2017)	Provide an insight into the use of corporate vehicles by corrupt officials in Hungary	• Shell companies were used by public officials either to distribute resources or create assets that could be sold for profit

Alstadsæter et al. (2018)	Determine the amount of wealth owned by each country in offshore tax havens	• The equivalent of 10% of world GDP is held in tax havens • Most of Russia's wealth is held offshore

Table 7. Overview of research on illicit uses of shell companies

Gup and Beekarry (2009) analysed the characteristics of limited liability companies and the extent to which they pose a threat to money laundering and terror financing. The characteristic traits of these entities such as secrecy, flexibility, low cost of incorporation and compliance requirements made them an attractive tool for illicit actors. This study found that LLCs provide opportunities for tax evasion, regulatory evasion, money laundering, and financing acts of terrorism. The authors suggested the need to focus on due-diligence requirements and increasing transparency.

Additionally, they point out the limitations of FATF recommendations concerning anonymous entities which are limited to identification of the beneficial owner. The authors suggest adoption of a proactive approach towards those responsible for the incorporation of such entities; they also favour the employment of professionals. Singh (2010), using a case study analysis, attempted to identify the attributes of shell companies in India and made recommendations for Indian regulatory authorities. He observed that these entities were used for rotation and siphoning of funds, creation of equity in their names, and for holding real estate. Similarly, Does de Willebois et al. (2011) point towards the use of legal structures in the United Kingdom to accomplish such illicit activities. On observing one hundred and fifty cases of large-scale corruption, they found that many involved the use of shell companies to hide illicit wealth.

Stack (2015c) analysed the role of shell companies in Latvian-type correspondent banking and resulting money laundering operations. He examined financial flows from Russia and the former Soviet Union, and highlighted the use of shell companies in the movement of funds from those associated with corruption and organised crime. He found that these entities moved funds from Russia, Ukraine and other Soviet countries through international correspondent banking relations to offshore savings accounts and business suppliers. Jancsics (2017) added to this discussion by describing how corrupt public officials use corporate vehicles in Hungary. The study aimed at understanding the reasons for using shell companies in fraudulent transactions, identifying the sectors in which these entities are most frequently used, the actors responsible for interaction through these entities, and the political and social

context for their existence. He found that all the reported cases of corruption were related to public policy decisions and involved shell companies. They were used mainly in the tobacco and agricultural sector with the objective of distribution of resources for client-building or for market capture.

The intensive use of shell companies for illicit purposes by a wide range of users was highlighted in the report known as the Panama Papers by the International Consortium of Investigative Journalists (Harding, 2016; Obermayer et al., 2016). Similarly, Cooley et al. (2018) detail various instances of how shell companies have been used by kleptocrats to launder funds.

The literature has also emphasised the critical role that offshore centres and tax havens have played in the growth of shell companies (Alstadsæter et al., 2018; Christensen, 2011, 2012; Picard & Pieretti, 2011; Sikka & Willmott, 2010; Stack, 2015a, 2015b, 2015c; Zucman et al., 2015). Sikka and Willmott (2010) examined the role of tax havens and shell companies to evade taxes. The authors observed that 26 percent of assets and 31 percent of net profits of American multinational corporations were in tax havens, and over three thousand major US companies were sheltering in the US Virgin Islands and Barbados alone. The authors found that entities would sell their products to trading subsidiaries at below-market prices, which in turn would sell the products to end customers at market prices and pocket the difference. The trade subsidiaries located in tax havens were generally shell companies.

Similarly, Christensen (2011, 2012) and Harding (2016) highlighted the role of tax havens in facilitating shell companies to hide and disguise illicit financial flows and beneficial ownership, thus aiding in corruption. Zucman et al. (2015) highlighted that shell company and offshore accounts allow the rich to invest at home and abroad under a shroud of anonymity, thus facilitating evasion of taxes. According to Alstadsæter et al. (2018), ten percent of the total world's Gross Domestic Product (GDP) is held in tax havens with most of this being held in the British Virgin Islands, Panama and other such tax havens where the wealth is held mainly in shell corporations.

2.3.3 Effectiveness of regulations related to shell companies

The possible damage associated with the use of shell companies comprises financial losses, both direct and indirect, reputational damage, loss of operations and the possibility of lawsuits. Consequently, the use of these entities should be of immense concern to legal and

compliance professionals, business partners and agents, wholesalers, customers, government operatives (especially tax officials), anti-corruption non-governmental organisations (NGOs hereafter), and so forth. The scholarly attention received has resulted in suggestions and recommendations being made as well as the reasons being identified for the failure to combat this growing problem (Allred et al., 2017; Bateman, 2016; Cowdock, 2017; Does de Willebois et al., 2011; Findley et al., 2013, 2015; Gilbert & Sharman, 2016; Gup & Beekarry, 2009; Ho, 2017; Hubbs, 2018; Jancsics, 2017; Lee & Palstra, 2018; D. Murray, 2018; Niels & Gabriel, 2014; Pol, 2018a, 2018b; Sharman, 2012, 2013; Vail, 2018; Vaughan, 2018; Zucman et al., 2015).

Bateman (2016) emphasised the need to have a legal framework for regulating shell companies. Efforts have been made to increase the transparency of such entities by providing beneficial ownership information to prevent them from being used for money laundering, corruption, bribery, terrorism financing and other such crimes. The FATF, the international institution responsible for overseeing corporate transparency, and the G20 have continuously urged countries to implement standards for regulating beneficial ownership information to increase trust in businesses, improve corporate accountability and to facilitate successful combatting of illicit practices (Ho, 2017). Similarly, Vail (2018) emphasised the need to have transparent beneficial owner information, a shared beneficial owner registry and the ways to accomplish it. However, despite the emphasis placed on transparency through international standards and recommendations, the incidence of non-compliance highlights the failure of policymakers and scholars to assess the effectiveness of policies. They tend not to consider the countervailing pressures that are faced by democratic governments as they attempt to tackle the problems of corruption; at times, these pressures may be related to personal benefit or electoral incentives.

Sharman (2012) stated that shell companies that cannot be traced to real owners act as a corporate veil to conceal the proceeds of crime and corruption. The emphasis on corporate transparency would facilitate law enforcement agents to catch wrongdoers. As per Sharman (2012), the information on beneficial owners could be accessed in two ways. First, the corporate registry is required to collect and hold information with proofs about the identities of beneficial owners. Another way is to regulate the company service providers (CSPs hereafter) who could collect information about the beneficial owners of entities and provide it to regulators upon request. The CSPs may be individuals, law firms or other firms with the sole purpose of incorporating companies. They may be present in an OECD country, tax haven or

a developing country and take care of the formalities required for establishing a company on behalf of a client, the beneficial owner (Sharman, 2013). There do exist international regulations such as the FATF guidelines to prevent the use of legal entities for hiding and transferring the proceeds of crime and corruption by regulating licensing of CSPs, subjecting them to a legal duty of collecting, holding and verifying identification data and imposing penalties on failure to do so (FATF, 2012). However, as Sharman (2012) points out, it is costly to ensure enforcement of international standards. Additionally, there is a lack of resources in maintaining access to beneficial ownership information.

The efforts and resources directed towards fighting money laundering and corruption are linked with restrictions placed on the formation of anonymous companies. The more restrictions there are on forming these, the more need there will be for directing resources. Findley et al. (2013) examined the effectiveness of regulations restricting the formulation of anonymous companies. The study was motivated by concerns surrounding the effectiveness of these restrictions because of different geographical locations of illicit actors and the legal domicile of CSPs. They found non-compliance with international standards requiring CSPs to obtain documentation identifying the beneficial owners. Anonymous companies were still being created and the presence of international standards did not increase compliance rates.

Findley et al. (2015) extended their previous study and found evidence that contradicts the common notion that OECD countries are compliant with international standards while developing countries are unable to comply and tax havens are unwilling to comply. Overall, raising the standards of international law, in terms of strict regulations to comply with, was found to have no significant effect, with material self-interest remaining a powerful compulsion to violate international standards. Allred et al. (2017) extended this research stream further with a focus on corporate governance and its execution. They found that country-level compliance with international standards is not an indicator of firm-level compliance, and this is consistent with Findley et al. (2015).

Motivated by the tendency of the world literature to have an overstated notion of compliance with international standards, Gilbert and Sharman (2016) shifted the focus of compliance away from firms and over to states and governments. The objective was to determine whether democracies would comply with international standards prohibiting foreign bribery. The study employed process-tracing case studies of British Aerospace, the Australian Wheat Board and the Reserve Bank of Australia and found evidence of wilful blindness by

Australian and British governments concerning the violation of the OECD Anti-Bribery Convention. The failure of democratic governments to investigate the crimes of their respective corporate citizens suggests a disinclination towards compliance rather than a lack of ability. Gilbert and Sharman also point to the need to better protect and encourage whistle-blowers, anti-corruption NGOs and investigative journalists. Similarly, Jancsics (2017) provides explanations for the failure of conventional anti-corruption policies against shell companies in Central Europe, thereby further highlighting the fact that compliance frameworks alone are not enough. Among other findings, he contended that actors do not rationally evaluate the possible outcome of their behaviour and so a stricter criminal code or stronger law enforcement may be ineffective. He also concluded that trusted individuals control domestic shell companies, and there is no formal relationship or contract between the fake and real owners and thus even accurate and updated corporate registries will fail to reveal such connections.

2.3.4 Importance of transparency

The relationship between transparency and financial performance has been documented in the literature. Akhigbe et al. (2017) observed transparency having a positive effect on the financial performance of banks. Despite evidence of public and private actors' non-compliance and failure to implement regulations and recommended standards, efforts have been made by regulatory authorities and law-enforcement agencies to increase the transparency of beneficial ownership, on account of the widely accepted notion that greater transparency would facilitate prevention and detection of unlawful activities. With the Persons with Significant Control (PSC) regulations, the United Kingdom was the pioneer in making information available about the ultimate owners of a company in the corporate registry. Ho (2017) provided a brief background of the UK regulations and evaluated the implementation of similar regulation in Hong Kong. The idea behind PSC regulations in the UK was to tackle tax evasion, corporate misconduct and other illicit activities. Instead of legal persons, the focus was on natural persons who own and take advantage of assets of a legal person and exercise control or influence. However, the regulations did not apply to all entities. The entities with voting shares listed on stock markets in the US, UK, Switzerland, Japan and other European Economic Area (EEA) were exempted.

Lee and Palstra (2018) conducted a study to evaluate the effectiveness of the United Kingdom's ownership register and highlight issues in ensuring the quality and compliance of data. They analysed over ten million records of data on PSCs from the UK Companies House

and documented the limitations of the regulation, the lack of data validation and verification, the poor quality of data on the corporate registry, and prevailing trends which could attract further analysis. Methods used to hide the real owners included filing a statement that the company had no owners, using an ineligible foreign company as the beneficial owner and using nominees or a circular ownership structure. The efforts directed to combat the problem associated with shell companies have been towards increasing transparency. It is essential to understand that achieving transparency should be one of the objectives and not the ultimate goal for preventing shell companies from being misused. Having a global, transparent governance regime is theoretically desirable, but the regulation required to apply it in practice could be at best challenging and possibly more damaging than helpful. Balakina et al. (2017) point out that the demand and supply for tax and financial havens exist because of the need for banking secrecy. Hence, implementing a transparent regime in one jurisdiction is likely to create a demand for secrecy and consequently reduced transparency in another jurisdiction.

The existing literature on shell companies is focused on regulations related to international standards aiming to achieve transparency and their implementation, as well as the regulation of CSPs. The opportunity lies in using a more innovative approach in combatting the hiding and laundering of illicit proceeds rather than focusing on improving the regulations.

2.3.5 Detection of illicit shell companies

It is a new research stream. The only study identified to have taken a step in this direction was by Luna et al. (2018). The lack of accessible real banking transaction data prompted the authors to develop a banking transaction simulator for shell and regular companies. The banking transaction simulator worked on multiple parameters affecting a company's banking activities such as the industry sector, annual revenue category, and the number of employees, suppliers and utilities. Simulated incoming and outgoing transactions were analysed to look for patterns to help determine whether a bank account belongs to a shell company, or not. Each account was summarised by a set of features derived from the nature and timing of the money flows. Anomaly detection techniques were then used to detect variation between expected and observed business transaction profiles of regular and shell companies. The rationale was to identify shell companies that could be investigated further for any illicit activity. However, the model focused only on banking transactions and therefore did not make use of publicly available information such as the number of directors and their backgrounds, and whether transactions were made to tax havens or countries with a weak banking regime. There is a need

for further research to analyse a dataset comprising real shell companies involved in illicit activities. There is also an opportunity to incorporate publicly available information in the detection of shell companies, thus avoiding the reliance upon the availability of banking transactions data.

2.3.6 Identification of research gap

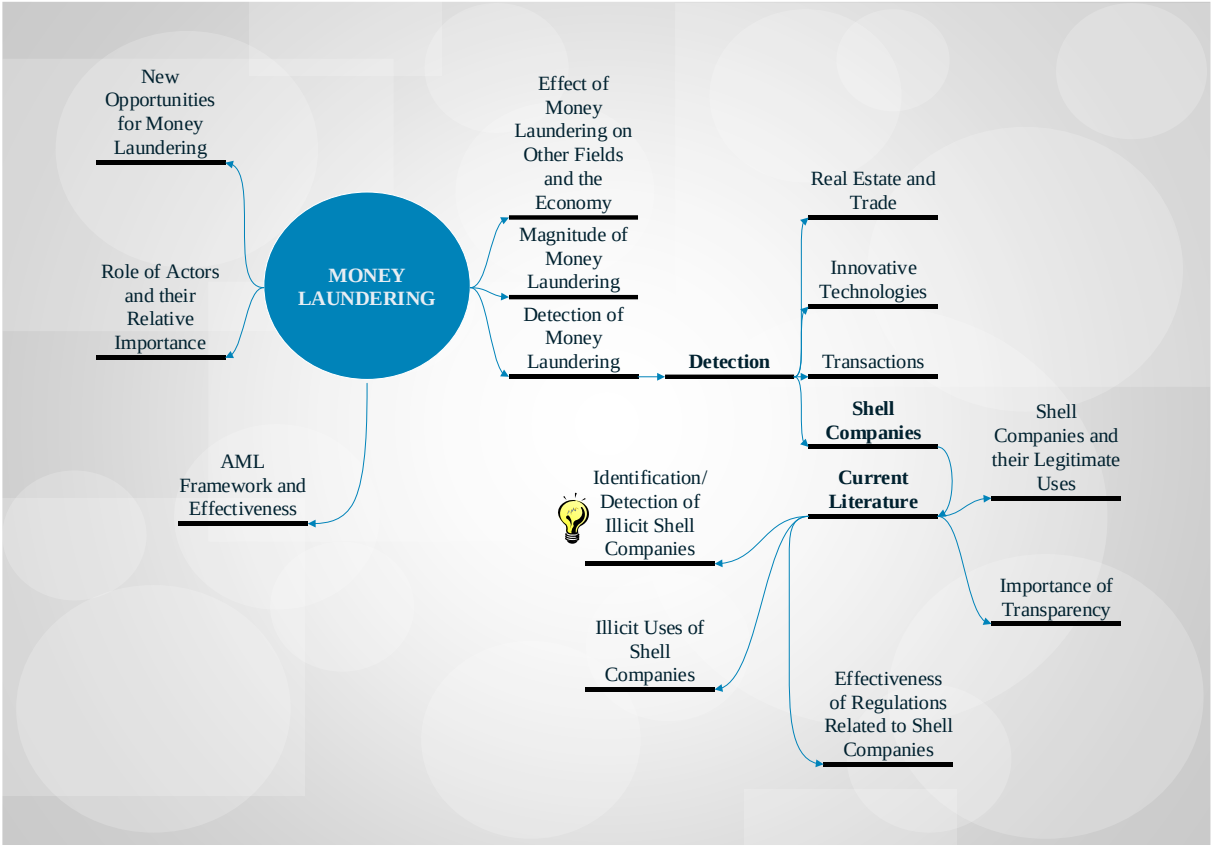

Figure 6: Framework for identification of research gap

A typology on money laundering literature has been formulated, as depicted in Figure 6. A review of the current literature led to the identification of money laundering and shell companies as an essential area that is currently under-researched. The existing research on money laundering has focused on the:

- AML framework and its effectiveness: Researchers have critiqued the existing AML regime and drawn attention to its effectiveness;
- Effect of money laundering on other fields and the economy: Prior research has investigated the effects of money laundering on the economy and its relationship with other fields such as accounting;

- Role of actors and their relative importance: Researchers have also examined the role of actors, such as accountants and auditors in undertaking money laundering and their respective importance;
- Magnitude of money laundering: In order to establish the gravity of the problem, researchers have made efforts to quantify the amounts of money being laundered globally;
- New opportunities for money laundering: The technological and regulatory changes have also motivated works that highlight the new technology-enabled methods of laundering funds;
- Detection of money laundering: There also exists some research directed towards the methods used to detect money laundering;

The detection process has been further categorised into four broad groups – the detection of money laundering through (i) banking transactions, (ii) real estate and trade, (iii) innovative technologies and (iv) shell companies. It was further identified that the detection of money laundering through shell companies had received limited attention. The existing literature on shell companies is focused on regulations related to international standards aiming to achieve transparency and their implementation, as well as regulation of CSPs.

The rise in financial crimes has led to a wide range of regulatory reforms to combat the problem. The debate over the effectiveness of regulations to accomplish the desired objectives has brought the regulators under pressure to justify their actions considering political, executive and judicial scrutiny. It has eventually led to risk colonisation, that is, risk playing an imperative role in defining the aspects, methods and rationale for regulations (Rothstein et al., 2006). However, instances of regulatory failures have raised the question as to whether the regulatory strategies can be adjusted to the dynamics of real life to combat the problem. The present situation and circumstances lay down the need for highly responsive regulation through a combination of various regulatory instruments to address the problem (Black & Baldwin, 2010). The attempts that have been made to identify shell companies being used for illicit activities such as bribery, corruption, money laundering, tax evasion and other such illicit activities are in a nascent stage because of the importance placed on making regulatory changes. However, the need for combining risk-based assessment with compliance-based assessment can act as an essential tool in the fight against financial crime. The development of a model to detect illicit shell companies being used to carry out illicit activities would aid in

contributing to the development of a “really-responsive” regulatory framework by improving the performance of regulatory tasks. The different regulatory tasks encompass detection of a non-compliant behaviour followed by a response to such behaviour through the development of tools and strategies, their enforcement, and the assessment of their success or failures, and then modifying them accordingly (Baldwin & Black, 2008). The detection of shell companies being used for illicit activities would assist combatting the active use of shell companies to accomplish laundromat schemes such as the Russian Laundromat and Azerbaijani Laundromat. The motivation lies in developing an approach to detect the entities used for hiding and laundering of illicit proceeds, rather than focusing on improving the regulations.

The research conducted in the past on shell companies and characteristics identified for detecting shell companies involved in illicit activities has been qualitative. A quantitative analysis would be complicated given the limited and inherently concealed data on shell companies, but it would help uncover patterns among connected networks of companies identified in money-laundering cases of the past, to develop strategies for their timely detection. Consequently, an approach to detect illicit shell companies through a quantitative framework by using traditional statistical and machine-learning approaches to develop a model would be a value-addition in the enhancement of regulatory effectiveness. Such a model based on publicly available information could act as the first line of defence for law-enforcement agencies to guard the wider public and economy against the harmful effects of illicit shell companies. The authors join the call of Dunstan and Gepp (2018) who direct attention towards the use of Big Data applications to analyse data for developing models for detection and prediction of misconduct. The technological advancements have paved the way for exploring relational inductive biases within deep learning architectures to facilitate insights into entities and for producing structured behaviours (Battaglia et al., 2018) which were not possible in the past, and hence taking advantage of such technological advancements could add to the breadth and depth of work on shell companies and the overall money-laundering literature.

2.4 Conclusion

The chapter highlights the gap in the existing literature and lays down the foundation for the need to develop strategies for the detection of such illicit shell companies. The review highlights additional opportunities for exploring the effectiveness of the AML regime and the steps that could be taken to make it useful in accomplishing the desired goals and objectives,

rather than being a mere tool of compliance. The debate around quantifying the magnitude of the problem of money laundering and the lack of consensus around its measurement is again brought to light through the current study. Thus, there still exists an opportunity for researchers to quantify the magnitude more accurately. The review on evaluating the new opportunities for money laundering through the use of innovative technology, consistent with Martin (2014), directs attention towards the transformation of drug distribution through online portals and the need for a potential paradigm shift in the global war on drugs, which at present has been costly and ineffective. For instance, an examination of the operations of Silk Road and drawing comparisons with conventional drug distribution networks led to the conclusion that cybercrime typologies do not reflect the complexities associated with Silk Road as they treat activities on it as a single act rather than numerous offences linked by a common purpose (Martin, 2014). This sets the tone for further research work to be carried out in the area of money laundering, which is currently doing substantial damage to economies all over the globe.

The review of existing literature identified various techniques available to launder funds. However, there seems to be a lack of research on the factors leading to a choice of technique adopted by a launderer. The next chapter extends the literature by synthesising existing work to develop a framework to provide insights into the techniques a launderer may adopt to launder funds. Such a framework may enable relevant practitioners and experts to be proactive in exercising professional judgement to come up with a suitable detection mechanism.

Chapter 3 Money-Laundering Framework

This chapter is based on a paper under submission to a peer-reviewed journal, namely: Tiwari, M., Gepp, A., & Kumar, K. (2021). Factors influencing the choice of technique to launder funds: The APPT Frameworks. (*Submitted for review: Crime Science) (Rank: Q1)*

The review of money-laundering literature highlighted aspects such as regulatory frameworks, the stages of money laundering, and ways of detecting it; however, there is a lack of understanding about the reasons underlying a launderer's choice of techniques. This chapter addresses that need by developing a new framework to provide insights into the techniques a launderer may adopt to wash funds among a range of available options. It is developed by drawing on existing literature and theories. The new APPT framework is named according to four factors that play a role in explaining the choice of techniques: the Actors involved, Predicate crime, the Purpose for laundering, and Technological innovations. The new APPT framework could be of use to practitioners in investigations, forensic accounting education and future research by incorporating the need to respond to changing circumstances surrounding the money launderer.

3.1 Introduction

Money laundering has received substantial research attention and has even been described as the mother of all crimes (Castells, 2011). The International Monetary Fund (IMF) estimated the level of money laundering to be between two percent and five percent of the world's gross domestic product (FATF, 2012). Money laundering is a further threat to the global economy as laundered funds may be used to finance other crimes (Rusanov & Pudovochkin, 2018). Such opportunities lead to economic distortions, erosion of financial sectors, reduced government revenues, and other socioeconomic effects (Barone et al., 2018, Bhattacharjee, 2020, Degryse et al., 2019, Walker and Unger, 2009).

Money laundering typically occurs after other illicit activities such as drug-trafficking, robberies, smuggling, tax evasion, terrorism, bootlegging, art theft, vehicle theft, and fraud (Mitchell et al., 1998a, 1998b). Efforts are made to disguise the nature and origin of the illicit income and to integrate it into the financial system without drawing attention from tax authorities and law enforcement (Compin, 2008). Money laundering has often been considered a varied and flexible process (Bichler et al., 2017b), which demonstrates the importance of practitioners such as investigators and forensic accountants in uncovering money laundering. Tiwari et al. (2020) reviewed the money-laundering literature and categorized it into having six themes: an anti-money laundering (AML) framework, economic effects, the key actors involved, the magnitude of the problem, new opportunities and the detection of money laundering. Notably, their review did not find a framework to explain a launderer's choice of techniques. Among a range of aspects related to money laundering, the techniques to launder funds have also been discussed in the literature (Unger & Hertog, 2012). Commonly identified techniques include the electronic transfer of funds, correspondent banking, structuring, casinos, real estate, prepaid cards, online banking, shell companies, and trusts. The complexity may vary depending upon the situation, with new techniques being created in response to changes in technology and government regulations (Gilmour, 2016b). However, no attempt is made in the literature to explain a launderer's choice of technique.

Gilmour (2016b) uses rational choice theory to suggest that money laundering is a risk-diversification process involving rational decisions by launderers who make decisions based on personal preferences and circumstances. However, Gilmour did not specify the nature of these preferences or circumstances. Consequently, it would be valuable to have a framework for money laundering that incorporates the interaction between critical factors to explain the

choice of techniques adopted to launder funds. This aligns with the views of Cornish and Clarke (1987) and Marteache et al. (2015) who state that the characteristics of offences provide a basis for selecting among alternative courses of action and this eventually influences an offender's choice. The result will be an improved understanding which may aid in the detection, and subsequent deterrence, of money-laundering schemes.

In response to the gap identified in the literature, this chapter develops the new APPT framework of money laundering to explain the factors influencing the choice of techniques adopted to launder funds. The rational decision-making of a money launderer can be explained through the concepts in systems theory, especially structural coupling, which acknowledges the codependency between factors in a system (Luhmann et al., 2013; Maturana & Varela, 1987). In this context, the factors influencing the choice of laundering technique are interrelated, such as the purpose for laundering of funds, the level of reliance on technological innovation, and personnel used to accomplish the objective.

Howieson (2005, 2018) states that practical wisdom, which is essential for sound professional judgement, can be developed by providing training in the practical skill of decision-making. The proposed APPT framework would facilitate doing so by encouraging critical and strategic thinking skills when investigating money-laundering cases; the need for the development of such skills has been emphasized by Davis et al. (2010). Digabriele (2008) and Van Akkeren et al. (2016) also highlighted a need for flexible, improvised approaches rather than a structured plan. The APPT framework contributes in this way by facilitating a better understanding of the thought process of a launderer in choosing techniques to launder funds rather than encouraging dissemination of some type of structured plan. Such an understanding would allow the use of an appropriate mechanism to detect money laundering once a predicate crime has been committed. For instance, the COVID-19 pandemic is forcing drug cartels to think of techniques alternative to trade-based money laundering to move illicit funds. The framework would encourage forensic experts to incorporate such social and environmental factors which may form the basis for understanding the choice of technique adopted by launderers. It is an addition to the traditional stages of money laundering describing the process which fails to consider the social and environmental factors in coming up with a proactive detection mechanism (Blankstein et al., 2020).

The rest of the chapter is organized as follows. Insights provided by researchers and practitioners are synthesized to identify the factors influencing the choice of laundering

techniques. The new APPT framework is then presented, followed by the use of real cases to demonstrate its applicability before concluding.

3.2 Factors influencing the choice of money-laundering techniques

In contrast to other crimes, where decisions taken by criminals may be irrational (Clarke & Webb, 1999), in money laundering the choices are made via a rational assessment of several direct and indirect factors. It is consistent with the views of Clarke (1983) to say a launderer will assess these factors to reduce risk and maximise rewards. This chapter identifies a range of factors influencing the choice of laundering techniques by synthesising prior work in fraud, forensic accounting, and related areas such as psychology, sociology and organisational behaviour. The framework is consistent with the views of Huber (2017), who stressed the need to consider n-dimensions of financial crime to be accounted for in a framework attempting to explain, prevent, predict, detect and prosecute financial crimes.

The influencing factors are summarised in Table 8. The nature, location and the amount of predicate crime, the purpose for laundering, and the kind of technology available and required, influence the choice between criminal and non-criminal actors to launder funds. (The criminal launderer is the one who commits the predicate crime and is laundering. The non-criminal launderer is someone unrelated to the predicate crime.)

Similarly, the choice between the motive to launder funds, that is, between integrating the funds into the economy or financing further crimes, influences the desire to maintain anonymity. It, in turn, leads to playing a crucial role in deciding the actors involved and the use of technology, as maintaining anonymity at times may be the least of concerns. The same holds in making use of the available technology. An explanation and justification of each factor follow.

Influencing Factor	Sub-factor
Actors Involved	Criminal: Actor responsible for a predicate crime
	Non-criminal: Professionals, or banks, or other organisations not direct parties to the predicate crime
Predicate Crime	The amount involved in the crime
	The nature of the crime, which may be quasi-legal or violent in nature
	The location of the crime
Purpose of laundering	Facilitation of integration into the economy
	Financing of further crimes
Technological Innovations	Technological intensity
	Less dependence on technology

Table 8. Factors influencing the choice of money-laundering techniques

3.2.1 Actors Involved

In contrast with other financial crimes, the act of laundering funds may or may not be undertaken by the actor responsible for the predicate crime. The knowledge and skills of the actors play a critical role in determining their participation in the illicit schemes (Wolfe & Hermanson, 2004). At times, sophisticated techniques to launder funds may not be required because of the evident link between the proceeds and crime; in such cases, criminal actors may launder funds by themselves. For instance, for laundering drug proceeds as reported by Van Duyne (2003), Reuter and Truman (2004), and Malm and Bichler (2013), criminals laundered funds themselves using simple mechanisms. However, Soudijn (2012) found non-criminal actors to be an essential part of criminal networks in the laundering of funds, mostly when money laundering is part of the criminal activity of such networks and it requires sophistication (Rusanov & Pudovochkin, 2018).

The competence of actors is critical in determining the techniques adopted in laundering funds (McCarthy et al., 2015). For instance, the use of virtual currencies for this depends on whether the actor has received the specialised training needed to operate (Dostov & Shust, 2014). The actors capable of laundering funds have a well-connected network of experts to undertake the illicit act with knowledge about jurisdictions that respond slowly to compliance requests; they have a suitable combination of incriminated and legitimate assets, and awareness of compliance standards in banks (Teichmann, 2020). As a result, the ability of actors, both criminal and non-criminal, in lending sophistication, knowledge and expertise in handling proceeds of crime is critical in determining the techniques they adopt.

Concerning non-criminal actors, several other factors need to be considered to explain their motivation to participate in the laundering of funds; these include occupational roles, individual characteristics, and the organisational and social climate (Ainsworth, 2013; Albrecht et al., 1984; Andon et al., 2018; Benson, 2016; Broidy, 2001; Fritsche, 2005; Knust & Stewart, 2002; Kranacher et al., 2011; Kumar et al., 2018; Langton & Piquero, 2007; Murphy & Free, 2016; Paternoster & Mazerolle, 1994; Sykes & Matza, 1957). However, dealing in depth with the motivation behind their participation is outside the scope of this current work.

3.2.2 Predicate Crime

An illicit activity that accompanies money laundering is termed a predicate crime. It is the underlying criminal activity that would eventually generate proceeds subject to money laundering. The definition of what constitutes a predicate crime varies between jurisdictions (Walters et al., 2012). Irwin et al. (2012) found that predicate crime offenders preferred specific techniques to launder funds. As per Bajada (2017) and Rusanov and Pudovochkin (2018), the predicate crime is a critical factor in determining the process of money laundering.

The nature, amount and location of the predicate crime influences the complexity of the techniques adopted. It is often stated that the more socially dangerous the predicate crime is, the more socially dangerous and complicated are the efforts to hide the proceeds. Predicate crimes such as corruption need complicated mechanisms of laundering, more so than crimes related to property and drug-trafficking. Furthermore, higher proceeds of crime result in more complicated techniques adopted to launder funds (Rusanov & Pudovochkin, 2018). The same was highlighted by Bell (2002), who states the extent of complexity in money laundering is dependent upon factors such as the volume of money and the type of predicate crime committed.

The location of predicate crime and the regulations surrounding it play a critical role in influencing the complexity of techniques adopted to launder funds. For instance, in a location where the interpretation of law requires predicate offence as an essential requirement to prove criminality, techniques to break those links between the crime and proceeds would be adopted (Murray, 2016). Similarly, the attractiveness of the actual location of predicate crime would influence the laundering mechanism (Unger et al., 2006).

3.2.3 Purpose for laundering

Rusanov and Pudovochkin (2018) observed that giving dirty money a legitimate appearance may not be the only objective of laundering. They stated that funds obtained from a criminal act are laundered, whereas, in other instances, laundered funds may be used to finance other crimes. Consequently, when considering the possible choice of the techniques to launder funds, the purpose needs to be considered. Research in the past has suggested that the motive influences the degree of sophistication adopted in laundering (Compin, 2008). For instance, Compin (2008), Krieger and Meierrieks (2011) and Vittori (2011) have documented the differences between money laundering and terror financing based on sources of funds, the direction of financial flows, financial sophistication and psychological profile. In line with the views mentioned above, Irwin et al. (2012) found that money launderers and terrorist financiers adopt different laundering techniques.

Such a distinction stems from the difference in the complexity adopted to launder funds depending upon the ultimate purpose. Money laundering is oriented to legitimisation (Koh, 2006), leading to the use of complex techniques. Launderers to maintain anonymity complement their actual business activities with fictitious transactions or an appropriate complex mechanism (Teichmann, 2020). On the other hand, terror financing is distribution-oriented, resulting in simple methods adopted to move funds. As Hobbs et al. (2005) point out, offenders operate where the benefits outweigh the risk involved; however, such an analysis may not be involved in the case of terrorism.

Finally, in money laundering, the source of funds is illegal, whereas in terror financing, funds may be from a legal source. In terrorism financing, the anonymity of the source is not the primary concern, but the focus is on hiding the destination of funds. Hence, terror financing does not involve the complexity associated with money laundering (Bantekas, 2003) because of the difficulty associated with proving criminality for funds intended to be used for terrorist purposes as the proceeds of that criminal intent (Kersten, 2002). The purpose for which funds

are laundered influences the need or desire to maintain anonymity. Additionally, the purpose of laundering is influenced by the ideology of actors, a factor considered necessary by Kranacher et al. (2011) in understanding the motivation behind committing an illicit act.

3.2.4 Technological Innovations

Richet (2013) observed that traditional techniques of laundering have evolved pursuant to the advances made in the online arena. The changes in technology have made it easier to commit cybercrime (a form of predicate crime) and laundering of funds (Bichler et al., 2017a; Kamps & Kleinberg, 2018; Sood et al., 2013; Speer, 2000). The increasing ease may be attributed to the extensive use of the online platform, which aids in overcoming the constraints of a social network such as geographical or social barriers. It facilitates collaboration with perpetrators across the globe and thereby increases the opportunity to commit illicit acts (Leukfeldt, 2014). Barone and Schneider (2018) view as a growing threat cyberlaundering and money laundering accomplished through the use of automatic electronic devices.

The recent innovations in techniques to launder funds comprise Bitcoins, online gaming (usually for small amounts), encryption software, and secured browser technology such as The Onion Router (TOR), among others (Soudijn, 2019). They have increased the difficulties associated with detecting money laundering by adding more clandestine variables as a result of the increased association with technology (Gilmour, 2016a; Soudijn & Been, 2020). The unregulated transactions and exchanges that take place on 'Distributed ledger technologies (DLT)' have been viewed as a threat to society through their use for money laundering, terrorist financing and tax evasion (Scholl & Bolívar, 2019).

The literature is full of examples of technological advances in committing predicate crimes such as fraud and laundering of funds (Dalins et al., 2018; Dostov & Shust, 2014; Tiwari et al., 2019). Smarter regulation could be aided by establishing a link between stakeholders (users of the technology) and the value generated from a technological innovation by drawing from the principles of public value and stakeholder theory, similar to cost-benefit analysis (Bannister & Connolly, 2014; Rose et al., 2018; Scholl, 2001; Scholl, 2004; Scholl & Bolívar, 2019; Twizeyimana & Andersson, 2019). Until this happens, advances in technology appear likely to increase the opportunities to commit financial crimes and launder funds.

3.3 Development of the new APPT Framework

Looking at one factor in isolation as critical in influencing the choice of money-laundering techniques can be misleading, as much depends on the characteristics of the crime, the actors, the kind of technology available and the purpose for laundering. The use of technology is influenced by the amount involved as part of the predicate crime. If the amount involved is large, the need to use virtual currencies and other innovative technologies may arise as a potential medium to launder funds. Another vital factor is the purpose of laundering. If the aim is to commit another crime such as related to terrorism, the technology adopted may be different. For instance, the choice of using online gaming to launder funds was influenced by the amount involved and whether the final objective was to execute an act of terror (Samantha Maitland Irwin et al., 2012). However, the choice of technological innovation in itself is influenced by the availability of technology in a particular location. Additionally, the capability of actors involved in the predicate crime or that of non-criminal actors needs to be considered while evaluating the possible choice of technology that could be adopted to launder funds. These factors are interrelated and interdependent, except in scenarios where the end objective is destruction and rational decision-making is absent. Such an approach would allow bypassing of the limitational oversight offered by theories such as the routine activity theory (Clarke & Felson, 1993; Cohen & Felson, 1979; Felson & Boba, 2010) attempting to explain the motivation for a crime.

The proposed APPT framework (as presented in Figure 7) addressed the interdependence between factors to shed light on why a particular approach was adopted to launder funds. The interconnected nature of the factors as described in the framework is in line with the views of Gilmour (2016b). Gilmour suggested that acknowledging this interconnection would increase holistic understanding of the money-laundering environment. With this better understanding, it would thereby become possible to consider the situation and the circumstances influencing the decisions of relevant actors.

The predicate crime affects the decision of who is going to launder funds. Notwithstanding cases where the money may be from a legitimate source, the decision of criminal and non-criminal actors to launder funds is influenced by the purpose of laundering. It may be to perpetrate another crime or to obtain clean funds for legitimate use. Further, if the amount involved is substantial and the criminal actors do not possess the required capabilities and technological expertise, non-criminal actors are included to aid in the laundering of funds.

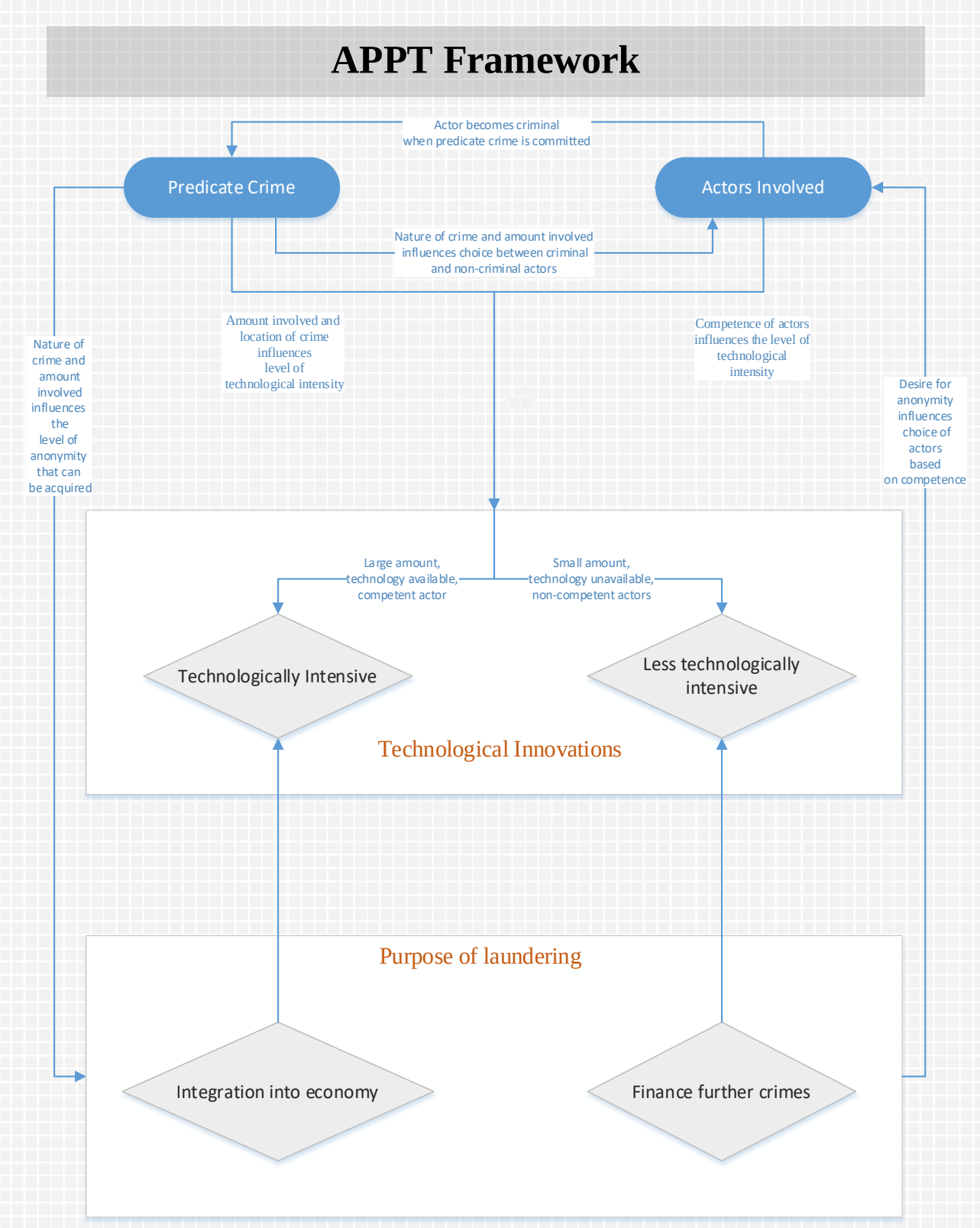

Figure 7: The APPT Framework for Money Laundering (Produced by the author)

Concerning the purpose of laundering funds (as presented in the APPT framework), if it is to commit further illicit acts such as funding a terror attack, discerning the money trail between the predicate crime and the laundering of funds may not be the primary concern. On the other hand, if the aim is to integrate the funds into the economy and give them a legitimate appearance, the use of sophisticated and complex techniques is common and it makes the money trail challenging to follow. The decision to use laundered funds for financing crimes in the future or to give them a legitimate appearance is influenced by the ideologies of the actors involved, a critical factor emphasised by Kranacher et al. (2011).

Concerning the use of technological innovations, as shown in the APPT Framework and based on the literature discussed above, if the predicate crime involves laundering small amounts of funds, then the use of less technologically intensive techniques may suffice. In contrast, virtual currency transactions may be used for laundering larger amounts. If the purpose is to ensure anonymity, more complicated technological innovations are brought into use, requiring the actors to be expert in such technologies, and their availability becomes critical.

Overall, the decision about the techniques adopted to launder funds could be considered a problem for a money launderer as depicted in the APPT framework. The decision is influenced by factors which encompass the pressures, constraints, beliefs, values and assumptions of the problem solver, in this case, the money launderer, in the environment containing the problem. It allows for the presence of an element of subjectivity in terms of risk-taking ability on the part of a money launderer. Additionally, the possibility increases of interaction between a variety of factors, the competence of the problem-solver, the evolving nature of the problem as well as adapting to the change (Mumford, 1998). It was Ashby (1961) who stated that upon encountering a complicated situation with multiple variables, the establishment of a link between variables could aid in viewing and addressing the problem as a single unit.

Further, just as it is with a complex problem in any other practical context (Stevens & Churchman, 1975), the decision to adopt a particular technique to launder funds is accompanied by difficulties and ambiguities, many of which have to be accepted in making the decision as depicted in the APPT framework. Moreover, as Beer (1985) points out in the context of problem-solving, the decision to choose among techniques involves a hierarchy of activities, namely, identification of routine tasks, assessment of difficulties, identification of factors to be

prioritised, and continuous evaluation and monitoring of the effectiveness of the technique or mix of techniques adopted to launder funds.

Consequently, the rational decision-making of a money launderer can be substantiated through the concepts in systems theory, such as structural coupling, which acknowledges the codependency between factors in a system – in this context, the factors influencing the choice of laundering technique (Luhmann et al., 2013; Maturana & Varela, 1987). This chapter is in line with Demetis (2018), who also acknowledges the call from Mumford (1998) to reconsider money laundering from a systems theory viewpoint to gain additional insights.

The developed APPT framework can be used to explain the modus operandi adopted by launderers, and the relevance is substantiated in the cases mentioned below. The cases highlight the connection and coevolution between the factors and their influence on the final decision (choice among technique or techniques to launder) (Luhmann et al., 2013; Maturana & Varela, 1987).

3.4 Application of APPT Money-Laundering Framework

There are numerous examples of money laundering scandals such as the Troika Laundromat, the Azerbaijani Laundromat, and the Danske Bank, among others (Bjerregaard & Kirchmaier, 2019; OCCRP, 2017, 2019). This chapter uses a selection of real cases to substantiate the applicability of the current framework. The criteria for choosing the cases below include either (i) involvement of a regulatory authority in the investigation of such cases, or that (ii) the scandal attracted considerable attention from the media and involved a substantial financial sum. The purpose was to demonstrate the applicability of the framework on, but not limited to, cases with a distinct nature, purpose and magnitude. The chosen cases are the Troika Laundromat, a case involving underground banking to launder drug profits, a case involving raising funds for terrorism, and Bestmixer.io.

3.4.1 The Troika Laundromat

The Troika Laundromat refers to a group of shell companies collectively operated by an independent arm of Troika Dialog, a Russian investment bank, to move an estimated USD 8.8 billion from Russia to the west (OCCRP, 2019). A complex web of transactions was created between the network companies to blend the money derived from illicit sources with legitimately earned private wealth. These companies used fake contracts to move wealth across

borders (Garside, 2019). The laundromat paved the way for Russian oligarchs and politicians to use laundered funds to purchase luxury goods and real estate, and make other investments. The laundromat scheme was dependent upon a broad range of actors, including the staff at Troika Dialog, who created a complex trail of money to trace while keeping the actual beneficial owners out of the reach of the authorities. The complexity of the scheme is evident from the existence of more than 1.3 million financial documents relating to the activities of Troika Dialog and the Lithuanian lender Ukio bank (Perryer, 2019).

3.4.2 Use of underground banking to launder drug profits[1]

As part of a Lebanon-based international crime syndicate, one of the members of the syndicate used informal money transfer systems, known as "hawala," to transfer drug profits to two other syndicate members residing in Australia. The first member, an Iranian national, received over AUD 1 million in cash, which was further sent to high-risk jurisdictions. The second member, an Australian citizen, was reported to have transferred an amount totalling AUD 244,000 to several countries. A joint initiative by the investigative agencies with assistance from the Australian Transaction Reports and Analysis Centre (AUSTRAC hereafter) and the reporting entities was able to identify the members of the crime syndicate and arrest them. As part of the investigation, another member was identified in possession of cash, diamonds and casino chips, and was eventually arrested. The banks provided reports on the movement of large, unexplained sums of money, and these were analysed by AUSTRAC to provide financial intelligence to investigative authorities (AUSTRAC, 2019).

3.4.3 Raising funds for acts of terrorism[2]

A joint investigation led to the identification and eventual arrest of people in Sydney and Melbourne who were planning a terrorist attack. The investigation of the Sydney-based suspects revealed the daily income from their employment was the primary source of their funding. In some contrast, Melbourne-based suspects relied upon donations to a fund for the heinous act. The investigation revealed the value of funds at the time of arrest was AUD 19,000.

[1] The names of this crime syndicate and the people involved have been kept anonymous in the public domain.

[2] Key details including people's names have been kept anonymous

In addition, the suspects had also relied upon credit card fraud schemes and fundraising activities (AUSTRAC, 2014).

3.4.4 Bestmixer.io

Bestmixer, a cryptocurrency mixer (a term applied to services responsible for blending cryptocurrencies from different sources), was used to obscure the trail of funds to its source (Europol, 2019). The users would employ the services provided by the dark web firm to avoid due diligence by blending illicit and licit cryptocurrencies. The service was dismantled collectively through the works of the Dutch Fiscal Information and Investigation Service (FIOD), Europol, and other authorities, working with support from McAfee, a cybersecurity firm (Vedrenne, 2019). The demand for such an opportunity is evident from the fact that Bestmixer, during its tenure of one year in operation, mixed an amount close to $200 million in bitcoins (Europol, 2019; Vedrenne, 2019).

The above-highlighted cases attempt to draw attention to the sophistication and complexity in techniques adopted in laundering funds, depending upon a wide range of factors. In the case of the Troika Laundromat, sophisticated techniques were used to hide the ultimate owners and obscure the money trail, as is evident from the use of shell companies and a complex web of transactions. The scandals involved wealthy people and a considerable range of professional actors such as lawyers, accountants and company service providers to execute the scheme. In the case of a crime syndicate, the syndicate members laundered the funds themselves using informal transfer systems and the available banking facilities.

In the case of financing the acts of terrorism, the level of financial sophistication adopted to cover the trail was minimal. However, the Bestmixer case directs attention towards a need to focus on the new opportunities becoming available to money launderers following the advent of technology. It reiterates the notion of cryptocurrencies being a conduit of illicit financial flows, particularly where the services to access these virtual currencies, and the actors proficient in it, are obtainable. From the information available on these cases, the extent to which technological innovations were used could not be extracted, but given the prominence of the use of virtual currencies, ignoring such a possibility would be inappropriate.

These cases exhibit the need to consider a combination of factors in determining the possible money-laundering techniques that may be adopted to launder funds. Up until now, there had been ambiguity around predicting them (Canhoto & Backhouse, 2007). These

ambiguities emanated from the presence of a wide range of predicate crimes, the actors involved, a lack of information-sharing and the evolution of techniques resulting from technology (Backhouse et al., 2005; Bell, 2002; Canhoto & Backhouse, 2007; Philippson, 2001). The proposed APPT framework incorporates a range of factors that need to be taken into consideration to understand the possible mechanism adopted by illicit actors to launder funds and to explain the modus operandi adopted once the predicate crime has been identified. Incorporation of such frameworks of financial crime could be value-additional in increasing the educational content value by training neophytes and experienced practitioners to think and respond with critical appropriateness.

3.5 Conclusion

This chapter has proposed the new APPT framework to explain the factors influencing the techniques adopted to launder funds. Any model of financial crime must recognise its multifaceted nature, and the factors that influence it. The APPT framework highlights the interaction between factors, using existing theories and observations, which may prompt the choices of both individuals and organisations to accomplish the purpose of laundering. The applicability of the APPT framework was then demonstrated through real-life cases. The framework proposed in this chapter differs from theories solely focusing on criminal actors such as self-control theory (Walters & Bradley, 2019) and individual trait theory (Schechter, 2004). In addition to individual factors, it draws attention to social and environmental factors influencing a person's decision-making process (Clarke & Cornish, 1985; Piquero et al., 2002) in the adoption of techniques to launder funds.

The rational decision-making of a money launderer (Gilmour, 2016b) can be substantiated through the concepts in systems theory, such as structural coupling that acknowledges the codependency between factors in a system – in this context, the factors influencing the choice of laundering technique (Luhmann et al., 2013; Maturana & Varela, 1987). This chapter is consistent with Demetis (2018), who also acknowledges the call from Mumford (1998) to reconsider money laundering from a systems theory viewpoint to gain additional insights.

The APPT framework has implications for neophytes, for experienced practitioners and for institutions teaching forensic accounting. For neophytes, qualifications incorporating a wide range of topics with opportunities to develop phronesis may increase their employment

opportunities in the field. Among experienced practitioners, such knowledge would aid in exercising professional judgement to come up with appropriate detection and deterrence mechanisms. In educational institutions, such a framework would suggest a move towards the incorporation of pedagogical techniques aimed at improving the content value and encouraging the development of skills valued by academics and practitioners. The APPT framework can also be leveraged. Future researchers could extend the present work by empirically examining the differences in applicability of the APPT framework for developed and developing countries. The framework can also be applied to new money-laundering cases to help uncover interesting insights. Additionally, a more detailed understanding of the motivation behind the participation of non-criminal actors in the act of money laundering could help to improve the framework.

The APPT framework may contribute to the understanding of the choice of techniques adopted to launder funds. This thesis extends further by gaining an insight into detection of one such technique to launder funds. The next chapter focuses on detecting illicit shell companies used to launder funds.

Chapter 4 Detecting Shell Companies Laundering Illicit Money

***** This chapter is based on a conference paper accepted for a conference, namely: Tiwari, M., A. Gepp, and K. Kumar. 2021. Shell Companies: Using a hybrid technique to detect illicit activities, in *2021 AFAANZ Virtual Conference.*

The previous chapter developed a framework to provide insights into the techniques a launderer may adopt to wash funds among a range of available options. As uncovered in the literature review (Chapter 2), amongst the detection of money-laundering techniques, the detections of shell companies used to launder funds was found to be under-researched. Shell companies can be used to launder dirty money to make it appear legitimate and hide information about the actual beneficial owners. Illegal arms dealers, drug cartels, corrupt politicians, terrorists and cyber-criminals have become some of the frequent users of shell companies. To combat this money-laundering technique, this chapter aims to develop a model for detecting shell companies in operation to launder illicit proceeds of crime using a new hybrid statistical approach. No prior study exists on developing quantitative models to detect illicit shell companies using publicly available information. The key stakeholders to benefit from such models would be legal and compliant professionals and government officials, especially accountants, tax officials and anti-corruption NGOs.

4.1 Introduction

Shell Companies have legitimate uses such as facilitating reverse mergers, being used as holding companies or for protecting small entrepreneurs from bankruptcy risks. However, these entities have also become instruments to launder the dirty money to make it appear legitimate and hide information about the actual beneficial owners. Illicit arms dealers, drug cartels, corrupt politicians, terrorists and cyber-criminals have become some of the frequent users of these shell companies. The ease of setting up companies, with trans-nationality involved and a low-level of compliance towards the Financial Action Task Force (FATF), standards have posed a challenge for law enforcement authorities in countering crime and corruption (Martini et al., 2019). In 2002, an anonymous shell corporation called "Anglo-Leasing" was used to launder €24 million of the total €30 million as part of the contract awarded to the firm to update the passport system in Kenya. The information about the beneficial owners could not be identified because of the anonymity the form of such entities provides (Allred et al., 2017; Findley et al., 2015). Other such instances involving shell companies would include that of China ZTE using shell companies to evade US sanctions; also, SBM Offshore N.V., a Dutch-based group, was paying bribes to shell companies owned by government officials (Hubbs, 2018).

Graph analysis may enable investigators effortlessly to infer ownership and relationships – for example, common or joint ownership of businesses – and hence detect these illicit shells. This chapter aims to facilitate the detection of money-laundering activities by using graph analysis with publicly available data on entities identified in several corruption cases, with the aim of developing a detection model.

The automated anti-money-laundering (AML hereafter) detection may be split into three subsets based on data: Those that can be detected based on data available on usual account activity statements; those where detection requires correlation that might potentially violate the bank's data policies; and those where detection involves data that are not directly available from the bank's information system but are available from other publicly accessible sources, such as a list of high-risk money-laundering countries. This chapter focuses on the latter subset.

The rest of the chapter is organised as follows: a summary of the data sources is presented first, followed by an overall schema of the data collection procedure. It is followed by providing a rationale for the inclusion of variables in the analysis and graph construction.

The chapter then explores new insights gained from data through traversal queries. Finally, the modelling techniques are introduced and used, and the results are discussed.

4.2 Data and methodology

4.2.1 Data sources

Transparency International, UK (TIUK), an anti-corruption NGO, is kindly supporting this project and has provided for analysis a list of names and company numbers of 804 companies along with the associated cases. TIUK used open-source data from various investigation reports to produce a list of these companies (Cowdock, 2017). They went back to 2004, with records and leaked documents from Open Corporates and UK Companies House, the British corporate registry, published in the 2017 report called "Hiding in Plain Sight: How UK Companies are used to Launder Corrupt Wealth". These entities were used as a corporate veil to launder illicit funds and hide the real beneficial owners. Even though some of the entities were incorporated for accomplishing other illicit activities, laundering of funds was the central theme for all the entities. The breakdown of the company type is presented in Table 9 as follows:

Number of Companies	804
Incorporation Country	UK
Estimated amount of funds laundered	£80 billion
Company Types:	
Limited Liability Partnership (LLP)	436
Limited Partnership (LP)	158
Limited Company (Ltd)	210

Table 9. Data on shell companies

Among the 208 limited companies considered (two were duplicates out of the total samples of 210), the names of the cases for 13 entities were unidentified in the public domain and were placed into the "Unidentified Cases" category. In addition to this, for the purpose of obtaining a matching sample, a sample of 205 limited companies was selected based on their cash balance and, when that was unavailable, the period of operations and company status, whether active, dissolved or in liquidation. The entities in the matching sample may be

involved in illicit activities, but in line with assumptions made by Ravenda et al. (2015), it is assumed that a low probability exists for an entity's being chosen from the large population of companies registered with the UK Companies House to be involved in illicit activity.

Out of the total initial sample of 417 companies collected from OpenCorporates, four were found to be duplicates and so were eliminated; hence, 208 corrupt and 205 non-corrupt companies were considered for analysis.

OpenCorporates has been a preferred choice for investigating and analysing company data because of its ability to provide what is referred to as "White-Box Data" (OpenCorporates, 2019b). Among data analysts, a standard classification of data is into "White-Box Data" and "Black-Box Data". Black-box data are vague in representation and have an unknown source of origin. On the other hand, white-box data are well-defined, transparent, regularly updated and accompanied by provenance.

Additionally, to cater to the growing needs of businesses, governments and banks, a data ecosystem is required, one which is regularly updated and facilitates connections between different users. In today's time when AML is no longer a tick-the-box affair, it is essential to have corporate data accompanied by provenance and consistency, and incorporating the cross-jurisdictional nature of business. OpenCorporates provides regularly-updated company data in a consistent and aggregated manner.

Information about the appointment of directors was obtained from the UK Companies House. Finally, other information sources considered for this study were EveryPolitician, OpenSanctions, UK Companies House Disqualified Directors and the Financial Secrecy Index. The following sub-section describes the data collection process.

4.2.2 Data collection process

The names of the companies, along with their company numbers and the corresponding cases, were imported to an open-source software called OpenRefine. For the matching sample, the companies were labelled as non-corrupt companies with no links to corruption. OpenRefine, formerly known as Google Refine, is a software program that facilitates analysis of messy data, cleansing of data and transforming them from one form to another. Moreover, it enables data extension through web-services, establishing links to databases, and requires the use of specific regular expression scripting language, also known as General Refine Expression Language (GREL hereafter) (Carlson & Seely, 2017; Hill, 2016; Kusumasari, 2016; Larsson,

2013). OpenRefine, through the use of the Open Refine reconciliation API, matches the list of company names to corporate legal entities (OpenCorporates, 2019a). OpenCorporates provides a reconciliation endpoint for OpenRefine which facilitates the matching of company names with legal entities on OpenCorporates. The OpenCorporates API returns information for companies as data in "javascript object notation" (JSON hereafter) format. The list of companies was reconciled with OpenCorporates through the OpenCorporates API endpoint at OpenRefine. On matching the company names with target entities through the use of company numbers as identifiers, data of companies were obtained in JSON format. The use of APIs to obtain data reflects the efforts to achieve granularity and provenance of data. The data obtained in JSON format are parsed through the use of GREL to obtain information for each row item.

The information about the number of appointments of executives in companies was obtained from the UK Companies House. The information so obtained was added to the spreadsheet in OpenRefine containing data on companies. Additionally, web scrapping of the following sources was undertaken:

1. EveryPolitician: A list of all identified politicians was obtained and imported to OpenRefine.
2. OpenSanctions: A list of all individuals and entities with any sanctions imposed on them was obtained and imported to OpenRefine.
3. UK Companies House Disqualified Directors Data: A list of all the executives who have been disqualified from acting as directors in UK-incorporated entities was obtained and imported to OpenRefine.
4. Financial Secrecy Index (FSI): The data on the ranking of jurisdictions based on financial secrecy were obtained and imported to OpenRefine.

The information obtained and imported to OpenRefine was used to reconcile the list of executives for the entities with individuals in the lists (as mentioned above) to extend the data to incorporate any additional information. Further, the ranking of jurisdictions as per the FSI was incorporated in the dataset. Available upon request are the list of operations performed to obtain, cleanse and normalise data for further analysis, the codes used to perform the analysis and the final dataset comprising information about the companies and its executives.

4.2.3 Incorporation of variables

A wide range of information was considered to develop a property graph database model from publicly available data sources. The variables included were company status, incorporation date, dissolution date, availability of previous company names, number of previous company names, tenure of company previous names, registered company address, instances of change in registered address, number of previous addresses, tenure of previous addresses, industry codes of the companies, change in latest available cash balances, current assets, current liabilities and fixed assets of companies, total number of executives for each company, and other basic details including their nationality. Finally, information on the ultimate beneficial owners was also considered.

The rationale for considering such a wide range of information is as follows:

• **Previous Name**: Entities change their names for various reasons. One of them can be association with criminal activities in the past. As a result, the presence of a previous name for an entity can be considered important information to consider while distinguishing between entities for criminal use and those that are legitimate. Considering the presence of previous names is consistent with Lee and Palstra (2018), whose work suggests that companies changing their names frequently are to be flagged as suspicious and ought to be subject to further investigation.

• **Company Status**: The intention is to highlight whether the company is still in operation or has been dissolved. The objective is to assess whether the firm incorporated was dissolved after undertaking the purpose for which it was created, an illegal purpose in this case, or whether it continued to operate after the purpose was accomplished. Considering information about company status is consistent with Ravenda et al. (2018) who stated that owners of Mafia-controlled firms (MCFs) would decide to liquidate the Mafia-controlled shell companies to prevent detection from authorities once the purpose of such entities is accomplished.

• **Period of Operation**: The hypothesis is that difference between the incorporation and dissolution dates can provide information about the lifespan of entities used for illicit purposes. It could help develop an understanding about the timeframe in which the entities are used for carrying out illegitimate activities, which in turn might aid in distinguishing them from legitimate ones. The hypothesis is consistent with the views of Ravenda et al. (2018) who stated that Mafia-controlled firms (MCFs) are likely to have shorter lifespans than non-Mafia-controlled firms (NMCFs) as Mafia owners would decide to liquidate the Mafia-controlled

shell companies to prevent detection from authorities once the purpose of such entities is accomplished.

• **Nationality of Directors**: The idea to bring in corporate governance variables is to determine if there exists a trend or pattern in or a difference between the corporate structure of illicit entities from the ones being used for legitimate purposes. The choice of this variable is motivated by Lee and Palstra (2018) who found that some high-profile money-laundering scandals involved people from former Soviet countries. Further, corporate governance characteristics such as board structure have gained prominence during examination of the occurrences of wrongdoing (Chapple et al., 2018; Holtz & Sarlo Neto, 2014; Ndofor et al., 2015). However, the more sophisticated corporate governance variables that are studied in regular companies cannot be used, as detailed information about shell companies is not available.

• **Appointment of Directors**: The information about the number of companies in which directors hold executive positions could also be a significant factor in accessing the risk posed by an entity. It is presumed that an executive appointment in five or more companies should raise suspicion, as being involved with and managing the operations of so many companies is not possible realistically. It may be totally legitimate for individuals to be directors in more companies, but it is likely to raise suspicion that they are being used as nominees in place of real owners (Lee & Palstra, 2018).

• **Ultimate Ownership Information (Person of Significant Control Information – PSC Information)**: This refers to knowledge about the ultimate beneficial owner. The entities which provide this information may be considered relatively safer than those which do not and hence could be an important attribute in distinguishing shell companies for illicit purposes from the legitimate ones. The rationale for considering this information is supported by Singh (2010) who states that shell companies incorporated for illicit purposes would avoid revelation of their true owners. Further, Lee and Palstra (2018) outline common methods of avoiding disclosures declaring that a company has no beneficial owners, using an ineligible foreign company as a beneficial owner, and using circular ownership structures or nominees.

• **Financial Statement Information**: The incorporation of variables related to financial-statement information is consistent with Ravenda et al. (2015) who developed a logistic regression model for classification of MCFs from NMCFs using various financial variables. Further, within variables depicting the financial position, the process of considering

information on both assets and the availability of cash is consistent with the work of Floros and Sapp (2011) and Singh (2010) who state that shell firms are likely to be less capital-intensive and have lower total assets because of the absence of a real business structure.

4.2.4 Graph construction

A network can be classified as a specific type of relation connecting persons, objects or events. The sets on which the network is based are called actors or nodes. Therefore, a set of nodes and relationships between these nodes forms a network (Fitina et al., 2010). In recent times, there has been a surge in attention received to identifying economic networks in trade and products, and even in detecting fraudulent companies (Barabasi & Albert, 1999; Pacini et al., 2016; Schweitzer et al., 2009; Vitali et al., 2011). There exists literature interested in understanding the emergence of networks in nature, society and technology. The use of a set of unified tools and principles to understand networks is called network science (Barabási, 2013). However, understanding the emergence of a network of shell companies employing tools and principles such as the scale-free property and the small-world property network science is not within the scope of this research. The quantitative analysis of corrupt companies has been unresearched; we see this especially in the context of identified shell companies lacking analysis using publicly available information.

The novelty in examining the complex network of shell companies is substantiated by the views of Barabási (2009) who acknowledges the existence of commonality in networks but disregards the existence of a framework to reveal their universality. One of the objectives is to lay the foundation for the development of a model for illicit shell company detection by analysing a graph of shell companies identified in illicit activities. It extends the underlying idea of developing a detection system for various kind of fraudulent activities (Bangcharoensap et al., 2015; Battaglia et al., 2018; Van Vlasselaer et al., 2017) to shell companies involved in illicit activities. In case of a network of a shell, firms may exert control over other firms through a web of direct and indirect relations extending beyond countries. Consequently, it becomes essential to analyse the complex networks in order to uncover the structure of control and its implications.

Graph analysis techniques have become essential to find suspicious individuals, existing network relationships, unusual changes, geospatial dispersions, anomalous network structure, and being able to handle a large volume of data efficiently (Liu et al., 2016). Besides,

the visualisation of a dynamic and complex set of data in the form of graphs leads the users to have a detailed overview of the data, and to filter, select and look into networks details.

In graph processing, application needs can be categorised into online query processing, requiring low-latency computing, and offline graph analytics, which needs high-throughput computing. For example, community analysis on social networks or link analysis on click graphs are analytical tasks. Moreover, it is vital to ensure that the system also supports interactive user activities such as graph browsing and querying, in the same way as it supports approximate shortest distances relying on indices or sketches derived from the data. Therefore, their construction can be quite analytical (Shao et al., 2012).

As a result, graph data and graph networks are accompanied by challenges of their own. The topology of graphs developed from real-world scenarios is heterogeneous. The nodes in such networks exhibit high heterogeneity of node connectivity and the existence of the dense node problem. A dense node problem refers to a situation where a small fraction of nodes has connections to a significant fraction of other nodes. Secondly, the graph problems are data-driven, indicating that the computation is dependent upon the graph typology. As a result, optimisation of execution of graph algorithms is not possible as it is difficult to determine the computation structure of graph algorithm in advance. Thirdly, graph access patterns have poor spatial memory locality, resulting in large amounts of random memory access. Finally, the run time of most graph algorithms is dominated by memory access. Hence, what is required is a technology of graph storage and retrieval that provides support for a graph data model which is productive, capable of storing large graphs, and could execute complex queries on large graphs. Neo4J is capable of addressing all the challenges as mentioned above (Cattuto et al., 2013).

Graph database technology enables optimisation of interrelated and densely connected datasets to allow for the construction of predictive models and identification of patterns through the use of traversal queries (Miller, 2013). It utilises graph models to store, manage, and update relationships and data with free and flexible schemas (Huang & Dong, 2013). Neo4J, a graph database platform, was chosen to develop graphs from the data collected above. It involves the use of a query language called ‘Cypher’ and lends flexibility in setting up the data model. It provides features such as online transaction processing on graph data (OLTP) and graph analytics. The flexibility in setting up the data structure enables us to see hidden-relationships

in the data and draw conclusions accordingly (Van Bruggen, 2014). In Neo4J, the graph data model is composed of the following building blocks:

- Node: Is a term used to refer to the entities in the data.
- Relationships: Establish the connections between nodes and thus provide a way of structuring the data.
- Properties: Are fundamental attributes describing both the nodes and the relationships.
- Labels: Are a naming convention for nodes and relationships facilitating creation of sub-graphs, easing investigating and determination of hidden data patterns.

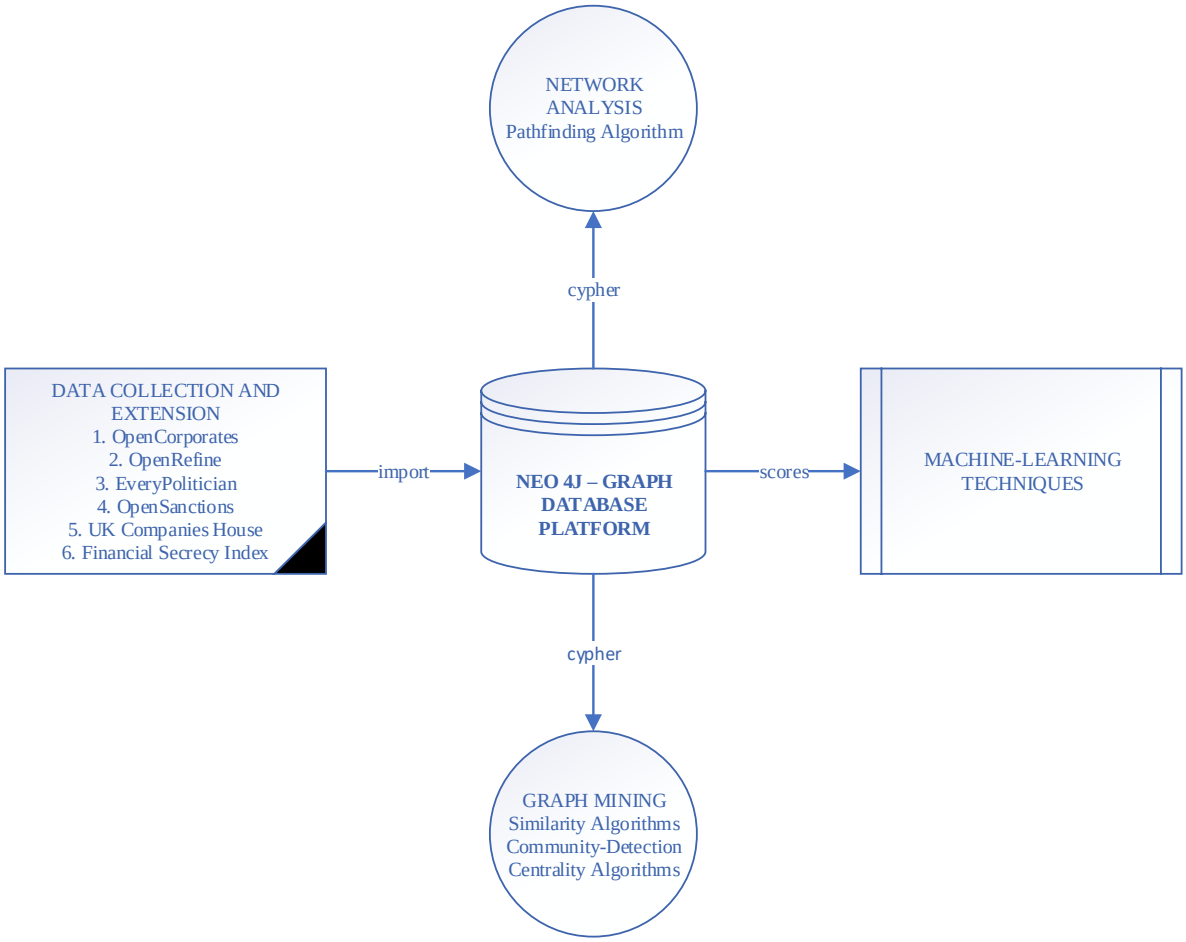

Figure 8: Methodology

The Figure 8 above provides an overview of the methodology used to perform the analysis for the paper. The data collected through the procedure above are imported in the form

of two CSV files. The data collected on 413 limited liability companies were randomly separated into training and testing sample of 320 (77.481%) and 93 companies (22.518%) respectively. The data from the training sample is imported to Neo4J using 'Cypher'. (The set of queries used to import and establish the database structure is available upon request).

A graph comprises nodes and relationships, and this aspect can be effectively used to model highly interconnected data. As part of this study, nodes for this graph database model comprise cases, companies, their owners and executives, addresses, and previous company names. The properties describe the attributes of nodes, and the relationships indicate the existing links between the nodes. The use of properties and labels along with nodes and relationships in Neo4J allows taking advantage of property graphs. As per Miller (2013), property graphs are attributed, labelled and directed multi-graphs facilitating representation of the most complex data in the form of graphs.

The database schema developed for the underlying data is provided in Figure 9 below.

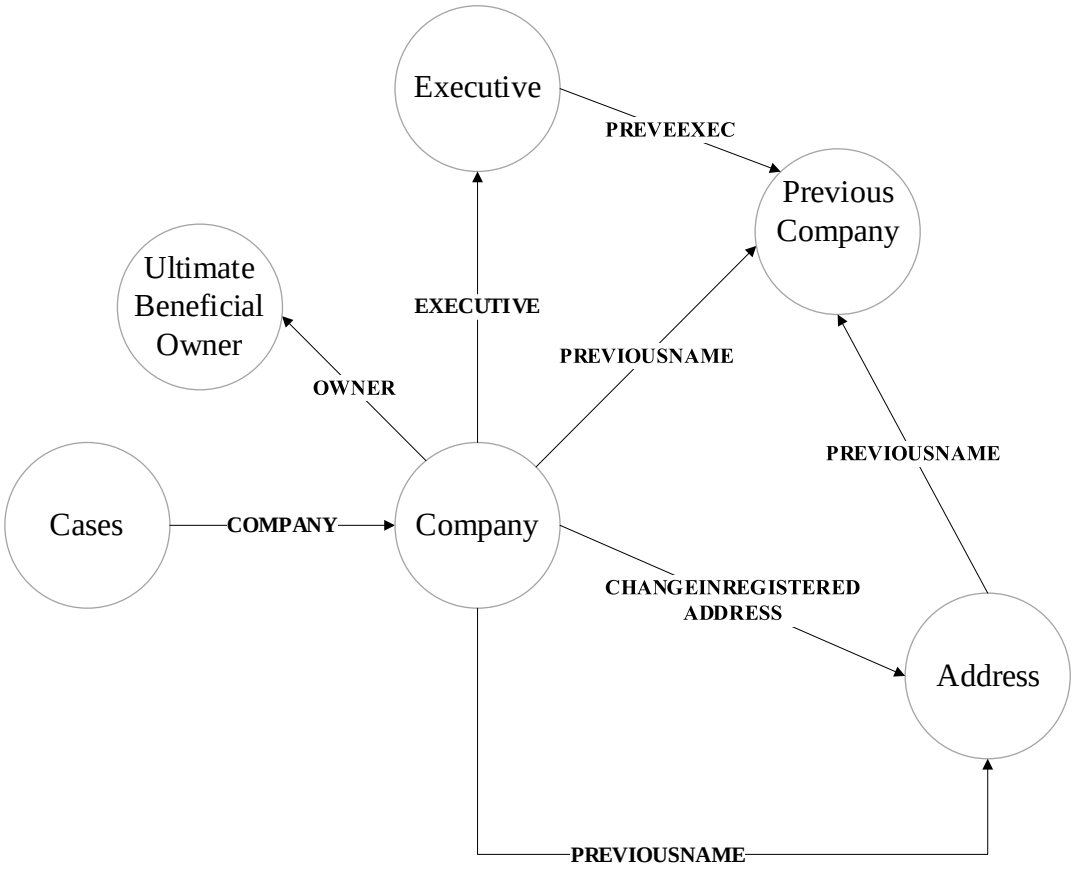

Figure 9: Database Schema

The root node is listed as Cases, and it has an immediate connection with the Company node. For the matching sample, the cases are labelled as "Non-Corrupt" followed by numeric to ensure the data schema remains consistent; the problem of node density can be avoided by attributing a numerical value to each company. A company is registered at an address which is denoted by "Company Address" in the database.

Additionally, a company will have executives and directors (denoted by "Executive") and owners (represented by "UltimateBeneficialOwner"). Finally, a company may have a previous name (indicated by "PreviousCompany") along with a previous address (denoted by "Address"). In case of a scenario where a company has a previous address and an earlier name, then the relationship would be depicted by "ChangeInRegisteredAddress" with the "PreviousCompany" located at that address and the relationship being described by "PreviousName".

The network construction is inspired by the views of Fakhraei et al. (2015) who state that models incorporating multi-relational nature of the networks gain predictive performance.

Additionally, this provides an opportunity to run some graph algorithms on the dataset and draw insights which could lay down the foundation for future research. It is consistent with the views of Drakopoulos et al. (2015). They state that graph databases not only act as a means for graph storage but offer opportunities to perform graph analytics techniques. Graph algorithms related to determining similarities, communities and node importance can be applied. One of the underlying rationales is to establish a base for the interaction between network structure and node attributes, rather than just considering the importance of nodes in a network, as it takes advantage of only network structure and not node attributes (Backstrom & Leskovec, 2011).

In the analysis of networks, a wide range of centrality measures and clustering algorithms are possible; however, the present paper only considers the metrics which improved the performance. Moreover, the lack of literature on which set of methods might perform better promotes the use of a mixed approach combining different methodologies. Determining and proving the outperformance could be something considered for future research.

The following section describes some of the investigative queries run to analyse the data and results of pathfinding graph algorithms performed.

4.2.5 Identification of patterns using traversal queries

The presence of graph database platforms facilitates examination of a network of illicit companies identified in cases of money-laundering schemes and to investigate essential links. The information obtained through identifying links between entities in such an illicit network could be used by investigative journalists and compliance professionals to deter the flow of dirty money. The central hypothesis is dependent upon the fact that entities in the network have links which are hidden and could be identified using a graph database to store the publicly available information on the entities.

As per Nougayrède (2019), to counter the global proliferation of shell companies the focus has been on the acceleration of inter-governmental measures aimed at combatting tax evasion, corruption and money laundering. These measures emphasise sharing of financial account information across borders and maintaining registers of beneficial ownership. However, these measures suffer from limitations such as resistance on the part of the jurisdiction implementing them, proactiveness on the part of national regulators and law enforcement agencies, and maintenance of good quality information by local authorities.

Consequently, the need to investigate and identify such a network of illicit activities is of immense importance.

The use of graph database platforms can add value to the following stakeholders: To investigators and journalists, the chapter provides an insight into organising the data on corporate entities on a graph database platform. It will facilitate investigation and identification of hidden links among entities to deter activities of corruption and money laundering. To the incorporation services and corporate registries, such a work lends the knowledge of importing the data on a graph database platform in an efficient manner and thus strengthening the first line of defence in the fight against money laundering. Finally, to the academics, it provides a platform to incorporate additional techniques to conduct further analysis.

The following sub-section describes some of the investigative queries run to analyse the data and results of pathfinding graph algorithms performed.

4.2.5.a Search Queries

Neo4J involves the use of a query-based language, called "Cypher" to look for patterns in data and draw relevant conclusions (Van Bruggen, 2014). Memon and Wiil (2014) state that Cypher is capable of performing operations of the path-algebra method such as traverse operation, merge operation and filter operation. As a result, the use of Cypher to examine networks in data leaks, such as the Panama Papers and Paradise Papers, and their use by investigative journalists to identify hidden patterns, is well-documented (International Consortium of Investigative Journalists; Kubzansky, 2018; Obermayer et al., 2016). Graph analysis was used by Liu et al. (2016) to detect suspicious activities in large health-care datasets. The flexibility provided by querying the data on graph database platform may reveal information unknown in the public domain.

For the dataset mentioned above, a range of cypher queries was executed to extract relevant information. A list of these queries is available upon request for reference. Apart from these, numerous other queries can be executed to reveal hidden patterns and information and draw relevant conclusions from the data. For instance, on querying the database to find companies with ultimate beneficial owners, it was found that only 51 in the dataset had an ultimate beneficial owner. On querying the dataset for the number of companies located at a postal address, 16 companies were located at the same one.

Further, querying the dataset to determine the number of executive appointments held by a director from a particular nationality, one individual was found to be a director in 139 entities. Similarly, another was found to be a director in 610 entities.

Another query to reveal hidden information was to identify executives in a company who were also directors in the company with their respective previous names. The graph of the existence of such a pattern is provided in Figure 10 below. Such instances are not necessarily an indication of fraudulent activity, but they do raise a suspicion, for further investigations.

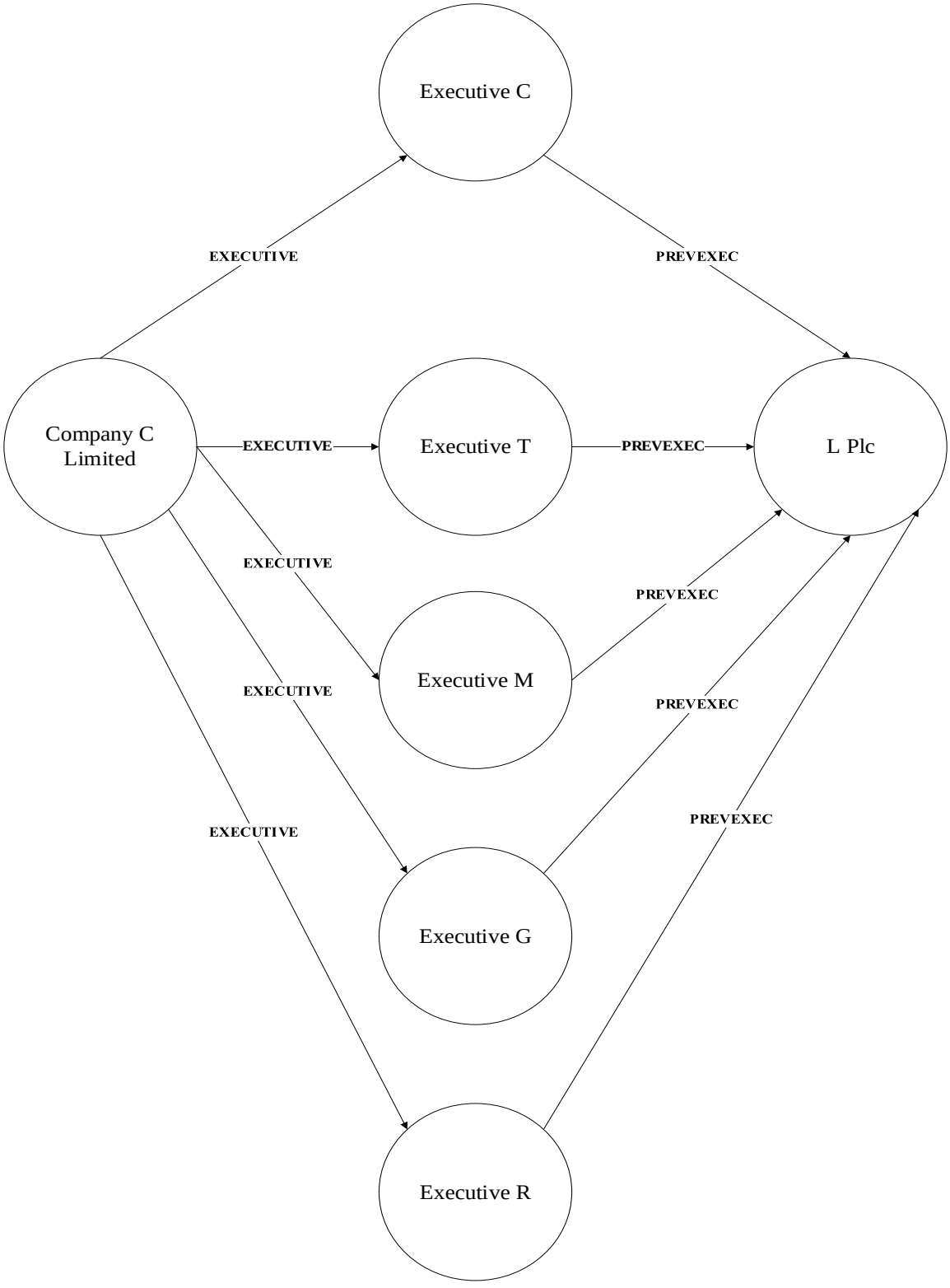

Figure 10: Appointment of executives in previous companies

4.2.5.b Pathfinding algorithms

Pathfinding algorithms increase the understanding of the way the data are connected (Needham & Hodler, 2019). In a general sense, these algorithms help to explore the shortest path and evaluate the quality and availability of routes. The literature is full of the ubiquitous applications of pathfinding algorithms and the detailed applications of these algorithms is not within the scope of this study. There is a variety of pathfinding algorithms such as the minimum spanning tree, shortest path, single-source shortest path, all pairs shortest path, A*, Yen's k-shortest paths and random walk. The pathfinding algorithms used in the study, along with their results, are as follows:

- The Shortest Path Algorithm

The Dijkstra shortest path algorithm, commonly known as the shortest path algorithm, was proposed in 1956 (Needham & Hodler, 2019). It calculates the shortest path between a pair of nodes and could be used as an extension to search queries to give a broader overview of the dataset. It could unveil the presence of hidden connections. As Norton (2018) points towards the existence of surveillant assemblage, algorithms such as shortest path could extract meaning out of data collected from various sources by establishing unidentified links amongst them. The algorithm could facilitate information about the degrees of separation, in cases of criminal and social networks.

For the dataset mentioned above, the shortest path algorithm was executed to extract the shortest path between a given pair of entities. The executed codes are available upon request. The graph depicting the path between each pair of nodes is presented in Figure 11 and Figure 12 below. The figures exhibit the traversal of relationships in the graph network to draw out the shortest path among the pair of nodes.

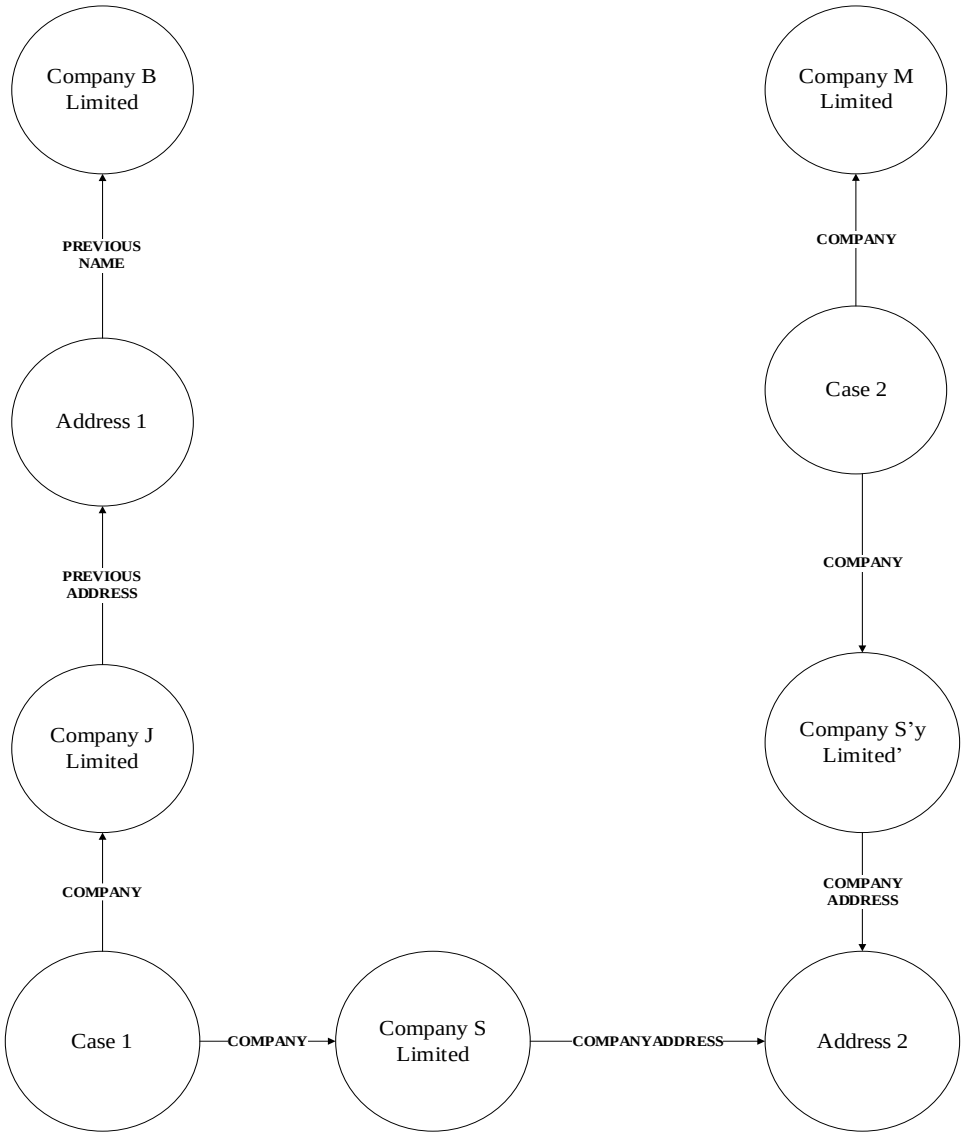

Figure 11: Shortest path between Companies B and M

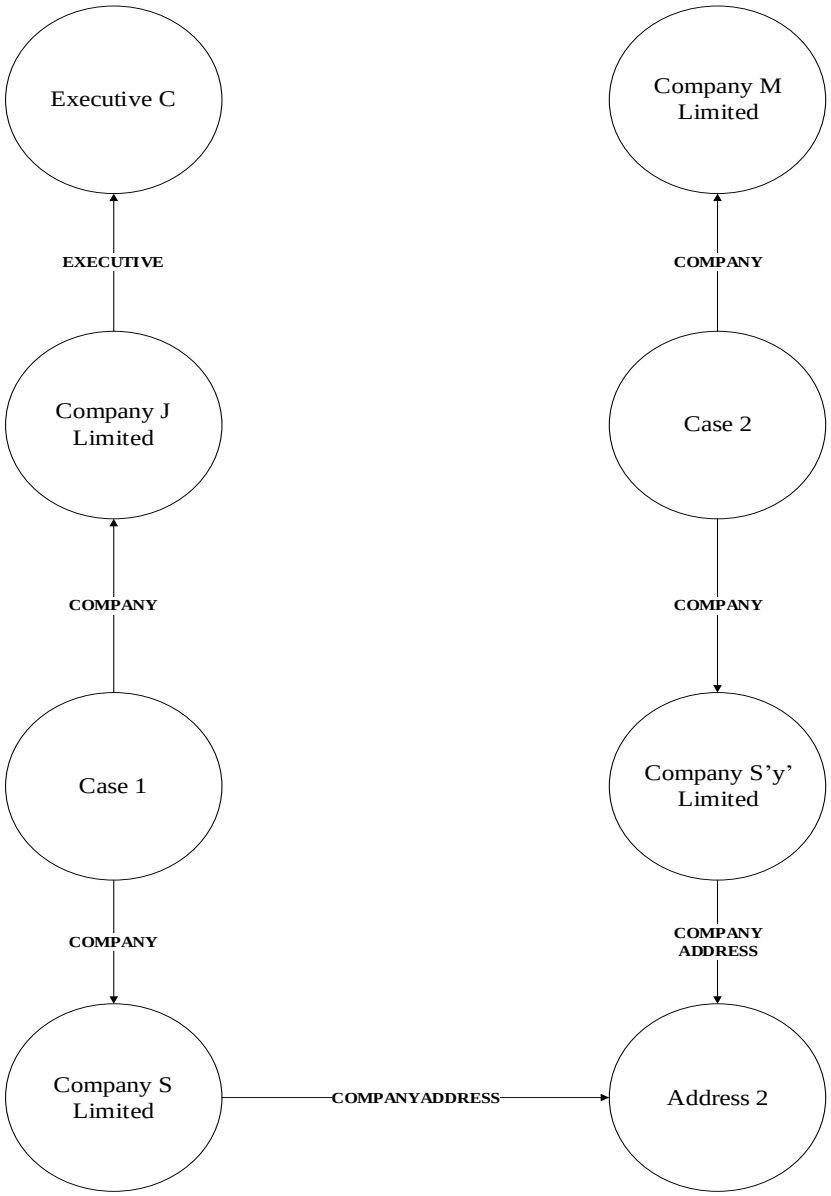

Figure 12: Shortest path between Companies C and M

Apart from the queries used, numerous other queries can be executed to reveal hidden links and information and draw a relevant conclusion from the data.

- The All Pairs Shortest Path Algorithm

The All Pairs Shortest Path algorithm (APSP hereafter), considered to be an improvisation of the Single Source Shortest Path algorithm, computes the shortest path among all pairs of nodes (Needham & Hodler, 2019).

For the dataset as mentioned above, the APSP algorithm was executed to extract the shortest paths between pairs of all nodes in the network. The codes to execute the algorithms are available upon request.

4.2.5.c Implications of a graph database platform

It is often argued on the part of corporate registries and company service providers that there exists a lack of resources to conduct the necessary due diligence on clients interested in incorporating entities. Findley et al. (2013, 2015) in their study have identified instances of non-compliance on the part of company service providers. The effectiveness of regulations surrounding the enforcement of AML regulations and their success in achieving the desired objectives have been questioned (Pol, 2018a, 2018b). Additionally, Becerra-Fernandez et al. (2000) and Hawking et al. (2005) have advocated the representation of complex networks into graphs to aid investigations. As per Eifrem (2019), government and financial institutions encounter large amounts of data and ever-changing criminal landscape and so the need for graph technology becomes more of a necessity. The storage of data on a graph database platform may facilitate identification of hidden connections between entities which may go unnoticed in the case of RDBMS. It can be through the visualisation of a dynamic and complex data set, in the form of graphs, that users are led to a detailed overview of the data, so they may filter, select and look into the details of networks.

Consequently, strengthening the first line of defence against a financial crime such as money laundering needs to be considered. A shift from a traditional form of data storage to a graph database platform may aid in the fight against money laundering. The need is to be proactive rather than reactive to financial crimes. Illicit actors attempting to accomplish their objectives can be deterred using recent advances of machine learning, and big data infrastructure. Taking advantage of data-driven methodologies helps identify standard patterns from real data and so on to detecting outliers deviating from the norm. Various approaches for outlier detection have been developed. These include density-based approaches to identify points in low-probability regions, proximity-based approaches to identify points isolated from others, subspace-based methods to identify rare classes, and supervised or semi-supervised learning methods to learn differences between normal and abnormal classes (Aggarwal, 2015).

The International Consortium of Investigative Journalists (ICIJ) used graph technology to map complex financial transactions and detect irregularities. It aided in exposing crime in the offshore finance industry through its investigations which are famously known as the

"Panama Papers" and the "Paradise Papers". Since the inception of the investigation in 2016, graph technology has enabled in recovering over USD 1.2 billion in fines and back taxes (Dalby & Wilson-Chapman, 2019; Romera & Gallego, 2018). Another instance of the use of graph technology has been exhibited by Dun and Bradstreet (D&B). They use graph technology to accelerate clients' compliance with company ownership checks.

In comparison to rule-based counterparts, data-driven approaches are flexible and computationally intense. This fact strengthens the argument for using a graph database platform to store data concerning corporate entities. Such a move could initiate company service providers and corporate registries to fulfil their responsibility in the fight against money laundering.

The combination of search queries and pathfinding algorithms helps identify hidden patterns and links in the network of illicit entities which may go unnoticed in the absence of a graphical view of the data. The use of a graph database platform and utilisation of search queries and pathfinding algorithms to extract hidden links and patterns is in line with the views of Baker and Faulkner (1993) who suggested the use of archival data to derive relationships. However, it is suggested by Sparrow (1991) that looking at individual links between nodes is not sufficient, especially in the case of criminal network analysis. He stated that a criminal network suffers from three problems, which are, incompleteness (the inevitability of missing nodes and connections that the investigators will not uncover), fuzzy boundaries (the difficulty in deciding on the incorporation of information), and dynamics (the networks are not static; they are always changing). As a result, instead of looking at the presence or absence of a tie, he suggests considering the waxing and waning strength of a tie dependent upon the time and task at hand, and this could form the basis for future research.

The present work lays down the foundation for future research by importing the publicly available information of a network of illicit entities on a graph database platform. As per Rodriguez and Shinavier (2010), the presence of multiple relationship types between nodes may complicate the design of network algorithms; however, the presence of graph query languages will be able to overcome such complications. It provides the possibility of performing a more robust graph analysis than regression models to investigate the explanatory power of different metrics or combined metrics. More simulations on alternative network topologies could provide meaningful insights into the data. The present study suffers from

certain limitations which could also be looked into during future research. The incorporation of map co-ordinates for the addresses could facilitate a more granular analysis in terms of lending a vector component to the data. Additionally, the use of other graph algorithms could also be undertaken.

The next section highlights the graph analytics performed on the dataset and the results obtained.

4.3 Overview of modelling techniques

The extent of literature on money laundering, and framework for detection of techniques to be used by the launderer, was described in earlier chapters. This section briefly introduces and explains the relevant terminology and classifications of the detection models.

This is followed by a discussion of application of data-mining techniques identified from other review papers before providing an overview of prior research into detection from the perspective of graph analytics. The motivation and limitation to use graph-analytics for detection of money laundering is as follows.

First, money laundering exploits a web of disguised relationships and unravelling this complex network of connections is suited to a graph. These relationships include the methods of placing money, its movement in the financial system, and the organisational entities and their owners involved in the process. Furthermore, specific entities, most often shell companies, may play a transitory role within the network used to receive and distribute money. The representation of data in the form of graphs would establish the presence, if any, of a relational structure, and graph computations can provide a stronger relational inductive bias.

Secondly, it is in line with the observations of Singh and Best (2016) who state that approaches reducing the burden of excessive information may improve the capacity to identify suspicious activities and may contribute to the effectiveness of anti-money laundering effort.

An obstacle while coming up with a detection model is the lack of availability of data related to a particular type of fraud. It leads to the creation of synthetic data which match closely with the actual data. An exception to this is the work of Ravenda et al. (2015). They developed a model for detection of legally registered Mafia firms by using logistic regression to determine whether accounting information of Mafia firms was different from that of lawful firms.

In addition, studies in the past to detect illicit activities like money laundering have focused on banking transactions, which may not be publicly available and may increase the burden of tracking an audit trail. For instance, Savage et al. (2016) using data on banking transactions presented a system for detection of money-laundering activities through the use of a combination of network analysis and supervised learning. Luna et al. (2018) aim to identify shell companies by examining synthetic data of incoming and outgoing banking transactions along with its various attributes and using anomaly detection techniques. Singh and Best (2019) made use of visualisation techniques to identify patterns of suspicious money-laundering activities through application of link analysis in detecting suspicious banking transactions.

This overview of modelling techniques complements the following sections that discuss the application of methodology in the model development.

4.3.1 Introduction to modelling terminology and classifications

There is a lack of consensus on the definitions of interrelated terms used in the modelling literature and their overlapping with each other. A brief description is provided to assist the reader unfamiliar with modelling and more information can be found in introductory sections of reputable textbooks on data mining or data science such as that by Rokach and Maimon (2015) and Sathya and Abraham (2013).

Data science comprises of all processes associated with data ranging from generation or collection through to processing and analysis. Data mining, knowledge discovery, knowledge mining and machine learning are parts of data science. They are involved in discovery of useful information, patterns, rules or models from one or more data samples. The types of techniques used in data mining can be categorised as Classification, Clustering, Outlier Detection, Prediction, Regression and Visualisation (Gepp, 2015; Ngai et al., 2011; Sharma & Panigrahi, 2012). These techniques comprises models that learn from data and hence the name, machine learning. This learning can occur in several ways including supervised, unsupervised, reinforcement or stochastic learning (Sathya & Abraham, 2013). A hybrid of supervised and unsupervised learning is most relevant to this study and is explained in the context of illicit shell company detection below.

4.3.1.a Supervised and unsupervised learning methods

Supervised learning methods uses existing data to learn the relationship between the independent or explanatory variables and the dependent variable. This process to gain an

understanding of the relationship between independent and dependent variable is referred to as training a model. For an illicit shell detection, the dependent variable is often a binary variable that indicates whether it is either corrupt or non-corrupt. When the dependent variable takes on a predefined outcome (such as two, corrupt or non-corrupt), the resulting model is often termed a classification model.

Supervised learning methods learn from data comprising independent variables explaining a range of known values of the dependent variable. Unlike supervised learning that requires training data with specified outcomes for the dependent variable (corrupt or non-corrupt), unsupervised learning does not require information about the dependent variable. Consequently, there is no reliance on past data with classifications of either corrupt or non-corrupt that could be misclassified, and it can be an advantage of this type of learning.

As opposed to understanding the existing relationship between inputs and output, unsupervised learning methods look for any relationships in the data. An example of unsupervised learning is clustering. Anomaly detection can be a mixture of both supervised and unsupervised. Similarly, techniques such as neural networks can be trained using either supervised or unsupervised learning (Gepp, 2015; Sathya & Abraham, 2013; Sudjianto et al., 2010).

4.3.2 Application of data-mining techniques in detection

Elkan (2001) defines data mining as a process for obtaining unknown insights which are statistically reliable, and actionable from data which must be clean, available, adequate and relevant. Similarly, Lavrač et al. (2004) state that a data-mining problem should be well-defined, unsolvable by query and reporting tools and guided by a data-mining process model. It is applied to extract and uncover hidden truths behind large volumes of data, and this feature has led to its increasing use in coming up with a range of detection mechanisms to isolate illicit activities. Ngai et al. (2011), on systematically analysing 49 journal articles published between 1997 and 2008 on the subject of fraud detection, found extensive use of data-mining techniques such as logistic models, neural networks, the Bayesian belief network and decision trees in the detection of financial fraud.

The primary objective of a detection mechanism is to identifying suspicious or fraudulent applications and transactions. For instance, financial statement fraud detection involves distinguishing fraudulent financial data from factual data and hence disclosing

fraudulent financial behaviour or such activities. It would facilitate decisionmakers to develop strategies to decrease the harm done by fraud. There are specific attributes present in data for detecting each fraud type. For instance, crop insurance data would focus on ratios comprising the amount of compensation, and premium and liability figures; management data involving financial ratios would have components such as the allowance of doubtful debts and accounts receivables (Little et al., 2002).

Similarly, the data on home insurance are made up of customer behaviour and financial status (Von Altrock, 1996), whereas automobile insurance data involve binary indicators grouped into categories. The elements common to medical insurance data are treatment details, patient demographics, policy and claim benefits (Williams, 1999). Domain-specific attributes are exhibited in credit transaction data (Chan et al., 1999; Ghosh & Reilly, 1994), and in telecommunication data (Cahill et al., 2002; Cortes et al., 2003; Fawcett & Provost, 1999).

In order to ensure that a detection-mechanism is useful, it becomes imperative to consider the strategic interaction or moves and countermoves between a fraud detection system's algorithm and the perpetrator's modus operandi as it is cost-prohibitive to manually check the majority of external parties' identities and activities (Phua et al., 2010). For instance, in the case of application fraud, fraudsters apply for insurance entitlements using falsified information and apply for credit and telecommunication products and services using non-existent identity information or someone else's identity. In the case of transactional fraud, fraudsters take over or add to the usage of an existing, legitimate credit or telecommunication account. Additionally, it is essential to keep in mind that the volume of both fraud and legal cases will fluctuate independently of each other; hence, class distributions (proportion of illegitimate examples to legitimate examples) will change over time. Additionally, multiple styles of fraud can happen simultaneously. Each style can have a regular, occasional, seasonal or once-off temporal characteristic. Legal characteristics and behaviour can change over time. Once the modus operandi of perpetrators has been uncovered, they will supply new or modified styles of perpetration until the detection systems start generating false negatives again (Fawcett, 2003).

With the growing focus on illicit activities, the academic literature has focused on coming up with a wide variety of automated systems to detect them (Baader & Krcmar, 2018; Battaglia et al., 2018; Chang et al., 2008; Gepp, 2015, 2016; Gepp et al., 2018; Khaled et al., 2018; Ngai et al., 2011; Perols, 2011b; Phua et al., 2010; Ravenda et al., 2015; Sahin et al.,

2013; Song et al., 2014; Van Vlasselaer et al., 2017; Wedge et al., 2017). Chang et al. (2008) highlighted the use of a set of coordinated visualisations based upon keywords identification in wire transactions to detect fraud. The authors in depicting the relationship between keywords and accounts over time were able to detect transactions and accounts exhibiting suspicious behaviours. Phua et al. (2010) directed attention towards the limitation of data-mining fraud detection research in terms of lack of publicly available real data to perform experiments on well-established and accepted research methods and techniques. They addressed these issues by garnering all related literature for categorisation and comparison, selecting some innovative methods and techniques for discussion and pointing towards data sources as possible alternatives.

On a similar note, Perols (2011b) compared six popular statistical and machine-learning models in detecting financial statement fraud under different assumptions of misclassification costs and ratios of fraud firms to non-fraud firms. The study found that logistic regression and support vector machines exhibited better performance than artificial neural networks, bagging and stacking in detecting financial statement fraud. Sahin et al. (2013) developed a new cost-sensitive decision tree approach to detect credit card fraud aimed at minimising misclassification cost, and they compared the performance of this approach with traditional classification models. They found that a cost-sensitive decision-tree algorithm outperforms the well-known existing methods on the given problem set with respect to the well-known performance metrics such as accuracy and true positive rate, but also on the basis of a newly defined cost-sensitive metric specific to credit card fraud detection. Song et al. (2014), using a dataset containing 110 fraudulent firms and 440-non-fraudulent firms of equivalent size in the same industries presented a model for assessment of financial statement fraud risk. Bahnsen et al. (2016) developed a mechanism for detecting credit card fraud by addressing cost-sensitivity and features pre-processing to achieve improved fraud detection and savings.

Ngai et al. (2011), on reviewing English-language journal articles between 1997 and 2008, found an extensive application of data-mining techniques. They found an emphasis on the detection of insurance fraud followed by corporate fraud and credit card fraud. In contrast, they found a distinct lack of research on mortgage fraud, money laundering, and securities and commodities fraud. In recent times, areas such as bankruptcy prediction and credit risk have also received attention from academics. (Ezawa & Norton, 1996; Foster & Stine, 2004; Gepp et al., 2010; Kumar & Bhattacharya, 2006; Kumar & Haynes, 2003).

The works above are by no means an exhaustive list but they do provide a representative cross-section of the breadth of areas of application of detection through data-mining.

4.3.3 Graph analytics

Graph analytics involve analysis of the data by querying, using statistical methods, visualisation or incorporation of graphs into machine-learning tasks to provide insights into the data stored on the graph. The goal is to find suspicious individuals and relationships between them, and incorporate into this understanding any changes that might have taken place over time and structures of networks. Liu et al. (2016) classified graph analytics techniques in two categories, namely, the ego-net approach and the structural approach. The ego-net approach emphasises individual nodes and examines features from a node's local neighbourhood. The structural approach analyses network relations and looks for communities with secure connections or standard practice. Goyal and Ferrara (2018) categorised graph analytics related objectives into four categories, namely, node classification (determination of node labels based on other labelled nodes and network structure), link prediction (forecasting of missing links or occurrences of links in the near future), clustering (grouping of similar nodes through discovery of similar subsets) and visualisation (obtaining insights into network structure).

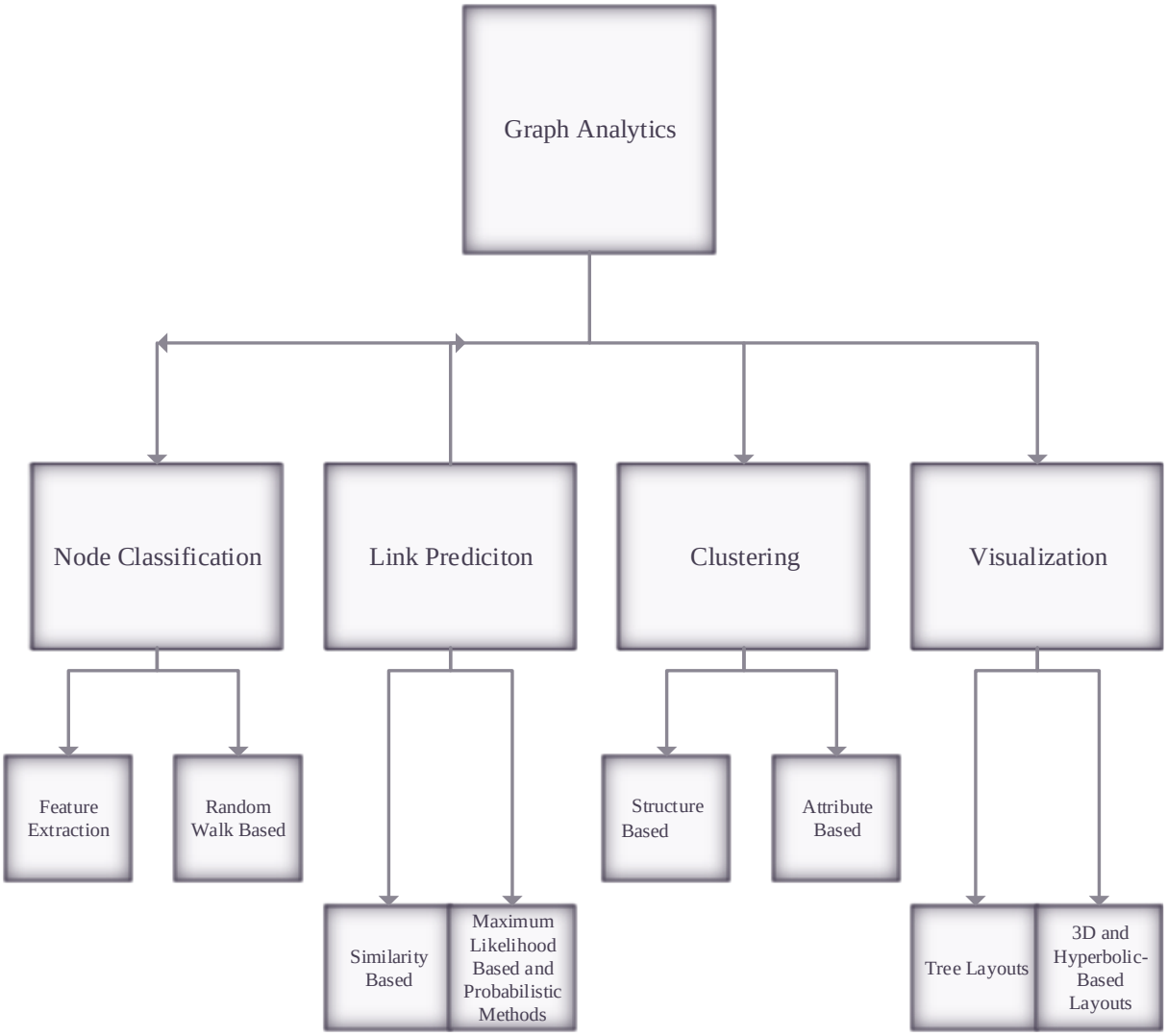

Figure 13: Classification of graph analytics

Concerning the Figure 13 above, the tasks related to graph analytics can be described as follows:

- Node Classification – In a network, there are nodes which may be labelled. The labelling of nodes varies depending upon the context of a network. For instance, in the case of a social network, node labels may refer to interests, relationships and so forth; for a corporate network, they may refer to the name and location of companies and their executives. However, at times, labels for a large proportion of nodes in a network may be unavailable. The prediction of these missing labels is known as node classification, and the approaches to predicting these labels are feature extraction-based and random walk-based approaches (Bhagat et al., 2011; Goyal & Ferrara,

2018). For feature extraction-based approaches, features for nodes are generated depending upon their local network statistics and neighbourhood and then by applying a classifier for predicting the labels. On the other hand, random walks propagate labels for the nodes in a network (Azran, 2007; Baluja et al., 2008).

- Link Prediction – In real-life scenarios, the construction of networks based on observed interactions between nodes may be incomplete or inaccurate. Link prediction predicts missing interactions or future links among entities of a network. The task has uses in terms of cost-savings (through attribution of monetary values to prediction accuracy) and development of relevant recommendation mechanisms (Goyal & Ferrara, 2018; S.-y. Wu et al., 2019). The algorithms used to predict links are classified into similarity-based, maximum-likelihood based and probabilistic methods (Adamic & Adar, 2003; Clauset et al., 2008; Katz, 1953; Liben‐Nowell & Kleinberg, 2007; White et al., 1976).
- Clustering – Network partitioning, more commonly known as clustering, refers to grouping of similar nodes into subsets; the approaches for these are structure-based and attribute-based clustering. Structure-based clustering could be further sub-classified into community-based clustering (to determine subgraph density with high frequency of intra-cluster edges and low frequency of inter-cluster edges) and structural equivalence clustering (identification of nodes with similar roles) (Ding et al., 2001; Newman & Girvan, 2004; Xu et al., 2007). In the case of attribute-based clustering, in addition to observed links, node labels are also utilised to cluster nodes (Zhou et al., 2009).
- Visualisation – The necessity for identification of patterns in data might have prompted the use of data for visualisation. Data for visualisation refers to technologies which facilitate users to see information for a better understanding and contextualisation (Singh and Best, 2016). The human ability to comprehend complex information visually aids in understanding large volumes of data visually and drawing concomitant insights. The transformation of data into visual representations facilitates suitable analysis (Thomas & Cook, 2006). As a result, graphs have found applications in a wide range of fields (Gansner & North, 2000; Theocharidis et al., 2009). Graphs may be in the form of the tree, 3D or hyperbolic-based layouts (Herman et al., 2000).

Overall, graph analytics make use of the relationship. They are used to uncover hidden information, perform hypothetical testing and make predictions (Needham & Hodler, 2019).

Documented in the literature is the potential in making use of graph analytics. There is a variety of algorithms and visualisations from which to draw inferences, leading to their diverse applications.

4.3.3.a Application of graph analytics

As per Becerra-Fernandez et al. (2000) and Hawking et al. (2005), representation of complex networks into graphs and their analysis would aid investigators to identify relevant patterns of activities. Bangcharoensap et al. (2015) supported the notion of using graph algorithm techniques such as PageRank, community detection and centrality algorithms in developing detection systems. Monge and Elkan (1997) proposed a find-union algorithm to detect database records that are near duplicates. Becerra-Fernandez et al. (2000) developed a system for assisting an analyst in discovering complex networks of potentially illegal activities by correlating through graph visualisations. Krebs (2002) used degree centrality and closeness centrality algorithms to map networks of terrorist cells. Similarly, Morselli and Roy (2008) used the betweenness centrality algorithm to determine the role of brokers in maintaining flexibility in criminal networks. Chang et al. (2008) developed a system for visual analysis of financial transactions through the combination of visual and textual approaches.

Vitali et al. (2011) used the strongly connected component (SCC hereafter) algorithm to identify the structure of international ownership along with the percentage of control held by each owner. SCC draws a picture on the level of entanglement in a network and has applications in explaining the reduction of transaction costs, anti-takeover strategies and risk-sharing. The extent of network connectedness indicates the level of intricacy in a network. Didimo et al. (2011) designed a system for discovering criminal patterns of money laundering and fraud. They used a combination of clustering techniques, novel graph algorithms and interaction functionalities for visually exploring networked datasets. Kido et al. (2016) proposed the application of the Louvain method for modelling of topics based on the detection of communities in graphs. It can be challenging to identify communities where members of the same community have more interactions with each other. In graph application, a community is a group of nodes with dense connectivity between them. The ability to find and analyse communities can provide more knowledge about the network's structure. Liu et al. (2016) developed graph analysis techniques with an application in real-world health-care datasets to detect fraud, waste and abuse activities. The representation of health care relationships through

heterogeneous graphs leads to the identification of relationships, anomalous individuals and communities through analysis of local and global graph characteristics. The graphical representation leads to a reduction in the list of suspects and focused investigation of suspicious individual or activity.

Commercial systems making use of graph analytics include Xanalys Link Explorer (Watson & Schneider, 1999), Netmap (Tracy et al., 2001) and i2 Analyst Notebook (Stewart & Rosemann, 2001). As per Peslak (2005), the applications as mentioned above involve classical layout algorithms such as circular drawing algorithms, hierarchical layout algorithms and force-directed algorithms for the representation of relational data. Needham and Hodler (2019) broadly classify graph algorithms into pathfinding and search, community detection, centrality computation and similarity algorithms. Each of these categories comprises various techniques under it.

In addition to graph search algorithms, pathfinding algorithms are used to explore routes between nodes by initiating at one node and traversing through relationships to reach the destination. These algorithms have applications in logistics planning and gaming simulation. Some of the commonly used pathfinding algorithms are the shortest path (finding the shortest distance between two nodes), all pairs shortest path and single-source shortest path (finding the shortest paths between all pairs of nodes or from a chosen node to all other nodes), minimum spanning tree (determining a connected tree structure with the least cost for visiting all nodes from a selected node) and random walk (considered to be an essential prerequisite for machine learning workflows and other graph algorithms).

Centrality algorithms help in determining the roles of nodes in a graph and the effect they have on the network. The objective is to identify essential nodes and draw inferences about the network based on that. It is essential to keep in mind that different centrality algorithms yield different results based on what they were created to measure. Some of the commonly used centrality algorithms are degree centrality (a baseline measure for connectedness), closeness centrality (the importance of a central node to the group), betweenness centrality (for determining control points along with an alternative for approximation) and PageRank (for understanding the overall influence).

The existence of a community is pervasive to networks of all types and identification of such communities could be critical in the process of evaluation of group behaviour and emerging phenomena. The underlying rationale in identifying communities is that members of

a community shall have more relationships within the group than with members outside it. Identification of communities has wide-ranging applications such as determining preferences of peer groups and preparation of data for further analysis. Some of the representative community detection algorithms are triangle count and clustering coefficient (for determining overall relation density), strongly connected components and connected components (for determining connected clusters), label propagation (for determining groups based on node labels) and Louvain modularity (used for examining group quality and hierarchies). Finally, similarity algorithms examine the similarity between nodes by using several methods such as Jaccard similarity to compare information such as node attributes.

Graph analysis techniques have become essential to find suspicious individuals, existing network relationships, unusual changes, geospatial dispersions, anomalous network structure and to facilitate the efficient handling of large volumes of data (Liu et al., 2016). It is in line with the observations of Singh and Best (2016) who state that approaches reducing the burden of excessive information may improve identification of suspicious activities and may contribute to the effectiveness of anti-money-laundering effort. There has been a focus on using graph networks to come up with detection models related to financial frauds. There exists a body of literature advocating the use of graph analytics techniques in detecting money laundering using suspicious banking transactions (Bolton & Hand, 2002; Chang et al., 2008; Didimo et al., 2011; Needham & Hodler, 2019; Singh & Best, 2016, 2019).

Savage et al. (2016) using data on banking transactions presented a system for detection of money-laundering activities through the use of a combination of network analysis and supervised learning. Luna et al. (2018) aim at identifying shell companies by examining synthetic data of incoming and outgoing banking transactions along with its various attributes and using anomaly-detection techniques. Singh and Best (2019) made use of visualisation techniques to identify patterns of suspicious money-laundering activities through application of link analysis in detecting suspicious banking transactions.

However, an obstacle while coming up with a detection model is the lack of availability of data related to a particular type of fraud. It leads to the creation of synthetic data which match closely to the actual data. An exception to this is the work of Ravenda et al. (2015). They developed a model for detection of legally registered Mafia firms by using logistic regression to determine whether accounting information of Mafia firms were different from lawful firms. Furthermore, studies in the past to detect illicit activities like money laundering have focused

on banking transactions. These may not be publicly available and they may increase the burden of following an audit trail.

4.3.4 Decision trees

Decision trees can be used for both regression and classification, respectively. Depending upon the purpose, they are known as regression or classification trees. They are usually binary trees that comprise a root node, other leaf nodes and non-leaf nodes connected by branches, such that each non-leaf node has two branches leading to two distinct nodes, as shown in Figure 14 below.

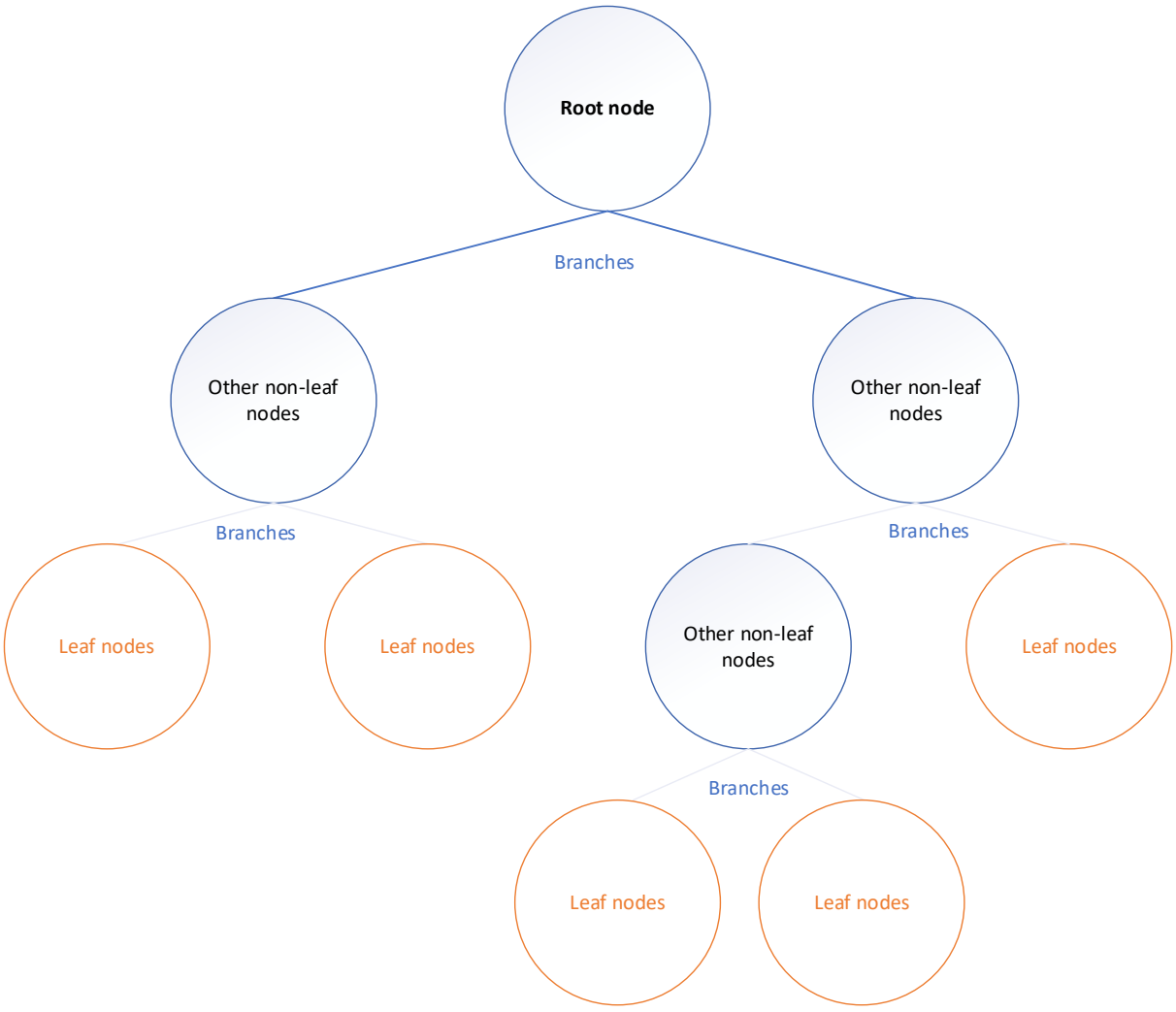

Figure 14: Structure of a binary tree

The construction of tree is through a recursive process of splitting the data when moving from a higher to a lower level of the tree. This process is described by decision rules that are associated with every non-leaf node including the root node decision. When applied to classification problems such as an illicit shell detection, leaf nodes represents classification groups such as corrupt or non-corrupt. A terminal node is assigned as corrupt or non-corrupt according to which classification produces the lowest error cost on the training sample. The tree structure models interactions between multiple explanatory variables that classify an entity as corrupt or non-corrupt depending upon generated decision rules.

Standard regression-based techniques are limited to modelling pre-defined interactions, and this is difficult and time-consuming, especially when there are many variables and many or unknown interactions. On the other hand, decision-tree interactions are more flexible and can correspond to specific regions of data compared with traditional interactions in regression equations (Gepp, 2015). This is an advantage over standard techniques because the appropriate transformation is not always clear in the real world (Derrig & Francis, 2008; Sutton, 2005).

The other advantages of decision trees include that they are non-parametric and are able to model interactions similar to artificial neural networks. Additionally, they are also transparent, visually representable and interpretable. Furthermore, decision trees are also immune to outliers and are easy to develop into automated systems. However, they also have disadvantages. A major disadvantage is that they do not produce an accurate probability of classification due to their inability to differentiate between cases classified into the same leaf node. Similar to artificial neural networks, their construction is sensitive to small changes in the training data set (Sudjianto et al., 2010) and they therefore perform better when trained on larger data sets. Consequently, the choice of the decision-tree building technique is important (Derrig & Francis, 2008) as there can be a large variation in accuracy between them. The tree building techniques determine how many nodes to include in the tree.

Sophisticated decision-tree software called CART (Classification and Regression Trees) based on the seminal work of Breiman et al. (1984) is sold exclusively by Salford Systems. Consequently, most trees are built using a two-stage process to:

1. Create a tree with many nodes, and then
2. “Pruning” the tree to a desired level of complexity by multiple node sub-trees with single leaf nodes, required for accuracy on holdout data (Breiman et al. 1984) .

Salford Systems claim that CART outperforms all competitors in terms of features, accuracy, reliability and robustness (Steinberg 2015). Additionally, CART provides classification accuracy to assess the relative importance of explanatory variables. CART- a variable importance score ranging from 0 to 100 highlights contribution of variables in the model.

4.3.4.a Bagging and Random Forests

Bagging (Breiman, 1996) is designed to improve accuracy and stability of individual models. It is based on repeated sampling with replacement. Samples are taken from the data; models are then fitted to each sample, and the results are aggregated to provide a classification (Sutton, 2005).

Random Forests (Breiman, 2001) is an example of bagging that uses decision trees. Random Forests using CART decision trees is a program exclusively available through Salford Systems, but other similar implementations are available. For each tree, Random Forests draws a random sample from the entire training data set and uses it to grow an unpruned tree using a different randomly chosen subset of explanatory variables at each node. The result is a form of dynamically constructed nearest neighbour classifier (Whiting et al., 2012).

Random Forests have advantages over single-decision trees in terms of increased stability through reduced variance and reduced sensitivity to the training data. Furthermore, they provide increased accuracy (Aldhous, 2012; Bhattacharya et al., 2011). A disadvantage of Random Forests is its black box nature caused by the complexity of a large number of trees.

4.3.4.b Boosting and TreeNet

The classification power of decision trees can be enhanced by iteratively applying the classification function and combining the output so that the classification error is minimised. Boosting is different from bagging in terms of assigning weights to incorrect predictions and use of simple classifiers (Gepp, 2015).

Stochastic gradient boosting (Friedman, 1999; Friedman, 2002) is a leading method of boosting. TreeNet, provided exclusively by Salford Systems, is the commercial product based on Friedman's work. This process also incorporates random sampling and uses the next tree to model errors from the current tree (instead of reweighting data) to improve results (Friedman, 1999).

Stochastic gradient boosting possess advantages over single decision trees in terms of increased stability through reduced variance and reduced sensitivity to the training data. Additionally, it provides increased accuracy. Moreover, stochastic gradient boosting is particularly good at classifications near region boundaries with smooth decision boundaries (Derrig & Francis, 2008; Whiting et al., 2012) and is capable of handling unbalanced data sets (Whiting et al., 2012). Once again, the drawback is the black-box nature of TreeNet. This ranking is very useful because variables have many opportunities to be used (as a result of many trees), and their importance is built up slowly one iteration at a time.

4.4 Graph algorithms

As per Mondragon et al. (2018), it is essential to use a combination of information from various sources to represent the information in the form of networks. They proposed a multi-link community detection method for multiplex networks based on extending link communities to a multiplex network framework, which aided in revealing the richness of such networks. Malinick et al. (2013) examined the importance of the location of individuals and their characteristics in print-media coverage using 2-mode data. They combined the data on social actors from public sources with their location to find that network centrality is associated with media coverage controlling for actor attributes. Hite et al. (2005) had used a network of school administrators from a qualitative paradigm using network theory and methods to observe the presence of multiple networks, thus suggesting that school administrators use multiple networks to achieve organisational objectives.

At times, the need to acknowledge that two or more of the given relationships can be joined to form a semantically meaningful compound relationship pattern is not given due importance. A heterogeneous network because of various node and relationship types involved has to explicitly define a set of semantic rules that describe the different relationships and their valid combinations (Memon & Wiil, 2014). Rodriguez and Shinavier (2010) state that the incorporation of multi-relational networks adds to the complication of network algorithms. However, the extensive application of path algebras to single-relational networks can be extended to multi-relational ones. Similar to path algebras, graph query languages such as 'Cypher', with different levels of expressivity, serve as a function for querying graphs for data. They facilitate the application of single-relational network algorithms to complex network data. The literature is still not consistent with the terminology used to define heterogeneous, multi-

relational, multiplex, multilayer, multi-modal and multi-modal and multi-relational networks. Efforts have been made to establish clarity around them (Aleta & Moreno, 2019; Memon & Wiil, 2014). However, outlining these inconsistencies is beyond the scope of this research.

This section applies algorithms aimed at identifying similarity, community and centrality of nodes in the network to come up with scores to be used for a classification model (the codes used for running the algorithms are available upon request). The literature comprises the use of community-detection approaches in tandem with other graph algorithms to yield better results. For instance, Seifoddini and Hsu (1994) in their study found better results when similarity coefficient based algorithms were used to identify communities. Similarly, Zuo et al. (2012) used a combination of PageRank, community detection and domain knowledge of brain regions to access changes in brain structures of individuals with age. Yao et al. (2018) classify community-based approaches as one of the categories to predict links among networks. The identification of communities could aid in inferring similar behaviour displayed by a group, assisting in discovery of a nested relationship, and preparing the data for use in further analysis (Kido et al., 2016; Needham & Hodler, 2019). It also has an application in identifying functional modules in biochemical networks (Raghavan et al., 2007). As per Hao et al. (2018), studies in the past have attempted to determine the influence of nodes in complex networks using a range of measures; however, studies do not consider overlapping communities in the network. On examining network structure and overlapping communities on the real-world networks, they found their proposed method to outperform several benchmark algorithms and found applications in large-scale networks.

Further, the studies consider the direction of the relationship between nodes to be outward. This is in agreement with the views of Hoffman et al. (1990) who, working from the argument of Emerson (1962) on power relations, stated that centrality in a sending network might increase an organisation's power relative to other organisations within the network. Similarly, centrality in a receiving network may add to relative dependence of the organisation in the network. In the context of a network of shell companies, nodes with outward links to other nodes would be more central, and hence the direction of relationship between nodes has been considered as outwards.

The below tables 10 and 11 provide a brief overview of the algorithm categories and the main measures under those categories that have been used as part of this study:

Algorithm Category	Overview	Motivation, Objective or Application
Similarity	• Similarity-metric based approaches compute the similarity of node pairs as per the attributes of a node or topological structures.	• Limitations of feature selection, unbalanced output classes and problems of computational cost make similarity-metric based methods attractive (Yao et al. 2016; Yao et al. 2018) • These approaches are simple and have exhibited superior performance on complex networks and outperformed machine-learning approaches in the past (Lu et al. 2017)
Community - Detection	• A community in a network can be categorised as a group of objects which are similar to each other and dissimilar from the remaining objects in the network. • The identification of communities could aid in inferring similar behaviour displayed by a group, discovering nested relationships and preparing the data for use in further analysis (Kido et al. 2016; Needham and Hodler 2019).	• A similarity measure is computed between objects, and a clustering algorithm is used to group those objects into families based on a corresponding similarity measure (Seifoddini and Hsu 1994). • The underlying principle is that similar nodes exhibit dense interconnectedness among themselves and sparse connectivity to objects in the network (Raghavan et al. 2007; Needham and Hodler 2019). • It also has an application in identifying functional modules in biochemical networks (Raghavan et al. 2007). • Luna et al. (2018) used companies with the same bank accounts to classify communities of shell companies in their study. • Gao and Ye (2007) analysed money-laundering networks through link analysis (comprising manual, graphical and structural approaches), community generation (using techniques such as K means and clustering to generate binary relationship-based communities) and network destabilisation (comprising power analysis, cohesion and role analysis to disturb the flow in-network)
Centrality	• Centrality algorithms facilitate understanding of the nodes' importance and group dynamics (Needham and Hodler 2019)	• The rationale to use centrality algorithms lies in a phenomenon known as homophily in network science. Homophily refers to the tendency that connections exist between fraudulent entities and these entities work in collusion to accomplish an objective (Bangcharoensap et al. 2015).

		• The most commonly used measures are Degree Centrality, Closeness Centrality and Betweenness Centrality, as proposed by Freeman (1978). As per Ruhnau (2000), all three measures depend on the size of the graph. • As per Chen et al. (2012), Betweenness Centrality and Closeness Centrality are prominent geodesic-path based ranking measures. • A well-known variation of the Eigenvector centrality is the PageRank algorithm proposed by Page et al. (1999).

Table 10. Overview of the algorithm categories used

Algorithm and Categories	**Overview**	**Brief Description and Application**
Jaccard Index – Similarity	• Paul Jaccard proposed the Jaccard Index in 1901 (Lü and Zhou 2011). The Jaccard index is used for information retrieval and is a normalised version of the Common Neighbor similarity algorithm by considering the influence of a node in the network	• It solves the problem of the Common Neighbour similarity algorithm by emphasising the links of non-influential nodes to make sure that the common neighbours among them exist because of their similarity and not their influence (Lu et al. 2017). • It measures similarity as a proportion of elements two objects have in common in comparison to elements that are not common to them. It is distinct from an index such as Cosine similarity which considers information related to vector similarity (Lewis et al., 2006). • The value for Jaccard Index varies between the range of 0 and 1 with a value close to 1 indicating a higher proportion of similarity; it can be used for community detection especially in the case of dense graphs (Raghavan et al. 2007; Needham and Hodler 2019).

Overlap – Similarity	• The Overlap Similarity algorithm, also known as Hub Promoted Index (HPI), aims at measuring the overlap between two sets (Lü and Zhou 2011). It considers the strength that weak connections share among themselves (Granovetter 1973).	• It considers the strength that weak connections share among themselves (Granovetter 1973).
Triangles and Triangle Count Algorithm – Community Detection	• In a graph network, triangle refers to a set of three nodes whereby each node is related to all other nodes in the set. The triangle counting algorithm aims at detecting communities by determining the number of triangles passing through each node in the graph network (Needham and Hodler 2019).	• The technique gained immense popularity in network analysis because of the size of networks such as the world wide web (Schank and Wagner 2005)/ • Van Vlasselaer et al. (2017) aimed at identifying companies intentionally going bankrupt to avoid tax payment. They did so by assessing the effectiveness of network information in social security fraud detection using network-based features such as triangles to identify such companies. • The importance of triangles is quantified by the clustering coefficient which is interpreted as curvature (Eckmann and Moses 2002).
Betweenness – Centrality	• Betweenness Centrality, as proposed by Freeman (1977, 1978), determines the influence a node has over the flow of information in a graph. It tends to find nodes that act as a bridge in a graph network between other nodes.	• Morselli and Roy (2008) examined the importance of brokers in criminal networks using the betweenness centrality algorithm. They found the position of a broker to be critical in resource pooling and coordination of activities.

Approximate Betweenness - Centrality	• Randomised – Approximate Brandes ("RA-Brandes") algorithm, also known as approximate betweenness centrality, enables fast calculation of approximate scores of betweenness centrality between nodes of a graph (Needham and Hodler 2019)	• It involves the calculation of shortest paths between a subset of nodes instead of all pairs of nodes in the graph. The nodes may be selected uniformly at random or there may be random selection of nodes with high degrees.
Eigenvector – Centrality	• Eigenvector Centrality was pioneered by the works of Katz (1953) and Bonacich (1972, 1987).	• It is based on the idea that the node is central if it is related to central nodes. The value of centrality instead of the number of adjacent nodes can be the determining criteria.
PageRank - Centrality	• PageRank Centrality algorithm, a variant of Eigenvector centrality, measures the connectivity of nodes (Needham & Hodler, 2019). • It involves traversing through a graph and computing the frequency of hitting each node during these traversals. • The algorithm provides a network centrality score in light of the entire graph structure.	• At times, the goal is to determine the importance relative to a small subset of the objects (Gleich 2015). • PageRank methods have been used in the past to study engineered systems such as road and urban space networks (Jiang et al. 2008; Schlote et al. 2012). • Zuo et al. (2012) used PageRank combined with community detection and known brain regions to understand the changes in brain structure across a population of 1000 people correlated by age. • Mooney et al. (2012) used it to determine changes in the network of molecules linked by hydrogen bonds among water molecules.
Harmonic – Centrality	• The Closeness Centrality algorithm aids in node detection in a graph that aims to spread information through a sub-graph. However, the performance of the algorithm is subject to the connectivity of nodes in a graph network (Needham and Hodler 2019)	• Krebs (2002) used closeness centrality scores to reveal terrorists in network cells vital for carrying out their operations. Colladon and Remondi (2017) used the closeness centrality measure to identify factoring businesses in Italy responsible for undertaking trade-based money-laundering activities • Marchiori and Latora (2000) used this as a representation of the average shortest path in their study of small-world networks. The algorithm is

	• A variant of closeness centrality, to address the issue of real-life networks of the absence of connectedness, is harmonic centrality, also referred to as valued centrality (Needham and Hodler 2019)	useful in ascertaining the importance of node across the entire graph rather than within its subgraph.

Table 11. Overview of the algorithms used

The study uses various combinations of similarity, community-detection and centrality algorithms (namely, Jaccard Index, Overlap Index, Triangles and Triangle Counting Algorithm, Betweenness Centrality, Approximate Betweenness-Centrality and Harmonic centrality algorithm).

The scores obtained in Neo4J on performing graph algorithms are retrieved. The scores are exported to CART with the binary predictor being corrupt (denoted by 1) and non-corrupt (denoted by 0) respectively. CART decision trees were assessed using a holdout sample of data on private limited companies incorporated in the UK.

4.4.1 Supervised approach

Supervised learning methods use existing data for learning the relationship between input variables and an output variable, a process referred to as training. Such methods can be used to train classification models on past (or simulated) known data before being used on new data. Supervised learning methods train models using a binary output variable. For illicit shell detection, the output variable is binary indicating either fraudulence or legitimacy.

Many different modelling techniques use supervised learning methods. Discriminant analysis and logistic regression, which are parametric modelling techniques, have traditionally been popular for analysing classification problems. In recent times, the use of non-parametric modelling techniques, which are more accurate and less distribution-dependent, have become prominent. These include decision trees, artificial neural networks, and ensembles of multiple decision trees such as TreeNet and Random Forests. To date, very few research studies on financial crime, especially illicit shell companies' detection, have used decision trees and ensembles of them.

The literature in the past has made use of supervised and unsupervised hybrids on labelled data (Cahill et al., 2002; Cortes et al., 2003; Phua et al., 2010). There has been growth of both supervised approaches, such as Decision Trees and Artificial Neural Networks, and unsupervised approaches such as link analysis and graph mining.

There are advantages in using decision trees; they are immune to outliers, are non-parametric, resistant to irrelevant variables, can easily model interactions between explanatory variables, are easy to interpret and simple to develop into automated systems. Decision trees have been used in the areas of medicine, engineering, finance and marketing as well as for fraud detection (Gepp et al., 2010; Ghosh & Reilly, 1994; Kumar & Bhattacharya, 2006; Kumar & Haynes, 2003). Link analysis and graph mining have been used in law enforcement, anti-terrorism and other security areas (Phua et al., 2010).

Decision Trees have applications in addressing problems related to regression and classification and therefore are commonly referred to as regression and classification trees respectively when addressing problems of the same nature. Al Hasan et al. (2006), in their study of the co-authorship network, laid down the foundation for extraction of features to be used in supervised learning for a systematic link prediction. They considered factors such as proximity and individual attributes to extract features from the network. They found that considering link prediction as a binary classification problem and using useful features in a supervised learning framework increased accuracy. The fact that features are so critically important emphasises the need for selecting appropriate features in data mining. On using the PageRank algorithm to rank features, Ienco et al. (2008), found that higher feature-ranking led to the influence of a node in a network and this resulted in greater classification accuracy.

On the downside, similar to artificial neural networks, decision-tree models suffer from being sensitive to small changes in the training data set (Sudjianto et al., 2010). However, newer ensemble techniques such as TreeNet overcome this issue and provide stable models that also make better classifications close to region boundaries. Salford Systems are the providers of CART decision trees (Breiman et al., 1984), TreeNet (Friedman, 1999) and Random Forests (Breiman, 2001). For this study, three algorithms were considered, namely, Decision Tree, TreeNet and Random Forests. The performance of these algorithms was observed using different performance metrics like Area under ROC (AUC), precision, recall and F-value. The scores obtained using various combinations of graph algorithms were used

for the classification models to compare the performance and determine whether the classification accuracy is consistent across them.

4.4.2 Results

The representation of the data with the schema, as described above, led to the identification of entities as part of independent cases of corruption linked to each other. It does denote the importance of the need to move to the graph database structure on the part of corporate registries to stop attempts to establish an illicit network in its initial stages.

The analysis involved the incorporation of similarities among nodes as relationships in the graph network to facilitate better results. This approach aligns with the works of Seifoddini and Hsu (1994), who stated that the use of similarity coefficients aids in flexibly incorporating various types of data for analysis. The use of community detection algorithms with centrality algorithms in the study is consistent with the work of Zuo et al. (2012) who used community detection with PageRank algorithm to better understand the changes in the brain structure. Once imported, several graph algorithms were performed, mainly related to determining similarities, communities and node importance. One of the underlying rationales was to establish a base for the interaction between network structure and node attributes, rather than just considering the importance of nodes in a network (because the latter takes advantage of only network structure, and not node attributes) (Backstrom & Leskovec, 2011). Additionally, the approach adopted in the study is comparable with the views of Hao et al. (2018), who state that such an approach allows accounting for overlapping communities. This can aid in determining node influence as the number of communities a node belongs to represents its propagation capacity. They do emphasise that metrics such as Betweenness Centrality and Closeness Centrality have no or little correlation with node influence.

On training and testing the data using Decision Trees, TreeNet and Random Forests as the primary classification algorithm and using a different combination of scores obtained from graph algorithms several performance metrics were obtained. These are provided in the tables 12-14 below:

Combination of Algorithm Scores	Classification Accuracy	Area under ROC Curve	Precision	Recall	F-Value
Jaccard, Triangle Counting, Approx. Betweenness, Harmonic and Eigenvector	91.88%	95.093%	97.50%	90.70%	93.98%
Jaccard, Triangle Counting, Betweenness, Harmonic and PageRank	97.85%	97.79%	97.67%	97.67%	97.67%
Jaccard, Triangle Counting, Betweenness, Harmonic and Eigenvector	92.47%	94.402%	97.50%	89.16%	91.93%
Overlap, Triangle Counting, Approx. Betweenness, Harmonic and Eigenvector	88.17%	92.116%	94.44%	79.07%	86.08%
Jaccard, Overlap, Triangle Counting, Approx. Betweenness, Harmonic and Eigenvector	93.55%	93.977%	95.12%	90.70%	92.86%

Table 12. Performance of Decision Tree with Different Combination of Algorithms

Combination of Algorithm Scores	Classification Accuracy	Area under ROC Curve	Precision	Recall	F-Value
Jaccard, Triangle Counting, Approx. Betweenness, Harmonic and Eigenvector	93.55%	98.95%	95.12%	90.70%	92.86%
Jaccard, Traingle Counting, Betweenness, Harmonic and PageRank	97.85%	98.140%	97.67%	97.67%	97.67%
Jaccard, Triangle Counting, Betweenness, Harmonic and Eigenvector	94.34%	97.977%	97.50%	90.70%	93.98%
Overlap, Triangle Counting, Approx. Betweenness, Harmonic and Eigenvector	94.62%	95.140%	97.50%	90.70%	93.98%

Jaccard, Overlap, Triangle Counting, Approx. Betweenness, Harmonic and Eigenvector	94.34%	96.442%	95.12%	90.70%	92.86%

Table 13. Performance of TreeNet with Different Combination of Algorithms

Combination of Algorithm Scores	**Classification Accuracy**	**Area under ROC Curve**	**Precision**	**Recall**	**F-Value**
Jaccard, Triangle Counting, Approx. Betweenness, Harmonic and Eigenvector	93.55%	95.558%	95.12%	90.70%	92.86%
Jaccard, Triangle Counting, Betweenness, Harmonic and PageRank	96.77%	97.349%	97.62%	95.35%	96.47%
Jaccard, Triangle Counting, Betweenness, Harmonic and Eigenvector	97.85%	97.302%	97.62%	95.35%	96.47%
Overlap, Triangle Counting, Approx. Betweenness, Harmonic and Eigenvector	91.40%	93.558%	97.30%	83.72%	90.00%
Jaccard, Overlap, Triangle Counting, Approx. Betweenness, Harmonic and Eigenvector	93.55%	96.72%	95.12%	90.70%	92.86%

Table 14. Performance of Random Forests with Different Combination of Algorithms

4.4.3 Implications

In 2002, an anonymous shell corporation called “Anglo-Leasing” was used to launder €24 million of the total €30 million as part of the contract awarded to the firm to update the passport system in Kenya. Information about the beneficial owners could not be identified because of the anonymity provided by such entities (Allred et al., 2017; Findley et al., 2015). Other such instances involving the use of shell companies include China ZTE using shell companies to evade US sanctions, and also SBM Offshore N.V., a Dutch-based group, paying bribes to shell companies owned by government officials (Hubbs, 2018). Shell companies in the UK have been linked to laundering of proceeds amounting to £80 billion (Houlder, 2017).

The International Consortium of Investigative Journalists (ICIJ) in its reports highlighted the intensive use of shell companies by Politically Exposed Persons (PEPs), to hold wealth in offshore centres; for instance, these may include influential politicians and sports personalities (Harding, 2016).

Shell Companies have legitimate uses such as facilitating reverse mergers, being used as holding companies or for protecting small entrepreneurs from bankruptcy risks. However, these entities have become instruments to launder dirty money to make it appear legitimate, and to hide information about the actual beneficial owners. Arms dealers, drug cartels, corrupt politicians, terrorists and cyber-criminals have become some of the frequent users of these shell companies. It has become easier to set up transnational companies, with a low level of compliance towards the Financial Action Task Force (FATF) standards. These have posed a challenge for law enforcement authorities in countering crime and corruption (Martini et al., 2019).

Cowdock and Simeone (2019), after conducting a forensic analysis of over 400 cases and interviews with academics and experts in the domain, pointed out the need to further corporate transparency reforms to prevent abuse of companies in the United Kingdom and offshore financial centres. It is necessary for jurisdictions such as the United Kingdom and Singapore to take up more responsibility, because they supply opaque offshore structures and thereby reduce the effectiveness of efforts towards transparency and integrity (Lasslett, 2019).

As per Nougayrède (2019), the recent focus to combat the illicit use of shell companies has been on the acceleration of intergovernmental measures to prevent tax evasion, money laundering and corruption such as the exchange of financial information across borders, with a view to increasing corporate transparency. The empirical effect of these measures is yet to be ascertained; however, there do exist potential limitations for their effective implementation. The limitations associated with effective implementation of regulations may be attributed to resistance from some jurisdictions such as the USA; there may be a lack of proactiveness of national regulators and enforcement agencies, and also poor quality of information maintained by local service agents. Consequently, to combat the illicit use of shell companies the need is to develop means to detect these instruments being used to hide the proceeds of bribery, corruption and tools for financing the acts of terrorism.

4.5 Conclusion

Chapter 3 developed a framework to provide insights into the techniques a launderer may adopt to wash funds among a range of available options. As uncovered in the literature review of Chapter 2, amongst the detection of money-laundering techniques, the detection of shell companies used to launder funds was found to be a subject under-researched. This chapter addressed that need by developing a model for detection of shell companies being used to launder illicit proceeds of crime. The opportunity rests in using the networks prevalent among entities in a corrupt network and analysing the links and similarities. The analysis would facilitate scores which could be useful in distinguishing corrupt entities from the non-fraudulent ones.

To the best of our knowledge, no prior study exists on facilitating models to detect illicit shell companies using publicly available information quantitatively, and this is where the originality of the proposed research lies. The study capitalises on the work of Baker and Faulkner (1993) who suggested the use of archival data to draw relationships among entities of a network, and this work bases itself on the hypothesis that a strong relationship exists between entities in a money-laundering network. This is also consistent with Bangcharoensap et al. (2015).

The key stakeholders to benefit from such models would include legal and compliance professionals and government officials, especially tax officials and anti-corruption NGOs. Also, regulatory agencies and banks with access to transaction information could use this alongside suspicious transaction analysis to increase the rate of discovery of entities they term suspicious. The developed model would assess the risk of a company being involved in illicit activities and whether there is a need to investigate further.

This chapter is a starting point in what can emerge as an essential area for future research. In an ever-changing landscape of regulations, the implementation of regulations can be challenging and so it would be interesting to determine if an alternative approach in combination with the existing regulatory framework could be more effective in combatting the problem arising out of intensive use of shell companies for illicit purposes.

The chapter lays down the foundation for future works on similar lines. It could involve the incorporation of distances between entities to assess whether entities within proximity might be used to misguide the authorities to accomplish illicit activities. The use of weighted

measures of relationships could also add to the accuracy of the model. For instance, Bangcharoensap et al. (2015) found that weighted degree centrality was a useful measure in distinguishing between legitimate and fraudulent users in their respective study. An experiment with more simulations on variations of network topologies along with weights on relationships could provide better information about the utility of metrics across network topologies. The incorporation of graph-embedding methods to the present study could be insightful. In terms of use of algorithms, the present study makes use of the traditional graph algorithms. However, the new algorithms as proposed in the literature for node influence could also be considered (Chen et al., 2012; Fei et al., 2018; Hao et al., 2018; Liu et al., 2018; Lv et al., 2019; Raychaudhuri et al., 2020; Salavati et al., 2019; Srinivas & Rajendran, 2019; J. Wu et al., 2019; Zhang, 2014). As per Lü et al. (2016), there is a need for further development in using centrality measures to identify influential nodes, and a benchmark of their performance could aid in the choices of measures in the future. Additionally, combining the graph analysis of publicly available information with banking transactions data could provide a more accurate result.

Chapter 5 Initial Coin Offerings (ICOs) As an Opportunity to Commit Fraud

* This chapter is based on a published paper in a peer-reviewed journal, namely: Tiwari, M., A. Gepp, and K. Kumar. 2019. The future of raising finance - a new opportunity to commit fraud: a review of initial coin offering (ICOs) scams. *Crime, Law and Social Change*.

Reprinted by permission from **Springer Nature. Crime, Law and Social Change: The future of raising finance - a new opportunity to commit fraud: a review of initial coin offering (ICOs) scams: Milind Tiwari et al 2019**.** DOI https://doi.org/10.1007/s10611-019-09873-2

The APPT framework (Chapter 3) had highlighted the possibility of technological innovations paving the way for new opportunities to commit predicate crime and launder funds. Amongst many, one such innovation which has contributed to this direction is blockchain. One use of blockchain is an Initial Coin Offering (ICO), a digital method of raising finance involving issuance of tokens in exchange for cryptocurrencies or fiat money. It is a cheaper, easier and quicker way to raise funds compared with traditional public offerings. However, it has raised a new opportunity for fraud and money laundering. An estimated ten percent of ICO funds have been lost to fraud. Using case-study analysis, this chapter determines characteristics of such fraud schemes and the regulatory changes made in response to them. The chapter reveals key lessons for investors in terms of proactive steps that can be taken to protect themselves from being victims, for issuers to ensure awareness and take steps to secure investors' trust, and for regulators to promote a safe environment. This chapter documents the effect of ICO fraud schemes on the regulatory environment, which is going through a series of amendments to provide protection against such fraudulent schemes. Additionally, it provides direction for future research to further investigate the risks of this new method of raising funds. This chapter helps in reaffirming the need to incorporate technological innovations as one of the elements of the APPT Framework.

5.1 Introduction

More than one billion US dollars were invested in blockchain technology in 2016 because of potential benefits that the technology may provide (Kennedy, 2016). The potential application of blockchain extends far beyond cryptocurrencies. The innovation and prominent use of blockchain technology have given birth to a new way of raising finance known as the Initial Coin Offerings ("ICOs" or "ICO"). This new method is a cheaper, more accessible and quicker way to raise funds compared with traditional public offerings. In an ICO, the issuer issues tokens to investors in exchange for other cryptocurrencies or fiat money during a specified time frame, sometimes to raise funds for development activities pursued by the issuer. The issued tokens will facilitate owner-access to services provided by the issuer or may be used as an independent virtual currency. The investment in an ICO does not grant ownership in the company, as is the case in an initial public offer (IPO), but is considered an investment in a virtual product which is likely to appreciate in the future. The appreciation is based upon investment in the technology provided, growth of business and increased demand for the virtual product being offered.

An ICO should not be confused with crowdfunding. Crowdfunding facilitates solicitation of investments or donations by providing a platform to leverage the geographical and social reach of the internet to connect fundraisers with a vast number of potential supporters (Fleming & Sorenson, 2016). The two methods of funding may appear similar, but they have essential differences. In terms of accessibility, crowdfunding is generally limited to a particular country or region, whereas ICOs are accessible to a broader range of investors. In terms of product, ICOs generally fund technology-related products while crowdfunding may span various categories such as hardware, software, technology and food. However, in recent times, ICOs have expanded beyond technology offerings. Differences also exist concerning crowdfunding and ICOs related to their regulations; the regulations related to ICOs and their evolvement will be briefly discussed in this chapter.

The excitement around other cryptocurrencies and the urge to be part of something innovative has led to a surge in raising funds through an ICO, particularly by tech start-up firms. In 2017, an amount close to four billion US dollars was raised through ICOs (Ernst & Young, 2017). This method of raising funds did not require compliance with securities regulations and hence provided a way to avoid compliance costs. It made it easier to pursue business development activities, especially for start-ups. There is no doubt that this new way

of raising finance is creating new opportunities, but at the same time, it has provided an opportunity to commit fraud. The frenzy around ICOs and lack of due diligence on the part of those investing in them provide an opportunity for fraudsters to efficiently carry out their operations, as is evident from the fact that more than ten percent of funds raised through ICOs has been lost to fraud (Ernst & Young, 2017).

Consequently, it is essential to examine the modus operandi of these large-scale fraudulent schemes to protect investors from falling prey to such schemes in the future and losing their hard-earned money. Additionally, it is necessary to be able to distinguish between potential fraudsters and genuine firms seeking to raise funds so as not to stifle the growth opportunities presented by this new fund-raising method. These modi operandi will remain a source of reference for regulators to consult as they improve the regulations surrounding such means of raising funds.

Research makes it clear that the risk posed by terrorism used to be underestimated as was the scale and extent to which it could affect people (Kotabe, 2005). A proactive approach towards ICO frauds might help prevent repeating the mistake committed in the case of terrorism. Consequently, the primary objective of the chapter is to analyse the instances of ICO frauds to determine the characteristics of such schemes. An analysis was conducted on cases available in the public domain. There are plenty of smaller, alleged ICO scams, but there is often little information about these, and the reliability of the information that is available is questionable. This problem does not exist with cases that government authorities are involved with and so they are the focus of this research.

It is essential to understand the regulatory environment and the historical changes that have taken place, as different countries have different regulations, and what may be considered illegal in one country may be acceptable in others (Kshetri, 2005). These differences provide opportunities to perpetrate fraud. Hence, the second objective of this part of the research is to cast light on the regulatory steps taken in different jurisdictions about ICOs and what is the current regulatory stance concerning them. The jurisdictions covered represent those in which either a clear regulatory position has been taken or in which meaningful ICO activity, in terms of the amount of funds raised, has taken place. The information provided can inform both issuers and investors of the country-specific regulatory developments in which an ICO is being offered and the extent to which the offering is compliant with existing or possible future regulations. The motivation is to aid genuine issuers in avoiding the cost of non-compliance

and for investors to check the degree of compliance of an ICO being offered, and to some extent determine its legitimacy and the security of the funds being invested. The provided discussion can also inform future policy initiatives relating to this emerging field.

The blockchain technology, because of its essential feature of virtual immutability, is being brought to a wide range of fields such as supply-chain and logistics, financial data verification and real-time updates of financial information. It has also provided a unique opportunity for firms to raise funds via ICOs to finance their operations. As pointed out above, ICOs differ from other methods of raising funds in terms of accessibility, cost, time efficiency, projects funded and regulations involved. However, the benefits of ICOs come at the cost of creating a new opportunity for perpetuating fraudulent activities. The present work is the first attempt to document the effect of ICO fraud schemes on the regulatory environment, which is going through a series of amendments to protect against such fraudulent schemes.

The research also contributes to the literature by providing critical insights for the concerned stakeholders (issuers, investors and regulators) to help them be proactive in countering ICO fraud. Proactive methods are outlined for investors to protect themselves. Information is provided for issuers to ensure awareness and to help them take steps to secure the trust of investors. Finally, insights are offered for regulators to aid them in providing a safe regulatory environment.

The rest of the chapter is organised as follows: the section on the blockchain provides an insight into the technology upon which ICO is based, along with its various uses and current application. It is followed by an introduction about ICOs and the regulatory steps taken in meeting the country-specific regulations. The chapter then provides an overview of four cases of ICO frauds, namely, AriseBank, RECoin and Diamond Reserve, PlexCorps and Benebit, to analyse their modus operandi in cheating the investors. Finally, key insights are provided for investors, issuers and regulators, followed by conclusions and potential implications.

5.2 Blockchain

One of the important technological revolutions of the 21st century has been the blockchain. A blockchain can be described as a digitalised version of a ledger which is decentralised and distributed among the users of its peer-to-peer network (Underhill, 2018). In simple terms, it can be understood as a text file which records events – for instance, transactions through consensus among participants of the network with no involvement of an intermediary.

The blockchain comprises a chain of blocks which essentially are a record of all transactions that have taken place in its network. This aggregation of transactions in units called *blocks* and their addition to similar existing *blocks* in a chain takes place through a cryptographic technique composed of what is called a *Proof of Work (Sullivan & Burger, 2017)*. *Proof of Work* is the mathematical procedure used to authenticate and validate transactions, and to add new blocks of transactions in a blockchain. The mathematical procedure in a blockchain network is performed by nodes called *miners,* and the act of using this mathematical procedure is termed *mining*. Once a transaction is *mined*, a solution is produced called a *hash*. It is demonstrated in Figure 15 – it has three blockchains; each hash is verified by comparison to the corresponding hash in the other blockchains. In this case, all hashes are consistent in each blockchain and so all are valid. In practice, there would be a much larger number of blockchains distributed throughout the entire network, which is why blockchain is known as 'distributed ledger technology' (DLT). The other simplification made in Figure 15 is that the hashes are two-digit numbers when, in reality, they are very long and complicated. It is crucial to notice that the *previous hash* matches the *new hash* of the previous block. For example, Block 3's *previous hash* of 34 matches the *new hash* from the previous Block 2, which is another level of validation. That is, each block contains information from both previous blocks and the current event, and the integrity and the authenticity of each item are checked against previous events. Since the hash value of the previous block is part of the computation of the hash value of the current block, it assures transaction history and saves time in verifying and tracing transactions to their source.

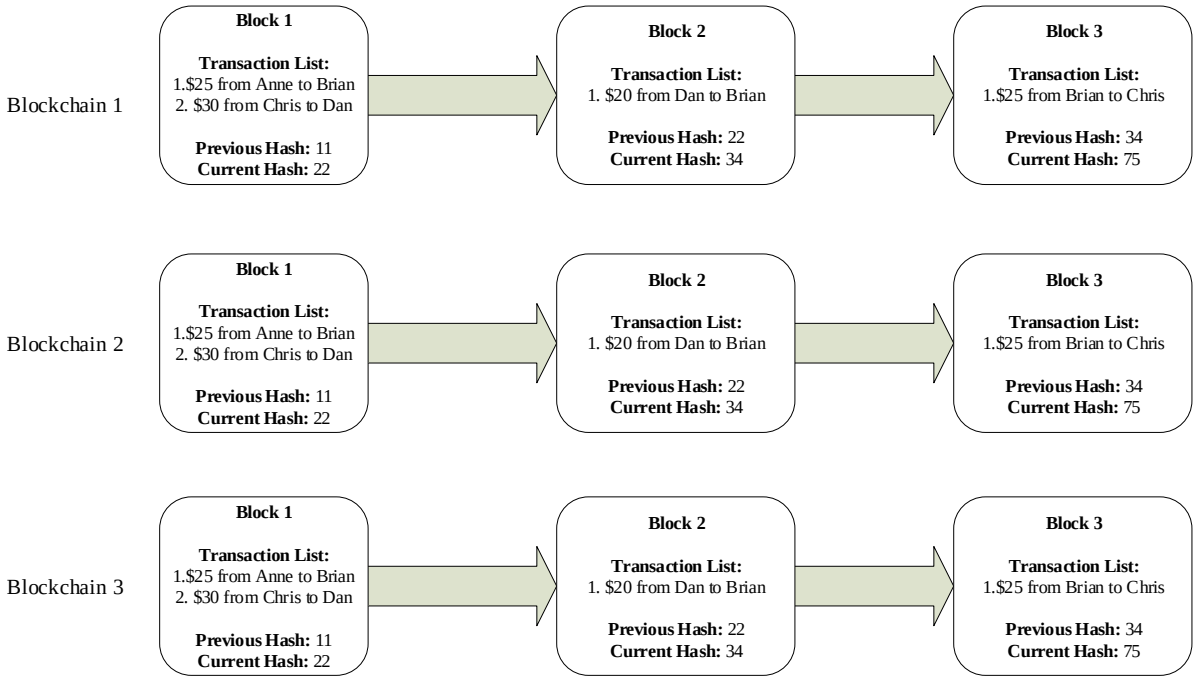

Figure 15: Example of Working Blockchain Network[3]

When any transaction or event takes place on the blockchain, the ledger gets updated for all users. That means in case of inaccuracy the hash solution produced will not match the hash in other blockchains in the network, which will result in it and future blocks on that chain becoming invalid, as demonstrated in Figure 16. In this case, consider that a hacker changed the amount from $20 to $30 in Block 2 of Blockchain 1. It results in a hash of 89, which is different from 34, the corresponding hash in the other blockchains in the network. Consequently, Block 2 in Blockchain 1 is invalid, which automatically invalidates all future blocks as well (Block 3 in this case). Thus, a hacker cannot successfully change only one blockchain, because the rest of the network will realise the data have been corrupted.

[3] The initial concept for this figure was provided by Alexander Lee, "Blockchain—A Visual Explanation," Medium, https://medium.com/@kkomaz/blockchain-a-visual-explanation-afe82d19a234 (accessed 15 February 2018).

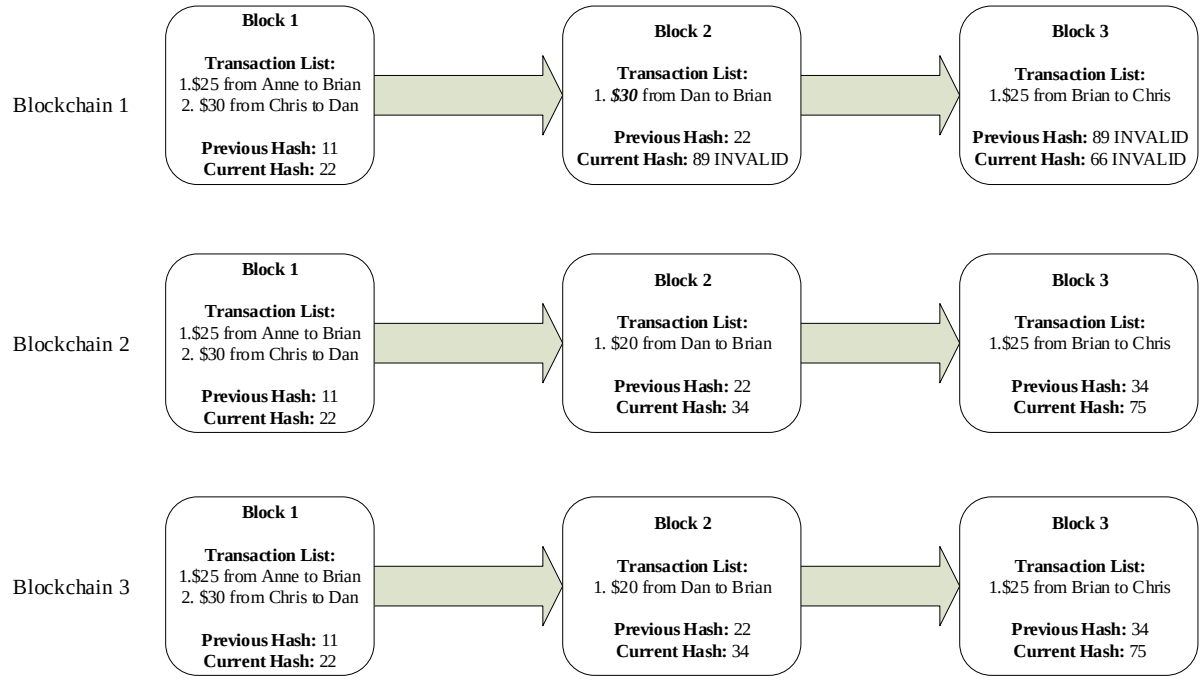

Figure 16: Example of a hacker modifying Block 2 of Blockchain 1 from Fig2

Blockchain can be broadly classified into two types, namely, public or open blockchain, and private or closed blockchain. A private blockchain is a closed network and requires permission for access to the network, and therefore it limits access to those who are thought to be known and trusted. On the other hand, a public blockchain does not require any permission to access the network. Consequently, anyone can have access by downloading and running the software required for the network (SEC, 2018).

One such example of a public blockchain is the Bitcoin, a virtual currency which facilitates transactions among its users in the absence of a central intermediary, that is, without a financial institution. Anyone can join the network by downloading the Bitcoin software and participating in the network. The blockchain of Bitcoin is updated when its participants validate a particular transaction. It is essential to understand that Bitcoin is just one example of a currency that uses blockchain. There are numerous others such as Bitcoin Cash, Ether, Litecoin, Tether and so on.

Satoshi Nakamoto proposed a version of electronic cash in 2008 that uses blockchain in the absence of a financial institution (Nakamoto, 2008). He proposed a way to avoid reliance upon trust by facilitating the use of coins authenticated by digital signatures and avoiding the problem of double-spending by recording the history of transactions immune to being changed.

The proposed system will be protected from an attack if the majority of participants in the network do not want the attack. Nakamoto's proposal was based on individual interest being collectivised and needed for changes to be incorporated through a consensus rather than a top-down hierarchical approach, using the network of participants to validate an event.

The main features of blockchain technology can be identified in terms of its decentralisation and encryption. It is depicted through its reliance upon its network of participants rather than a central authority and the ability for anyone to access the network and view the event at any time. Furthermore, the use of encryption in maintaining the security of the record of transactions allows the technology to have a variety of uses.

5.2.1 Uses of blockchain technology

Blockchain technology has uses beyond financial transactions. Businesses are interested in ways to improve accuracy and reduce the costs related to the hiring process (Moore, 2017). A human resource department can use blockchain for selecting better employees through having access to a wide variety of information about candidates that is known to be authentic and immune to tampering (Catalini & Gans, 2017). The data related to potential candidates would be stored in a virtual database that could be queried by human resource departments to obtain an authenticated pool of candidates meeting the required criteria. Additionally, job seekers would be able to exercise control over the sharing of their data.

Financial data related to companies could also be verified using blockchain-enabled databases that are accessed through the entity's website. As it is with real-time updates provided for bank account transactions, corporate financial information could be provided in real time (Gepp et al., 2018). The incorporation of blockchain technology could provide real-time verification in this process. It would provide transparency to financial statements and even highlight off-book transactions and accounts which are hidden (Tapscott & Tapscott, 2017). It would represent a big step forward in addressing the problem of financial statement fraud, the cost of which has been estimated at more than 1.2 trillion US dollars worldwide (Gepp, 2016).

The ability to provide real-time information updates through blockchain technology can also be utilised in legal matters, especially related to patent law where the timing of getting an idea recorded becomes essential. Real-time updates are also relevant to the logistic industry to facilitate tracking supplies of numerous parts in an efficient manner (Mansfield-Devine, 2017).

The maritime trading systems are plagued by security concerns relating to supply-chain issues (Barnes & Oloruntoba, 2005); blockchain could serve as a solution to this problem.

Blockchain technology can also be applied to contractual agreements, both short-term and long-term in nature. Furthermore, the technology can be used by companies to interact with customers on an individual basis to market their products. The data related to customers would be under their control, and it would not be possible for companies to profile the customers based on their online activity. However, customers could choose to grant companies access to their data, thus benefitting both the companies and customers by precisely matching the needs of both the parties. It would result in substantial cost savings through more efficient marketing.

Blockchain technology could also assure customers about the quality of a product or service. A likely application is within the precious stones industry (Knight, 2017). The technology is used to identify the source of procurement of precious stones as well as their authenticity. Each event or transaction in the blockchain is validated by the previous transaction, thereby ensuring that the asset, in this case, precious stones, is what it claims to be. Moreover, it helps to avoid the high degree of dependence on a central authority responsible for keeping track of records, thereby reducing the cost of tracking and storage of data (Mansfield-Devine, 2017).

In broad economic terms, blockchain technology offers multiple advantages: (i) reducing the cost of determining the authenticity and (ii) reducing the cost of establishing networks by avoiding reliance upon intermediaries (Catalini & Gans, 2017). The desire of a financial lending world without intermediaries could become a reality; however, such a transformation would also imply broadening the scope of regulatory implementation from national borders to a global approach (Lagarde, 2017).

5.2.2 Current application of blockchain technology

Apart from its widely publicised use in cryptocurrencies, blockchain technology is being used very actively by corporates and even by governments. One such example is in Estonia, where the government has implemented the technology in the application of its e-Residency program. It has enabled citizens to have improved control over and access to their electronic records. The use of technology in maintaining identity information also grants it security from data breaches because of the decentralisation (Sullivan & Burger, 2017).

Another application of blockchain technology is in global trade operations by Maersk, a global logistics and transportation company, which is partnered with IBM, a leader in providing blockchain technology solutions (IBM, 2018). IBM is also partnered with Sichuan Hejia Company Limited to take advantage of blockchain technology solutions in procurement of pharmaceuticals. Amazon Web Services (AWS) provides support to various blockchain applications such as Sawtooth, Corda R3, PokitDok and Samsung Nexledger, by providing a cost-efficient and secured development platform (AWS, 2018). It has been reported that the advantages of blockchain technology are being considered by other companies such as Walmart, British Airways, UPS, and FedEx (Krauth, 2018). Even the NASDAQ and New York Stock Exchange are trying to tap into the advantages of blockchain technology (Tapscott & Tapscott, 2017). The numerous advantages it offers beyond the present public view of cryptocurrencies highlight the tremendous potential of the technology and its capability to disrupt and transform current business practices.

5.3 Initial Coin Offerings

The use of blockchain technology has paved the way for raising finance through a new method. An essential feature is its virtual immutability which prevents a single user from making changes to the chain (as demonstrated in Figure 16 above). Consequently, this has resulted in firms using this technology to raise funds through an Initial Coin Offering (ICO).

An ICO, also known as an Initial Token Sales (ITS), refers to a digital method of raising finance whereby the issuer offers tokens to investors in place of other well-established cryptocurrencies or fiat money. The idea is to raise capital to finance future development activities of the business as well as to generate excitement and an established user-base for an entity's future offerings.

The creation and dissemination of coins (or tokens) in an ICO involve the use of blockchain technology, facilitating wide participation of investors. The ease with which funds can be raised and the growing popularity of ICOs are evident from the fact that a study on funds raised by 372 ICOs found that a total of USD 3.7 billion has been raised in 2017 (Ernst & Young, 2018). Start-ups generally view ICOs as an essential channel for raising funds (Underhill, 2018). However, with the growing popularity even established firms have launched or are planning to launch their respective ICOs, which is evident from the examples of Perth Mint and IAGON (Garvey, 2018).

The surge in fundraising through an ICO can be attributed to its being quick and cost-efficient. It is derived from the time and cost saved from compliance with securities laws and regulations which must be taken into consideration in the case of traditional methods of raising funds. Moreover, the use of blockchain technology attracts investors because it is an innovation with the potential to yield huge returns (Underhill, 2018). Investment in an ICO is different from investment in an IPO because the investment and ownership of coins acquired in an ICO do not guarantee ownership in a company, which is the case in an IPO. The ICO process begins with the announcement of an ICO by the issuer followed by marketing of the ICO through the company's website and other social media channels, and eventually the offerings of coins through an ICO within a designated time. The announcement of an ICO is accompanied by the release of a white paper, which can be considered similar to a prospectus in case of an IPO. The white paper contains information about the project, coins being offered, the rights available to investors, the lifecycle of the project, and other legal terms and conditions. It becomes necessary to understand that while the white paper serves a function like a prospectus, it is typically less detailed and does not adhere to any specified guidelines (Underhill, 2018).

The wide variety of ICOs also draws attention to the kind of coins being offered. At times, these may facilitate the holder to access products or services of the issuer or offerings which the issuer intends to develop from funds raised through the ICO (ESMA, 2017). Generally, this is the most common type of coin offered, where it facilitates access to services by payment exclusively through the coin. An example is the entity Token Report, which through an ICO offered Token Clarity coins, enabling users of those tokens to access databases dedicated to tracking other ICOs (Underhill, 2018). The other most common type of coins offered through ICOs facilitates users deploying them as normal currencies where acceptable, or being able to get them converted into fiat currencies (ESMA, 2017; Underhill, 2018). As per Lu (2019), partner at 256 Ventures (an early stage crypto-investment fund), the classification of tokens into "security" and "utility" tokens can be attributed to the US securities laws and may not apply to countries such as Australia. Consequently, Lu suggests a classification based on the rights the tokens generate. On reviewing literature across countries, he proposed a classification of tokens with a jurisdictionally neutral mindset. He classified tokens as:

- Investment tokens representing those that are considered assets and promise a financial return or benefit in the future,
- Utility tokens similar to digital coupons that provide participants with access or utility to an entity's product or service in the future and

- Payment tokens representing those which may be used as means of payment.

The coins in an ICO are usually offered through one of two formats. The issuer may issue the coins during or immediately after the sale. The other more common method is a pre-sale in which the coins are not developed for distribution and are scheduled for distribution at a later date (Underhill, 2018).

5.3.1 ICOs versus crowdfunding

According to Schwienbacher and Larralde (2010), crowdfunding can be defined as financing a venture by individuals instead of professional parties. Similarly, Mollick and Nanda (2015) refer to crowdfunding as funding projects by drawing small amounts of funds from a relatively more significant number of individuals without the use of standard financial intermediaries. In cases of crowdfunding, investors have clear expectations in place of their investment – in some cases they expect nothing and in others, they expect returns in the form of products, equity or monetary repayments with interest (Beaulieu et al., 2015; Gleasure & Feller, 2016).

Zetzsche et al. (2017) view ICOs as a combination of crowdfunding and blockchain. Crowdfunding and ICOs are similar in that their mechanism for raising funds allows investors early access to fund new ventures. Additionally, both provide an alternative mechanism for funding operations to businesses that are not of interest to venture capitalists or other institutional investors. Further, they do not rely on traditional financial intermediaries for raising funds and are generally cost-effective in comparison to an IPO.

However, ICOs and crowdfunding have fundamental differences. Crowdfunding involves the use of a central platform hosted by a third-party provider while an ICO makes use of blockchain and a decentralised peer-to-peer (P2P) network for raising funds (Schweizer et al., 2017). In an ideal scenario, crowdfunding platforms and banks serve as trusted entities for transactions whereas in the case of an ICO the verification of transactions takes place through a network-wide consensus (Arnold et al., 2019). In terms of accessibility, crowdfunding is generally limited to a specific country or region whereas ICOs are accessible more broadly. ICOs generally fund technology-related ventures while crowdfunding often spans various categories such as hardware, software, technology and food. However, in recent times ICOs have expanded beyond technology offerings, an example of which is providing tokens for real estate ventures (Bailey, 2018; Zmudzinski, 2019). There are also differences in investor

expectations and risk. ICO investors expect to earn a profit for their investment whereas crowdfunding investors may or not expect returns from their investment.

Additionally, in a crowdfunding project, investors have clear expectations about the outcome on completion, but clear expectations regarding the outcome from ICO funding is often absent. Differences also exist concerning regulations; regulations pertaining to crowdfunding are more certain and regulators have been overwhelmingly more positive towards crowdfunding. The less certain regulations relating to ICOs are discussed in the next section.

5.4 Regulatory steps towards ICOs in key jurisdictions

As of December 2017, there was no specific regulatory framework focused exclusively on ICOs, but the growing popularity, surge in volume of raising finance through ICOs, and the rise in fraudulent instances involving ICOs, prompted regulatory authorities across the globe to issue guidelines, make critical announcements and sometimes take action (Chance, 2018).

The regulatory developments and their evolution in jurisdictions that have taken a clear regulatory stance or in which a meaningful amount of funds has been raised through ICOs are discussed below.

- Australia

ICO activity has been on the rise in Australia. It is evident from the fact that the Perth Mint, one of the biggest gold refiners in Australia, is developing blockchain products backed by gold (Garvey, 2018). In response to this growing focus on ICO, the Australian Securities and Investments Commission (ASIC) issued guidelines about ICOs in September 2017 (ASIC, 2017). The guidelines aim to provide a clear sense of direction to businesses wishing to raise funds through the medium of ICOs. Through the guidelines, ASIC informed the businesses and investors alike that whether an ICO falls under the purview of Australian Corporations Act will depend upon the structuring and operations of the ICO as well as the rights gained through the ownership of coins offered through the ICO. Hence, if an ICO exhibits traits of a security, it will be subject to the Australian Corporations Act and if it does not resemble security, it will fall under the purview of Australian general and consumer law related to the offer of products or services (Chance, 2018). The main focus of the regulatory guidance issued in 2017 was the Australian Consumer Law and the

Corporations Act. In 2019, the regulatory guidance was updated to incorporate detailed obligations for cryptocurrency firms to comply with under the Australian Corporations Act, the ASIC Act and other laws. The guidance covered the requirement to hold an Australian financial services (AFS) licence and widened the scope of consumer protection.

- China

In September 2017, the People's Bank of China issued a circular banning ICOs (Borak, 2018), declaring them illegal, stating that ICOs may promote crimes of financial fraud, Ponzi schemes, illegal securities offerings and more (Chance, 2018). The Chinese regulators have been active in persuading foreign-listed Chinese companies to abandon plans for raising funds through ICOs. An example of this is Renren, a Chinese social networking website, which dropped its ICO plans in January 2018 (Yang et al., 2018). The Chinese government continues to maintain its stance against cryptocurrencies including the issuance of ICOs as illegal (Congress, 2018b; Williams, 2019).

- France

In October 2017, the French Regulatory Authority, Autorité des Marchés Financiers (AMF), published a discussion paper to obtain views of critical stakeholders relating to various possibilities of regulatory frameworks that can be applied to ICOs (AMF, 2017). The discussion paper considered the creation of a best-practice guide for ICOs. It also suggested extending the regulations surrounding them, and in fact developing an entirely new set of regulations. Additionally, the AMF announced a program to guide a framework regulating ICOs and protecting investors and issuers, called UNICORN (Universal Node to ICO Research and Network). The bill was passed in 2019 regulating the country's crypto industry including the establishment of a legal framework for ICOs. The bill provided the issuers of ICOs with an option to apply for approval from AMF if they complied with requirements such as (i) incorporation or registration within the jurisdiction, (ii) providing adequate information about the token, the project and the company and (iii) complying with the necessary anti-money-laundering (AML hereafter) and counter-financing of terrorism (CFT hereafter) requirements (Helms, 2019).

- Hong Kong

The regulatory authority in Hong Kong, the Hong Kong Securities and Futures Commission (SFC), released a press statement in September 2017, relating to ICOs (SFC,

2018). Consistent with the views of the Hong Kong Monetary Authority (HKMA), the SFC identified digital coins offered in ICO as a virtual commodity subject to regulations of Hong Kong securities law, depending upon the features they exhibit. Further, if the coin offerings fell under the definition of "security" then the activities of such coin would be regulated and subject to Hong Kong's product or licence authorisation requirement (Chance, 2018). The statement further warned investors of the risks of investments in ICOs. The regulatory authorities are still in the process of developing regulations to govern ICOs. As of December 2018, the SFC was set to tighten the regulations on cryptocurrencies including requirements such as ICOs for token which have been in existence for at least 12 months. The implementation of regulations is to take place in stages (Kihara, 2018).

- Japan

The amendments in the Payment Services Act (PSA) of Japan in early 2017 defined cryptocurrencies as "Virtual Currencies" and virtual currency exchanges as "Virtual Currencies Business Operators". The latter were required to be registered with Japan's Financial Services Agency (JFSA, 2017). As of December 2018, no regulations on ICOs existed in Japan and the need for a regulatory framework for ICO in Japan by JFSA is under evaluation (Chance, 2018; JFSA, 2017). In the meanwhile, the Japan Cryptocurrency Business Association (JCBA) came up with its recommendations on ICO regulations in 2019 (JCBA, 2019). The focus of the regulations was to expand cryptocurrency in Japanese domestic exchange, establishing clarity over the definition of and regulations surrounding security and utility tokens (Tashiro, 2019; Yakubowski, 2019).

- Russia

Russia is second only to the US in terms of the number of ICO projects originating from a particular country (Ernst & Young, 2017). The Russian government's approach towards cryptocurrencies has shifted from being cautious about acknowledging its presence and growth. However, at present, we found no regulations on cryptocurrencies. In June 2017, the Russian central bank along with the Ministry of Finance announced the development of regulations for cryptocurrencies (Chance, 2018). The Russian Ministry of Finances introduced a draft bill on digital financial assets in 2018. It limited the participation in ICOs to only qualified investors with exceptions to this condition to be decided by the Russian Central Bank. It also provided definitions for "digital assets" and "digital rights" (Congress, 2018a). The bill was ready to be enacted in January 2021.

- Singapore

Unlike that of many other countries, the approach adopted in Singapore towards cryptocurrencies has been positive (ACCA, 2018). In 2017, the Monetary Authority of Singapore (MAS) stated that if coin offerings through an ICO resemble a security offering, then it will be regulated within the purview of the Securities and Futures Act (SFA) (MAS, 2017b). Further, consistent with the US SEC, the issuers of such coins are required to put out a prospectus, and registration is applicable. Further, in a joint report with the Commercial Affairs Department (CAD), the financial crime division of Singapore Police issued a warning to investors about the potential risks of investing in ICOs (MAS, 2017a). The MAS updated its guidelines for businesses interested in raising funds through an ICO in 2018. It laid down guidelines for businesses to act in compliance with AML and CFT regulations. The guidelines required all the parties related to an ICO to comply with AML and CFT policies. Additionally, in 2018 it became a requirement to have a licence to issue ICOs and to advise on matters related to them (MAS, 2018).

- South Korea

South Korea ranks third after the US and Japan in the market for bitcoin trading and is the largest exchange market for Ethereum's cryptocurrency – the Ether (Kim, 2017). As per government data, around USD 89 million were raised in ICOs in September 2017 (Kim, 2017). As a result, just as with China, the Financial Services Commission (FSC hereafter), the South Korean regulatory authority, banned ICOs in the country (Kim, 2017; Nakamura & Kim, 2017). The regulatory authority cited a growing risk of financial scams and speculation as to the reasons behind the move. However, unlike the Chinese, the South Korean public could invest in foreign ICOs (Kim, 2017). In the first half of 2019, the FSC continued to maintain its stance of a ban on domestic ICOs on account of their being high risk. The stance was in response to a survey conducted by the Financial Supervisory Services (FSS) with respondents being companies who had conducted ICOs in foreign countries (FSI, 2019; Khatri, 2019).

- Switzerland

Switzerland has emerged as one of the key jurisdictions of raising funds through ICOs, raising 600 million US dollars, which is a quarter of the total funds raised in ICOs in 2017 (Australian, 2018). In September 2017, the Swiss Financial Market Supervisory

Authority (FINMA) stated that investigations were undertaken to probe the breaches of regulatory provisions by ICO (FINMA, 2017). The report further defined ICO as an initial public offering in a digital form that makes use of blockchain technology. Consistent with regulators in other countries, FINMA stated that the structuring of an ICO will determine the application of securities law, and if applicable, regulations relating to banking law, anti-money laundering and terrorist financing, among others, shall apply. The Swiss regulatory authority also warned the investors about the risks related to investment in ICOs. In a follow-up to the guidelines issued in 2017, FINMA then published guidelines regulating the treatment of ICOs (FINMA, 2018). FINMA determined the application of financial regulations on a case-by-case basis as each ICO is different. It further clarified its classification of tokens into payment (when used as means of value transfer), asset (when used as equity claim or debt) and utility tokens (when facilitating access to a service or application using blockchain-based infrastructure). Additionally, compliance with AML and CFT regulations for payment tokens was made mandatory (FINMA, 2018).

- United States

The United States of America was among the first countries to initiate the development of a regulatory framework towards ICOs. The laws and regulations applicable to ICOs in the USA vary, based on the location of the issue, the investors to which the ICO is being directed and the kind of services to be provided. Where an investment is made in an entity with a profit motive that depends on the managerial efforts of others rather than the utilisation of investment based on its functionality for personal consumption, then such coins will be considered securities and will fall under the purview of the regulator, the Securities Exchange Commission (SEC), and will be subject to its security laws (Chance, 2018; Tew & Freedman, 1973). In other words, if an investment in a coin offered through an ICO is made to earn profit rather than utilise the coin based on its functionality for personal use, then the coin would be considered a security and a subject of security regulations under the Howey Test (Chance, 2018).

To establish clarity about what falls under the purview of securities regulation, the SEC released an investigative report on an entity called the DAO in July 2017 (SEC, 2017a). The coins offered by DAO exhibited characteristics of a security. The SEC also stated that classification of coin offerings as security depends upon several factors and the assessment of a coin as security shall vary on a case-by-case basis; hence, at present no

applicable regulatory guidance exists on the issue (Chance, 2018). Further, in October 2017, LabCFTC, a division of the US Commodity Futures Trading Commission (CFTC), stated that if ICO coins do not meet the conditions of the Howey Test, they could be considered commodities and be a subject of their jurisdiction (LabCFTC, 2017). In May 2019, the SEC organised a public forum comprising experts from industry and academia to facilitate communication and a better understanding of DLT and digital assets (SEC, 2019).

- United Kingdom

In 2014, the Bank of England (BoE) played down the risk posed by cryptocurrencies to the stability of the UK's financial system (Ali et al., 2014). The Financial Conduct Authority (FCA) of the UK is yet to take definite measures towards the development of a regulatory framework for the ICO market in the UK. However, the FCA has been cautious about its approach towards ICOs and has warned against investing in them by terming them speculative and high-risk instruments (FCA, 2017). In 2018, the governor of BoE raised concerns over the need to regulate cryptocurrencies (Kharpal, 2018). In the context of the UK, any definitive measure regulating cryptocurrencies, including ICOs, is yet to be taken.

5.5 Cases of ICOs fraud

In 2017, in the US alone, the eagerness to bypass securities law using an ICO was evident from the fact that not one ICO was registered with the SEC. The lack of an established regulatory framework to regulate ICOs not only created confusion in the market for issuers but also provided an opportunity for people with ill intentions to carry out fraudulent activities relating to pump-and-dump schemes, pyramid and Ponzi schemes and even money laundering (Underhill, 2018). An ICO is an attractive opportunity for fraudsters resulting from a range of factors, including a lack of due diligence and information (DeVoe, 2018).

The issuance of a white paper accompanies an ICO, but unlike the contents of a prospectus, the information provided is not always accurate and detailed. Furthermore, the information cannot be verified, which leads to potential fraudsters using false information to mislead. Moreover, fraudsters may also create websites with vague and incomplete information. They may further make use of various social media channels and even use celebrity endorsements to attract the attention of investors in considerable numbers to perpetuate the fraud scheme on a large scale (Underhill, 2018).

There are numerous examples of ICO frauds such as Opair and Ebitz, Confido, Prodeum, OneCoin and Optioment. Recently, in April 2018 in Vietnam, over 600 million US dollars were identified to be lost to ICO fraud schemes through two ICOs, namely, iFan and Pincoin, but detailed information about the case is yet to be made public (Floyd, 2018). There are plenty of relatively small, alleged ICO scams, but because of a lack of reliable information, this study focused on cases that government authorities are involved with. The specific criteria for choosing the cases included (i) the case being discussed in online media and websites that specifically focus on cryptocurrencies, (ii) involvement of regulatory authorities in the investigation of such cases, (iii) the scheme garnering considerable attention from investors and (iv) a substantial amount being raised in the scheme. Four cases are discussed below. They have acted as a source for regulatory developments.

5.5.1 AriseBank

According to the company's website, AriseBank, also known as AriseBank Limited or AriseBank Foundation, LLC, was co-founded in early 2017 by Jared Rice Sr and Stanley Ford, with headquarters in Dallas, Texas. It was marketed as a decentralised bank with the ability to provide a wide range of banking products compatible with over 700 virtual currencies. Further, it was marketed as being among the world's largest platforms for cryptocurrency with the sole aim to establish it as a form of fiat money and change the dynamics of the banking sector (Aitken, 2018).

In October 2017, AriseBank launched its ICO and a test version of its banking operations. The ICO was promoted on social media, the company's website and through celebrity endorsements. Around the same time, it issued a white paper giving an overview of the products and the management team. The paper also gave a brief overview of the bank's digital currency called "AriseCoin" and its plan of offering it through the ICO. The AriseCoin ICO started in November with a "private sale", followed by a "pre-sale" in December. The bank released a press statement in January claiming to have raised around 600 million US dollars out of its goal of one billion. The coin distribution was scheduled for February 2018 (SEC, 2018).

In January 2018, a "Cease and Desist" order was issued by the Texas Department of Banking to AriseBank, prohibiting them from misleading investors about their engagement in the banking business in the State of Texas. Following this, the US Securities and Exchange Commission (SEC) filed litigation against AriseBank in the Federal District Court of Texas.

The SEC filed litigation to stop the issuance of securities by AriseBank for violating several sections of the US Securities Exchange Act on the following grounds(SEC, 2018):

- Issuance of unregistered securities

The securities law in the US makes it mandatory for companies to disclose their financial information by registering their securities with the SEC. The idea is to enable investors to make rational investment decisions based on available information. Since AriseCoin ICO was a security without registration of the coin or the bank with SEC, there was a violation of the Act. Also in 2017, the CEO of AriseBank Jared Rice Sr made false claims of AriseCoin not being a subject of regulations by the SEC.

- Use of misleading and false information

In January 2018, AriseBank made false claims about acquiring a Federal Deposit Insurance Corporation (FDIC) insured bank, KFMC Bank Holding Company, which facilitated offering secured services to its customers. However, no records supporting FDIC-insurance were found. FDIC had no records of any change in ownership involving the parties mentioned, rendering the claims to be false and misleading to investors.

Further, in its white paper, AriseBank claimed to offer its Visa cards that would facilitate payment for goods and services using any of the 700 cryptocurrencies that the customers could hold in their respective AriseBank account. It was stated that the card was being provided in partnership with Marqeta, a payment solution firm. However, the claims also turned out to be false when Marqeta publicly denied an association with AriseBank.

- Omission of material information

AriseBank provided brief information about the background of its executives on the company's website as well as in its white papers. However, none of these sources mentioned the criminal background of its two key executives. Such information would be necessary for investors in their decision-making.

As a result of the violations, the court froze assets of AriseBank and its co-founders and this ensured recovery of the various digital currencies held by AriseBank.

5.5.2 RECoin and Diamond Reserve

RECoin Group Foundation, LLC (RECoin) was a limited liability company incorporated in 2017 with its headquarters in Las Vegas, Nevada, and was marketed as a company involved in real estate investment and smart contracts for real estate through an ICO. Another such entity was Diamond Reserve Club, also known as DRC World Inc, which was incorporated in 2017 with its headquarters in San Juan, Puerto Rico. The principal business of DRC was the investment in diamonds through funds raised through an ICO. DRC was also marketed as obtaining discounts with retailers for investors in DRC. Both the companies were solely owned and managed by Maksim Zaslavskiy (SEC, 2017c). Between July and September 2017, Zaslavskiy raised 300,000 US dollars from investors in digital coins in RECoin and then DRC during their ICOs (SEC, 2017c).

The purported objective of these ICOs was the conversion of fiat currency or other digital currencies such as Bitcoin into a digital token that would derive its value from investment in an underlying asset. The underlying asset in the case of RECoin was real estate, whereas in the case of DRC it was diamonds. It was claimed that appreciation of investment or growth in business, or demand for coins, would drive the value of coins (SEC, 2017c).

In September 2017, the SEC filed litigation against Zaslavskiy and his companies seeking to stop issuance of securities for violating several sections of the US Securities Exchange Act on the following grounds (SEC, 2017c):

- Issuance of unregistered securities

  Since the securities being offered through the ICO of RECoin were not registered with the SEC, there was a violation of the Securities Exchange Act. Further, in the case of DRC, an attempt to bypass the registration regulation was made by Zaslavskiy through marketing the ICO as an Initial Membership Offer (IMO), offering membership in the entity rather than investment.

- Use of misleading and false information

  To attract investors, false and misleading claims were made by Zaslavskiy on various platforms such as social media, the companies' websites and in the ICO white papers. First, it was claimed that investment in RECoin and DRC ICOs granted investors ownership of digital coins when none existed. Secondly, it was falsely claimed that the RECoin ICO was successful in raising four million US dollars when only three hundred

thousand were raised. Thirdly, while none existed, it was claimed that RECoin and DRC had a team of professionals in the field to facilitate investments of funds raised. Finally, false claims were made about potential returns to investors from investment in these ICOs.

5.5.3 PlexCorps

PlexCorps, also known as PlexCoin and traded as SidePay.Ca, was an unincorporated entity controlled by Dominic Lacroix. As per the company's website, the company comprised a team of over forty professional experts dispersed across the globe and working towards the primary objective of increasing the accessibility of cryptocurrencies to the general public (SEC, 2017b). According to one of the white papers, PlexCorps was based in Singapore.

The PlexCoin ICO was launched through a pre-sale by PlexCorps in August 2017. The company's website stated that PlexCoin had the potential to become the mainstream cryptocurrency (SEC, 2017b). Further, one of the white papers declared an expected return above 13 times the original investment within a month (Shin, 2017). Subsequently, the PlexCoin ICO raised 15 million US dollars (SEC, 2017b).

In December 2017 SEC filed litigation against PlexCorps, Dominic Lacroix and his partner Sabrina Paradis-Royer, seeking to stop the issuance of securities for violating several sections of US Securities Exchange Act on the following grounds (SEC, 2017b):

- Issuance of unregistered securities

Since the securities being offered through the ICO of PlexCoin were not registered with the SEC, there was a violation of the Securities Exchange Act. Further, an attempt to bypass the registration regulation was made by Lacroix by marketing the coins being offered through PlexCoin ICO as cryptocurrencies rather than securities.

- Use of misleading and false information

In the circumstances similar to the previous case study, false and misleading claims were made by PlexCorps and Lacroix on various platforms such as social media, the company website and ICO white papers. First, it was claimed that appreciation in the value of PlexCoin tokens was based upon the investment of funds raised through the ICO. Secondly, PlexCorps's team was claimed to comprise over forty experts with the headquarters in Singapore. However, the claims were false as the entity had only a few employees, based in Quebec. Thirdly, claims were made to keep the identity of PlexCorps

executives hidden to avoid competition and issues relating to privacy. However, the main reason to keep the identity of Dominic Lacroix a secret was his record of being a violator of securities law in Canada. As a result, fake names were used to carry out the business activities and Lacroix's involvement in the business was denied. False claims were also made about potential returns to investors from investment in PlexCoin ICO.

- Misappropriation of funds

One of the objectives of the PlexCoin ICO was to raise funds to develop other products of PlexCorps, but a portion of funds raised through the ICO was misappropriated by Lacroix and his partner for personal expenditure.

5.5.4 Benebit

Benebit was a blockchain-based decentralized platform that facilitated interaction among geographically diverse entities (Top ICO List, 2018). The primary motive was to create a platform enabling customers to store and trade points from loyalty-based programs using cryptocurrencies (DeVoe, 2018). The company's website indicated the goal was a decentralised global network for virtual customer loyalty currency (Sedgwick, 2018).

Benebit's ICO pre-sale event was promoted by an ICO syndicate, a community of investors interested in ICOs. Benebit aggressively promoted its project, spending over 500,000 US dollars on marketing its campaign, hiring a public relations team and being active on social media. It drew the attention of potential investors and led to the development of a base of approximately 9,000 followers on a social media channel (Shome, 2018). However, the website and all its accounts on social media were pulled down once it was ascertained that the pictures of the management team were fake, having been taken from a school website. The scam resulted in the loss of investor funds to a figure somewhere between 2.7 million and 4 million US dollars (DeVoe, 2018).

There were two critical factors behind the success of Benebit's ICO scam:

- Element of Legitimacy

The considerable expenditure incurred from promoting the Benebit ICO led to a big following for the ICO across various social media platforms. It was further supplemented by positive reviews and high scores from various ICO reviewing websites, which granted

the Benebit ICO legitimacy, and convinced investors that the scheme was authentic (Shome, 2018).

- Lack of Due Diligence

One of the critical aspects of investing in a new opportunity involves conducting due diligence on the entities and its key executives. This process was overlooked in the case of Benebit, leading to the successful execution of the scam (DeVoe, 2018). Third-party promoters of Benebit did not undertake a verification procedure on the passport details of key executives of Benebit, which also contributed to the fraud being possible on such a large scale (Shome, 2018).

5.6 Key insights

The approaches to regulate ICOs differ across jurisdictions. Some countries such as China and South Korea have imposed an outright ban on ICOs, while the US has laid down clear guidelines around ICOs and others such as Malta and Singapore which have left no stone unturned in attracting businesses by providing a specific regulatory and administrative framework for ICOs (Lu, 2019; Mondaq, 2019). Malta, in particular, has earned itself the title of "Blockchain Island" (Mondaq, 2019). The presence of such a wide variation in the regulatory approaches and a continued lack of clarity at the global level makes it essential to have a set of guidelines to assist investors, issuers and regulators. Critical insights for these concerned stakeholders are discussed below.

5.6.1 Insights for investors

It is important to remember that not all ICOs are carried out with the purpose of cheating investors. However, investors need to take the necessary steps to protect themselves against the possibility of fraud. Based on the evaluation of the cases mentioned above, the following recommendations are made to investors to help them determine the legitimacy of an ICO.

- *ICO white paper*: Investors should not be enticed solely by the claims of the issuer and the marketing strategies adopted to lure them; instead, an investor should read all white papers in detail to understand the nature of the proposal and assist in determining its feasibility. Additionally, the long-term plans of the issuer concerning

the ICO should be evaluated; in most cases, this information should be mentioned in a white paper. A lack of clarity in long-term goals and objectives could be an indicator of fraud.

- *Offering's Utility*: A deep analysis of the value proposition of the product or service being offered through an ICO is recommended for investors to determine whether the proposal has sufficient benefits to warrant investment and whether it is feasible that these benefits could be realised. This information would be a useful indicator of the proposed ICO's legitimacy.
- *Management Due Diligence*: A detailed background check on all key executives would assist in determining the legitimacy of the proposed ICO. Thorough diligence would serve in protecting investors from fraud; this would include reverse searches of social media profiles, criminal record checks and an evaluation of past job history.
- *ICO Ratings and Reviews*: Investors should inform their decision-making from a variety of sources, including both the ratings provided by rating agencies and expert opinions available on multiple cryptocurrency websites. As is the case with traditional IPOs, in the case of ICOs the ratings and reviews do not guarantee protection, but they are still an excellent preliminary source of information to consider.

5.6.2 Insights for issuers

Prior scams where investors have lost their money have tarnished the reputation of genuine firms aiming to raise funds through ICOs. In light of the growing cases of fraud among them, it has become necessary for genuine issuers to provide as much information as possible to differentiate themselves from ICO scams and gain the trust of investors. The following recommendations are made to issuers.

- *Plain language:* Without compromising on accuracy, issuers should use plain language that is relatively easy to understand. This will aid investor comprehension and help to differentiate the genuine from the fraudsters.
- *Public disclosure of information*: To secure the trust of the investors, genuine issuers in all white papers should adopt the best practice of providing detailed information about their management team. It would facilitate verification background checks for management, something that investors are strongly encouraged to conduct.

- *Helpdesk*: As a best practice, ICO issuers should establish a helpdesk to answer the queries of investors and to explain the ICO offering and underlying technology if the investors require clarification. It is essential that this helpdesk also refers to professional financial advisors and third-party information sources such as government guidelines where appropriate.
- *Regulatory guidance*: In the absence of a clear, detailed regulatory framework, issuers are encouraged to seek guidance from the relevant regulators and develop a legal framework to avoid any issues in the future. It will become increasingly important as new laws and regulations are adopted. In addition to avoiding any compliance issues, this approach is also an essential step in building trust with investors.

The steps above are recommended as best-practice to issuers to increase transparency and provide improved assurances as to the legitimacy of ICO investments. It will help genuine issuers attract investors in the long run.

5.6.3 Insights for regulators

The uncertainties surrounding ICOs as new instruments make the role of regulators crucial. To ensure the safety of investors, and to provide a proper framework for issuers to adhere to, the following recommendations are made to regulators:

- *Dedicated unit*: Regulators should consider establishing a separate unit that exclusively investigates matters related to ICOs. It would allow the unique features of ICOs to be adequately considered. This dedicated unit could develop a tailored framework providing clear guidelines to potential issuers while safeguarding investors.
- *Low-cost compliance*: For many issuers, especially start-ups, a significant advantage of raising funds through an ICO lies in saving on compliance costs compared with a traditional IPO. As a result, to save on the cost of compliance, ICOs are viewed as a way of bypassing security regulations. A possible remedy is to establish a low-cost compliance framework for ICOs which would encourage issuers to comply with the regulatory framework and at the same time maintain the attractiveness of raising funds through an ICO.

- *Mandatory registration*: A mandatory registration requirement for ICOs signals to issuers that there is regulatory oversight, which is a subtle encouragement of legitimate behaviour. Registration may also provide investors with a sense of security regarding the funds being invested and promote an active marketplace.

A well-defined regulatory framework would establish clarity. This clarity would, in turn, encourage compliance from issuers. Investors would also be able to evaluate the extent of compliance associated with an ICO and use that information to assist them in determining the risk from investing in that ICO. As lower cost is one of the critical features of ICOs, regulatory frameworks must ensure the cost of compliance is relatively low to encourage compliant behaviour from issuers.

5.6.4 Notes on recommendations

At a broad level, these recommendations help to highlight the aspects to be considered by the relevant stakeholders so that an innovative opportunity for financing operations could be utilised to its full extent and hence yield returns to all those involved.

It is critical to understand that adopting the above recommendations for investors does not guarantee complete protection from ICO fraud. Instead, they are precautionary measures that can facilitate the discovery of fraud in the initial stages. For instance, in the case of AriseBank, following the recommendation of *Management Due Diligence* would have revealed the criminal background of the key executives involved. It would have acted as a red flag for investors in their decision-making or have been discovered by a dedicated regulatory unit. The same is true in Benebit, where the information about the management was fake.

5.7 Conclusion

A typical modus operandi for ICO fraudsters has been revealed from analysing four prominent cases. ICO fraudsters make attempts to attract investors using various social media channels and celebrity endorsements. Besides, information on the company websites and white papers is usually vague and intensively technological, and it presents the product in a complicated manner. Further, the old tactic of promising unrealistically high investment returns is present in all cases. Finally, the coins in the cases analysed were either offered in stages or were advertised to be offered at a discount for a limited period. The motive is to highlight the urgency and promote a fear of missing out on substantial investment returns.

The chapter provides implications for both investors and issuers. Investors should not jump on the first available opportunity to invest in an ICO. It is essential to read the white paper and to ensure that the concept adds value. The business motive for the ICO and the feasibility of the proposed product or service development should be evaluated. In the absence of regulations protecting the rights of those investing in an ICO, it becomes particularly important for a potential investor to conduct due diligence on the management team of the issuer. It is also essential to obtain views from various online forums about the project being undertaken through an ICO and views of rating companies. Traditional ratings given by the likes of Moody's and S&P do not guarantee the success of a company, and correspondingly, ratings given to companies aiming to raise funds through an ICO may not be completely reliable. However, it is an added measure which might be helpful to an investor.

The cases analysed should highlight a potential issuer about the need to adhere to regulations in order to avoid being subject to fines and penalties by regulators at a later stage. The issuers should evaluate their offerings to determine whether they qualify as a security or not and, if it is required, to obtain independent legal guidance. Issuers wishing to raise funds genuinely through an ICO need to overcome the negative association because of previous ICO scams. To build trust with investors, increased transparency is recommended through the public disclosure of detailed information using easy-to-understand language and establishment of a helpdesk to attend to any queries.

Regulators also have a pivotal role to play. There is a need for a regulatory framework specific to ICOs that protects investors while maintaining the low-cost advantage of ICOs as a method of raising funds. One recommendation is clear: the mandatory registration of all ICOs.

The adoption of suggested recommendations by investors and issuers, as well as the development of a tailored regulatory framework, will foster growth in the ICO market through reducing the prevalence of fraud. The findings lay a foundation for future research to analyse further ICO cases and develop a detailed best-practice guide concerning ICOs for all stakeholders and combat this new opportunity to commit fraud.

To further understand the need for APPT framework, detection mechanisms, and being aware of new technological innovations capable of paving the way for illicit acts such as money laundering, it becomes critical to recognise the magnitude of the problem. The next chapter of the thesis moves in that direction.

Chapter 6 Money Laundering through Cannabis in Australia

***** This chapter is based on a paper under submission to a peer-reviewed journal, namely: Tiwari, M., Gepp, A., & Kumar, K. (2021). The Evolution of Cannabis Regulation in Australia and the Overlooked Link with Money Laundering. (*Submitted for review: Criminal Justice Policy Review) (Rank: Q1)*

The need to address the problem of money laundering can be understood by getting an estimate of the magnitude of the problem. The review of existing literature identified a stream of research focusing on estimating the magnitude of money laundering (see Section 2.2.4). Within that stream in the review (see Section 2.2.4), it shows that there is still a need for more estimates to get a better idea of this magnitude. This chapter contributes by quantifying the amount of funds being laundered through cannabis trafficking in Australia.

Among a range of illicit activities, the money from drug trafficking is the most demanding for immediate laundering, and research work on money laundering would be incomplete without incorporating the contribution of drug trafficking to the amount of funds laundered. This chapter does that by providing an argument for possible policy implications on money laundering through the use of theoretical concepts of rational choice, individual decision-making and utility. It then empirically validates the effect of changes in cannabis regulations on the amount of money laundered, and finds some support for the argument that prohibitive measures towards cannabis use contribute to an increase in the need to launder the proceeds generated.

6.1 Introduction

As per the Australian Institute of Health and Welfare (AIHW), cannabis (marijuana) is the most often-used drug in the world and Australia (AIHW, 2017, 2020; UNODC, 2019). In 2016, the Australian federal government passed legislation to facilitate prescription of a range of cannabis-based products to patients by registered healthcare professionals (Lintzeris et al., 2020). Additionally, a bill to decriminalise the recreational use of cannabis subject to certain conditions came into existence with implementation in 2020 (ACT, 2019).

The work done around cannabis about its illicit consumption, medical benefits and regulatory changes has been a source of immense debate among policymakers, medical practitioners and academics alike. Keeping in mind the tremendous attention directed towards cannabis, its use and regulations governing it, the present study aims at assessing the development of regulations at a macro level on cannabis use in Australia through the lens of public-policy theories. It then attempts to present an argument to draw out its implications for money laundering. The presence of factors such as the high rate of illicit drug consumption and the prominence of cannabis, geographical isolation and lack of attitudinal shifts in regulatory changes makes Australia an exciting choice of study. To the best of our knowledge, a holistic assessment of the possible effect regulatory changes on cannabis may have on the extent of money laundering has been under-examined.

This study traces the evolution of cannabis policy regulations at the state and territory level in Australia through a review of published secondary data sources including peer-reviewed journal articles, government agency and media reports as indicated in the references. It then uses the concepts of rational choice theory, individual decision-making theory and utility to provide a theoretical view of the possible policy implications on money laundering.

The contribution of this study to the literature may be two-fold. First, the study through the use of multiple policy process frameworks applied to cannabis policy reforms at the state and territory level in Australia would increase the understanding around what enables or hampers policy change concerning cannabis. The use of multiple frameworks would aid in avoiding the limitation of using a single framework to explain policy change which may not be appropriate. The need to blend complementary policy frameworks can facilitate more considerable attention to a broader range of drivers that influence the move towards or away from a progressive policy change. Such knowledge may serve as a model for cannabis policy reforms in other countries as well.

Secondly, this study may result in an additional argument being incorporated in the debate around legalisation of cannabis use which has so far focused on health, crime, taxation, and education. Proceeds from organised crime's drug trafficking need laundering. The rationale to incorporate a high-level view of the effect of change in cannabis policy regulation in the quantum of funds laundered could be value-additional. It may not only aid in determining the effect the policy may have on the level of funds laundered but might also be critical in evaluating policy effectiveness. Such an argument would direct the attention towards its empirical validation. At present, data constraints limit the possibility of testing it empirically.

The rest of the chapter is organised as follows. The next section provides a brief overview of the work done around cannabis and an explanation of the link between money laundering, illicit drugs, and Australia as the choice of location for the present study. Then, the study describes the developments concerning cannabis policy that have taken place across Australian states and territories since 2001. The study assesses the development of cannabis regulations in Australia at a macro level through the lens of public policy theories, and endeavours to present an argument to draw out its implications for money laundering in Australia. Finally, we conclude, and direct attention to future research work.

6.1.1 Relevant literature

Researchers have paid considerable attention to understanding how drug policies are introduced or reformed (Hughes, Ritter, et al., 2017; Kübler, 2001; Lancaster & Ritter, 2014b; Von Hoffmann, 2016). Such an understanding facilitates the identification of elements critical for policy change. It lends transparency in observing the actors involved in the process, power dynamics, available knowledge, and expertise to shape the policy. In other words, a wide variety of factors, ranging from regulatory changes in other economies, to changes in the political regime, and the addition of new information to the knowledge pool, pave the way for a policy change.

Among a range of drugs, one such drug which has garnered attention of not only policymakers but also of academics, medical practitioners and media towards understanding its policy development and implications, is cannabis (Bogdanoski, 2010; Bresin & Mekawi, 2019; Chan et al., 2018; Chang & Jacobson, 2017; Chu & Gershenson, 2018; McGinty et al., 2016; Ritter & Sotade, 2017; Siklos-Whillans et al., 2020; Weatherburn & Jones, 2001). The changes in the cannabis policy landscape correspond with shifts in public attitudes towards cannabis often resulting from work in the domain and vice versa. For instance, Von Hoffmann

(2016) argues that the evolving international context in light of the growing debate around cannabis use, the role of epistemic communities and transnational activism explains Uruguay's drug policy reform of 2013 to legalise cannabis from seed to smoke. Such regulatory changes have continuously encouraged work concerning cannabis.

Lenton et al. (2000) and Baker and Goh (2004) found no increase in cannabis use when examining the effect of decriminalisation and depenalisation of cannabis use in three Australian states – South Australia, the Australian Capital Territory (ACT hereafter) and the Northern Territory, before 2001. Weatherburn and Jones (2001) found the illegal status of cannabis to be limiting its use through the application of a restraining effect on cannabis consumption with no effect on the prevalence of cannabis use. Ghosh et al. (2017) on analysing the effect of legalisation of recreational cannabis for the state of Colorado, USA, in 2014, found no increase in cannabis use for both youths and adults. Chan et al. (2018) assessed the changes in the level of cannabis use between 2001 and 2013 across socioeconomic status groups in Australia. The authors found a decline in cannabis use in Australia from 2001 to 2013, which occurred mainly among higher socioeconomic status groups. However, the research did not determine whether the people who stopped using moved to other drugs or simply stopped using all drugs. For the population with lower income or lower education, rates of frequent cannabis use remain unchanged. The study did direct attention towards the prevailing health inequality and a need to focus on disadvantaged cannabis users.

Chan and Hall (2020) on estimating the proportion of cannabis consumed in Australia by daily cannabis users found them to account for most of the total consumption. Such a finding has implications for jurisdictions that have legalised cannabis to impose taxes on cannabis products, strengthening social norms that discourage heavy consumption and restricting marketing practices directed towards heavy users. Shanahan et al. (2014), using a discrete choice experiment survey, assessed societal preferences for different cannabis policies, and found a strong preference for either civil penalties or legalisation compared to cannabis cautioning or criminalising the possession and use of cannabis.

In terms of observing regulatory differences, Bogdanoski (2010) reviewed the diverse legal approaches towards cannabis use in Australia, Canada and the US. Kilmer and Pacula (2017) directed attention towards the diversification of cannabis supply laws and the resulting challenges and opportunities arising out of it. They found a weak evidence base for assessing the strength of cannabis supply laws.

Apart from the regulatory changes (Ritter et al., 2011), medical benefits, other health effects (Lintzeris et al., 2020; Siklos-Whillans et al., 2020; Wang et al., 2018; Zahra et al., 2020) and changes in the proportion of cannabis use, attention has been directed towards other aspects such as (i) the type and extent of media coverage given to cannabis and its role in shaping public opinion and policy formulation (Hughes et al., 2011; McGinty et al., 2017; McGinty et al., 2016), (ii) additional factors influencing cannabis consumption (Livingston et al., 2020) and (iii) the effect on crime rates and educational outcomes.

Ritter and Sotade (2017) observed declining rates of cannabis use in Australia. Bresin and Mekawi (2019) in their meta-analytic review attempted to understand how various motivations for using are deferentially associated with cannabis use (frequency and quantity) and problems associated with cannabis use (reduced productivity, relationship conflict and legal issues). The authors categorised reasons for using cannabis, namely, to cope, for social commitment, mood enhancement, expansion of awareness and conformity. Such an understanding might have implications for intervention and policy development.

Chu and Gershenson (2018) examined the effects of cannabis use on intermediate educational outcomes in the USA. They found that medical marijuana laws affected college students in states with laws legalising cannabis for medical purposes. The students were found to spend approximately twenty percent less time on education-related activities and more on leisure activities than their counterparts in states with non-medical marijuana laws during weekends and summer when students had more time. However, the effect of such laws was heterogeneous and more prominent among part-time students with the likelihood of their being first-generation collegegoers and originating from underrepresented racial and ethnic groups.

The limited empirical evidence to support a positive or negative link between cannabis dispensaries and crime motivated Chang and Jacobson (2017) to assess the effect on crime in Los Angeles of short-term mass closing of hundreds of medical cannabis dispensaries. Interestingly, the authors found an increase in crime around dispensaries ordered to close relative to those allowed to remain open. Similarly, Chu and Townsend (2019) attempted to determine the effects of medical marijuana laws in the USA on violent and property crime and found no effect on criminality. On similar lines, Dragone et al. (2019) studied staggered legalisation of recreational cannabis on crime rates in Washington and Oregon, US. They found it did not increase crime.

The objective of the current study is not to provide an extensive review of the initiatives in the domain of cannabis but to highlight the breadth of work in the field.

6.1.2 Money laundering, cannabis and Australia

Money laundering can be understood as the act of giving dirty money a legitimate appearance. The United Nations Office on Drugs and Crime (UNODC) 2000 Convention (UNODC, 2004) defines money laundering as the process of converting or transferring the asset originating from a criminal source, to conceal the origin of the source or aid the criminal involved in committing the criminal offence.

There exists a range of methods to estimate the size of global money-laundering activity (Bajada, 2017). This results in varying estimates of it. For instance, the International Monetary Fund (IMF) estimated the aggregate level of money laundering to be between two and five percent of the world's annual gross domestic product or approximately USD 1.5 trillion (FATF, 2012). UNODC (2016) estimates the magnitude of global money laundering to be between USD 800 billion and USD 2 trillion. Similarly, Walker and Unger (2009) estimated it in Australia to be around AUD 4 billion in 2004. However, the estimates should be treated with caution as they are approximate.

Barone and Schneider (2018) state money laundering facilitates the use of illegal proceeds obtained from activities such as the drugs and weapons trades, cybercrime, corruption, human and wildlife trafficking. The likes of criminal activities mentioned are collectively referred to as predicate crimes and money laundering aids in drawing benefits from them. According to the Crime and Misconduct Commission (CMC), in the context of Australia, the common predicate crimes include drug trafficking, bribery, corruption, terrorism, white-collar and blue-collar crimes (CMC, 2005). The view that money laundering is the characteristic element following illicit activities such as illicit drug sales and corruption is supported by Mitchell et al. (1998a, 1998b) and Lyman (2011). The financial magnitude of illicit activities collectively referred to as organised crime can be determined from the works of Barone et al. (2018); (Barone & Masciandaro, 2011); Barone and Schneider (2018) and Reuter and Truman (2004).

The money from drug trafficking is the most demanding for immediate laundering (Hughes, Bright, et al., 2017; Paoli, 2014; UNODC, 2011). Consequently, Barone and Schneider (2018) assert that crimes leading to money laundering can be tackled through

legalizing drugs, driving out the need to hide proceeds from such activities. As a result, considerable attention among a range of drugs has gone to decriminalising cannabis for medical and recreational purposes. It is the world's most widely used illicit drug (UNODC, 2019).

For several reasons it is critical to consider the regulations around cannabis for a country such as Australia. First, the rate of illicit drug use is relatively high in Australia (Degenhardt et al., 2013; UNODC, 2015), which is intriguing given Australia's geographical isolation from global drug trafficking routes. Consequently, law enforcement may focus on domestic markets (Ritter et al., 2011), leading to additional risk for local traffickers and thereby resulting in higher prices for drugs (Global Drug Survey, 2015). On the other hand, the geographical isolation has also led to the popularity of the crypto market for illicit drugs by providing a new avenue for the procurement. According to the Australian Crime Commission (ACC) (ACC, 2015), the illicit supply of drugs is the biggest source of income for organised crime groups operating in the country and is generally associated with crimes such as money laundering.

Secondly, cannabis is one of the most consumed drugs in Australia with no price variation between online and conventional sales routes (AIHW, 2014; Cunliffe et al., 2017; Hughes et al., 2016). This consumption prominence creates a need to investigate cannabis regulations in Australia, particularly given the extensive debate across the world and the existing research evaluating the effect of cannabis use (Chan et al., 2018; Chang & Jacobson, 2017; Chu & Townsend, 2019; Dragone et al., 2019; Ghosh et al., 2017; Von Hoffmann, 2016; Wang et al., 2018; Zahra et al., 2020).

Thirdly, the lack of change in attitude in Australia towards cannabis consumption despite the regulatory changes in the country (Ritter & Sotade, 2017) provides an opportunity to focus on other possible implications of such regulatory change. The adoption of a prohibitionist approach makes it difficult to supply and procure cannabis for consumption and this in turn creates the need to launder the proceeds generated as a result of its sale. Consequently, it becomes interesting to consider the effect of changes in cannabis regulations on money laundering for Australia in the light of a lack of attitudinal shift.

The pro-legalisation and anti-legalisation arguments concerning cannabis have focused on criminal justice involvement and costs, tax revenues, education, public health consequences and crime rates. However, no study in the past has explicitly focused on the effect such regulatory changes might have on money laundering.

6.1.3 Cannabis policies in Australia

The legal frameworks governing the use and supply of drugs can be broadly categorised into a range comprising (i) full prohibition (considering the usage, possession and supply as a criminal offence resulting in a criminal record), (ii) depenalisation (involving lighter penalties for possession and usage but where supply remains a criminal offence), (iii) decriminalisation (criminal penalties are replaced with civil penalties, and drug supply remains a criminal offence) and (iv) legalisation (usage, possession, and supply remain legal) (Ritter & Lee, 2016). The drug policy reforms related to cannabis move around on this spectrum across the globe.

In Sweden, cannabis is not treated as less harmful than any other drug and the Swedes criminalise its possession and consumption. In the Netherlands, retail sales take place through coffee shops while cannabis production is prohibited. In Spain, cultivation and possession of cannabis are not criminalised, but the sale is. The procurement takes place through cannabis clubs which are private and non-profit organisations. The decriminalisation of cannabis in Europe was initiated by Portugal in 2001, followed by Estonia (2002), Belgium (2003) and later on by Poland and the Czech Republic (Chatwin, 2017; Kilmer & Pacula, 2017). Cannabis production and its use for recreational purposes were legalised in jurisdictions such as Uruguay and at a sub-national level in the US (Carliner et al., 2017; Dragone et al., 2019; Jacques et al., 2016; Kilmer & Pacula, 2017; Pardo, 2014; Von Hoffmann, 2016).

This study is not based on a legal analysis of national and sub-national drug laws. Its purpose is to overview the trajectory that regulations about cannabis have taken in Australia. Legislation in Australia is state-based with different penalties surrounding different drugs. Cannabis was decriminalised in three Australian States before 2001, namely, South Australia (1987), the ACT (1992) and the Northern Territory (1996). Similar to what has been observed in other countries, the decriminalisation and depenalisation did not increase cannabis use (Baker & Goh, 2004; Lenton et al., 2000). However, after 2001 the policy changes adopted a more prohibitive approach (Lancaster & Ritter, 2014a) up until 2015. In 2016, the Australian Federal Government passed legislation allowing for a range of cannabis-based products to be prescribed to patients by registered healthcare professionals (Lintzeris et al., 2020). The policy and legislative changes related to cannabis across states and territories in Australia (Hughes, 2020; Ritter & Sotade, 2017) have been documented in Table 15. There has been a shift from a prohibitionist approach towards a harm-reduction approach concerning cannabis policies

with cultivation for scientific or medical purposes legalised in 2015 and with further measures towards legalisation of cannabis for recreation in the ACT.

Year	**Jurisdiction**	**Policy and Legislative Changes**
2001	*South Australia*	Amendment to Cannabis Expiation Notice (CEN) resulting in a reduction of the number of cannabis plants attracting a fine on planting, taking the number down from three to one plant
2002	*South Australia*	Further amendment of CEN resulting in a ban on the cultivation of hydroponic plants
2003	*Western Australia*	Introduction of Cannabis Control Act 2003 to facilitate the issue of cannabis infringement notices
2004	*Western Australia*	Introduction of Cannabis Infringement Notice Scheme to facilitate personal use (decriminalisation)
	Victoria	Trial for roadside drug saliva testing for amphetamines and cannabis
2005	*Australian Capital Territory*	Simple Cannabis Offence Notice expiation scheme amended to reduce the eligibility criteria for the number of plants allowed and exclusion of hydroponically grown cannabis
	Tasmania	Introduction of roadside drug testing
2006	*New South Wales*	Increment in penalties for hydroponic cannabis
	South Australia	Commencement of random roadside drug testing
2007	*New South Wales, Queensland and Western Australia*	Introduction of Random Drug Driving Testing

	Western Australia	Review of Cannabis Infringement Notice resulting in expansion of scope to juveniles, reduction in the quantity of cannabis and increased fines for noncompliance
2008	*Northern Territory*	Adoption of roadside drug testing for amphetamines, cannabis and ecstasy
	South Australia	Increment in penalties against the cultivation of hydroponic cannabis
2009	*South Australia*	Adoption of strict regulation on the sale of equipment for hydroponic growth of cannabis
	Western Australia	Introduction of Unlicensed Driving Vehicle Sanctions affecting people who had their licence suspended under the Cannabis Infringement Notice Scheme
2010	*Australian Capital Territory*	Random Drug Testing Amendment Bill 2009 for testing of amphetamines, cannabis, and ecstasy
	Western Australia	Previous cannabis legislation replaced by stricter Cannabis Intervention Requirement (CIR) Scheme
2011	*Australian Capital Territory, New South Wales, Northern Territory, South Australia and Tasmania*	Imposition of a ban on the sale and use of synthetic cannabinoids
	Western Australia:	Making use, possession or cultivation of cannabis a criminal offence
2012	*South Australia and Victoria*	Banning sale of drug equipment such as bongs and cannabis pipes
2013	*Western Australia*	Introduction of offences concerning the sale and display of drug equipment incorporating anything that could be made or modified for smoking cannabis

2014	*Australian Capital Territory*	Introduction of Drugs of Dependence (Cannabis Use for Medical Purposes) Amendment Bill 2014 to allow use, possession and cultivation of cannabis for medical purposes
	New South Wales	Introduction of Terminal Illness Cannabis Scheme to facilitate police in not enforcing the law against registered adults and carers
	Northern Territory	Introduction of the Misuse of Drugs Amendment Act 2014 allowing police to charge a person with supply to the indigenous community of drugs such as amphetamines and cannabis
	Victoria	Introduction of Drugs, Poisons and Controlled Substances Amendment (Clinical Trials) Bill facilitating clinical trials of medical cannabis
2015	*Australian Capital Territory*	Passing of Crimes Legislation Amendment Bill 2014 to prohibit display but not the sale of drug pipes
	New South Wales	Regulatory changes to facilitate doctors' applications for prescriptions of cannabis-based medicines
	Northern Territory	Adoption of Traffic and Other Legislation Amendment Act 2015 to allow for random drug testing for methamphetamines, cannabis and ecstasy
	Victoria:	Announcement to legalise access to medical cannabis in exceptional circumstances from 2017
	Western Australia	Adoption of Misuse of Drugs Amendment (Psychoactive Substances) Act 2015 banning the sale, supply, manufacturing, advertising and promotion of

		psychoactive substances unless approved through existing regulation or legislation
2016	*Australian Capital Territory*	Announcement to establish a medical cannabis scheme as a priority
	New South Wales	Renaming of Terminal Illness Cannabis Scheme as Medical Cannabis Compassionate Use Scheme to evaluate its extension to non-terminal patients; authorisation to conduct medical cannabis cultivation research
	Queensland	Adoption of Public Health (Medicinal Cannabis) Act 2016 allowing medicinal cannabis products to be prescribed and dispensed to patients in Queensland
	Tasmania	Announcement to facilitate medical practitioners to prescribe medicinal cannabis for patients with severe illnesses through a Controlled Access Scheme (CAS)
	Victoria	Adoption of Access to Medicinal Cannabis Act 2016 to allow for lawful cultivation and manufacturing of medicinal cannabis products by patients with certain conditions and symptoms
	Western Australia	The Narcotic Drugs Amendment Act 2016 legalising cultivation of medical cannabis, prescription by a doctor and dispensing by a pharmacist
2017	*Victoria*	An inquiry into Drug Law Reform to monitor the effectiveness of laws, procedures and regulations concerning synthetic and illicit drugs and the misuse of prescription medication in minimising drug-related harm

2018	*Australian Capital Territory*	Proposition to legalise cannabis for personal use by removing possession of less than 50 grams of dried cannabis as a criminal offence
	South Australia	Issuance of Statutes Amendment (Drug Offences) Bill 2018 to increase penalties for cannabis possession
	Victoria	Proposition to legalise, regulate and tax recreational cannabis for people aged 18 and over
2019	*Australian Capital Territory*	Passing of The Drugs of Dependence (Personal Cannabis Use) Act 2019 to legalise personal cultivation, use and possession of cannabis for recreational purposes
	Northern Territory	Recommendation to amend the Misuse of Drugs Act to allow for uniform decriminalisation of cannabis use to address inconsistencies that exist in police discretion

Table 15. Cannabis policy changes at the state/territory level in Australia

The Drugs of Dependence (Personal Cannabis Use) Amendment Bill 2018 (ACT) (The Bill) was passed by the ACT legislative assembly in 2019 (ACT, 2019; ATODA, 2020). It resulted in amendments to the Drugs of Dependence Act 1989 (ACT) (The Drugs Act), the Criminal Code 2002 (ACT) and Medicines, Poisons and Therapeutic Goods Act 2008 (ACT). The Bill addressed issues about cultivation, possession and smoking of cannabis (TimeBase, 2019). According to the new legislation, residents aged 18 years or older will be allowed to grow cannabis plants at home. The limit will be two plants per person and four per household. The possession limit has been set to no more than 50 grams of dried cannabis per person. However, commercial sale of cannabis via retail outlets and supply of seeds or plants remains prohibited (Bright & Bartle, 2020). According to the ACT government, the use of cannabis is not legal but has been decriminalised by removing penalties for adults (aged 18 and over) who possess or use a small amount (ACT, 2020).

The Bill has received considerable support. The arguments provided in its favour involve (i) adaptation to new societal standards, (ii) drawing benefits of decriminalisation, (iii)

reducing stigmatisation, (iv) shifting the legal perspective of cannabis use from criminal justice to a health issue, (v) the creation of barriers to organised crime and (vi) the effectiveness of the harm-reduction approach. However, despite the support for the Bill, there exist elements in the legislation which are new and unfamiliar. Notably, the Bill lacks clarity on the enforcement of either the state or federal laws as possession for use and cultivation of cannabis is still a criminal offence under federal laws (Lee & Bartle, 2019).

6.1.4 Understanding cannabis policy development through public policy theories

The literature in the past has focused on understanding the introduction or reformation of drug policies (Hughes, Ritter, et al., 2017; Kübler, 2001; Lancaster & Ritter, 2014b; Lenton et al., 2000; Von Hoffmann, 2016). Such an understanding allows observation of actors, processes, knowledge and power dynamics interacting in policy formulation. Additionally, the deeply entrenched belief in prohibition shared by policymakers, government-backed investment agencies and a variety of advocates makes it challenging to transition to harm reduction. As a result, an understanding of how the change was brought about could be value-additional for other jurisdictions.

The process of policy change can be explained with the help of a range of theories. For instance, Sabatier and Weible (2014) list the following theories as the most promising to explain policy change: the Advocacy Coalition Framework (ACF), the Multiple Streams Approach (MSA), Punctuated Equilibrium Theory (PET), Diffusion Theory (DT), Internal Determinants Models (IDM) and Public or Institutional Entrepreneurship Theory.

Furthermore, Pivo et al. (2020) identify and categorise the factors, paving the way to monitor their interaction and explain the change through the use of the theories mentioned above. The first category is composed of factors affecting governing processes: collaborative group processes, coalitions and regimes competing for power, people leading, facilitating and informing decisions, organisational cultures and capacities, institutional laws, policies and governmental forms. The second category of factors encompasses social, economic, built and natural conditions where policy decisions occur. The final category of factors comprises policy features, such as their similarity and differences, which can influence the policy's chance of adoption.

Similar to the work of Townsend et al. (2020), this study draws on multiple policy process frameworks to formulate an understanding of the enablers or constraints explaining cannabis policy reforms in Australia at the state and territory level. We have used theoretical frameworks and triangulation of multiple data sources to understand the current state of cannabis policies in Australia. This results in attributing the policy change process to three theories at a macro level: the theories are DT (Walker, 1969), IDM (Berry & Berry, 2018) and MSA (Kingdon & Stano, 1984). These frameworks aid in understanding the state of cannabis policy reforms in Australia.

6.1.4.a Diffusion Theory

Diffusion Theory states that a government is influenced by policies adopted by other governments. The local policymakers may be influenced by successful policy outcomes in other jurisdictions, yielding to normative pressures, or may simply be influenced by mandates or incentives adopted by other regional, state, or federal governments. For instance, cannabis reforms in Uruguay have influenced governments across the world (Von Hoffmann, 2016). Similarly, in the USA the move to legalise cannabis for recreational purposes has been undertaken in nearly 30 states and the District of Columbia (Carliner et al., 2017; Dragone et al., 2019; Ghosh et al., 2017; Pardo, 2014). According to Kilmer and Pacula (2017), apart from the legalisation of large-scale cannabis production for non-medical purposes at the national or sub-national level, as of 2016 nine other countries permit (or will permit) cannabis to be supplied for medicinal purposes.

The move from a prohibitionist approach towards an approach more of harm reduction has been initiated in Australia because of the influence of the regulatory changes in the US and other jurisdictions. Within Australia, in addition to reforms internationally, the policy of one state or territory is influenced by the policies of others. The influence can be observed through the legalisation of cannabis for medical or scientific purposes, starting in 2015, followed by a move towards legalising cannabis for recreational purposes in 2020 (Hughes, 2020). The influence of policies in another state may be the reason for the change. Still, it may not be able to explain the pace at which the policy change takes place. For this, additional factors and theoretical frameworks need to be considered.

6.1.4.b Internal Determinants model

As proposed by Berry and Berry (2018), IDM emphasises the interaction of political, economic and social determinants in a given jurisdiction. The determinants may either

influence the motivation to develop innovative policies or else act as a hindrance in the development of innovative policies.

The policies adopted in each Australian state and territory may be ascribed to the interaction of the determinants above. For instance, in Western Australia, in 2001 the prohibition of cannabis use and possession with civil penalties was introduced, and further changes came in 2003 to allow for infringement notices. In 2004, changes were made to allow for alternatives to a criminal conviction relating to cannabis. In 2007, eligibility for the cultivation of cannabis plants was removed. In the same year, the Western Australian police commenced roadside drug testing for cannabis. In 2008, Western Australian Liberals were elected in coalition with the Nationals and Independents on a mandate to repeal the Cannabis Infringement Notice Scheme and provide a more robust response to the use of cannabis. In 2009, changes were proposed to make cannabis cultivation a criminal offence. A joint operation in 2011 led to the seizure of 29 kilograms of cannabis and AUD 25,000.

The state Organized Crime Squad seized AUD 20 million worth of drugs (cannabis and methylamphetamine) and assets in 2014. In 2016, in light of the changing public attitude towards cannabis, the government legalised the cultivation of medical cannabis. Further, it allowed for a doctor to prescribe and for a pharmacist to dispense cannabis. It was in line with new Commonwealth laws enabling access to medical cannabis, via the Narcotic Drugs Amendment Act 2016. Consequently, policy development through the mentioned example could be ascribed to the interaction between the determinants (Hughes, 2020).

6.1.4.c Multiple Streams approach

The theory emphasises, as proposed by Kingdon and Stano (1984), the importance of policy entrepreneurs in exploiting opportunities to promote specific policy choices. The policy choices are intended to address problems acceptably in whatever is the newly emerging policy situation. To formulate practical policy proposals, policy entrepreneurs combine elements, namely: problems, policies and politics. The problem stream is concerned with issues that are a priority for people or policymakers. The policy stream offers potential solutions to problems varying in cost, feasibility, acceptability, and situational utility. The politics stream combines the mood of the electorate, the views of pressure groups and the turnover in elected or appointed leaders.

In the Australian context, MSA can explain the development of cannabis policies to the present level. The problem stream comprises illicit consumption of cannabis, which has been an issue of concern from both the criminal justice and the public health perspective. Concerning policy, the solutions to the problem of illicit cannabis consumption consist of providing solutions on the spectrum, with prohibition and legalisation being the counterposed extreme ends (Ritter & Lee, 2016).

For a policy entrepreneur to provide a practical policy proposal, it would be essential to choose a solution addressing elements from the politics stream. For example, in 1996, to address the issue of cannabis consumption in Victoria, the Premier's Drug Council Report recommended cannabis decriminalisation and diversion. It failed to win support as Liberal backbenchers opposed it. The inclination towards the prohibitionist approach was visible even in 2010 when Leader of the Opposition Ted Bailleau proposed that upon election, he would impose a ban on the sale of bongs (an instrument for cannabis consumption) to communicate the harmful effects of cannabis on young people. The Victorian Liberal party was elected under Premier Bailleau in the same year under a platform of a strict zero-tolerance approach to crime. Subsequently, amendment to the Drugs, Poisons and Controlled Substances Act 1981 banned the sale, supply and display of bongs in Victoria (Hughes, 2020).

In 2014, Opposition leader Daniel Andrews announced that, if elected, the Labor Party would put the issue of medical cannabis to the Victoria Law Reform Commission, in order to find a legal path for the consumption of cannabis for medical purposes. In the same year, the Coalition Government introduced a bill to facilitate clinical trials of medicinal cannabis and later in that year the Victorian Labor Government under Premier Andrews was elected. Subsequently, upon recommendations from the Victoria Law Reform Commission's Medicinal Cannabis report, legal access to medicinal cannabis from 2017 in exceptional circumstances was announced. It resulted in the adoption of the Access to Medicinal Cannabis Act 2016 (Hughes, 2020).

These policy changes were in line with the changing public attitude towards cannabis. According to the National Drug Strategy Household Survey 2016, community tolerance towards cannabis consumption increased with more support towards legalisation and less support towards the imposition of penalties for sale and supply (AIHW, 2017). At the time of the 2018 Victorian election, proposals to legalise, regulate and tax recreational cannabis for

adults aged 18 and over were made (Hughes, 2020). The exploitation of opportunities to promote specific policy choices is evident through the combination of multiple streams.

6.1.5 The effect of regulations on money laundering

In recent times, the global cannabis policy landscape has been witnessing a transition. There has been a shift from prohibition to medical decriminalisation or from medical decriminalisation to recreational legislation across economies at national and sub-national levels (Wang et al., 2017). The policy question of several debates is whether it is better to continue to regulate cannabis as a legal product, prohibit it unconditionally, or adopt the middle road of decriminalisation. Social commentators and academics alike have argued that prohibitionist measures may increase victimisation and retaliation by reducing access to the law (Jacobs & Wright, 2006; Jacques & Wright, 2013; Rosenfeld et al., 2003). Such measures may restrict a supplier's access to formal means of dispute resolution in case of wrongdoing, and according to Jacques et al. (2016), this may encourage violent retaliation. Additionally, there exists a notion that drug policies intended for public protection based on prohibition and criminalisation have had detrimental effects on public health. They drive people who use drugs away from health services and contribute to stigma (The Lancet, 2016).

To conclude, from a communication research aspect, the framing or focus on specific aspects of an issue can influence its appeal to the audiences and influence public policy support (Scheufele & Tewksbury, 2007). The aspect focused on by anti-legalisation arguments has been adverse public health. In contrast, the pro-legalisation arguments have directed attention towards criminal justice and economic issues such as a reduction in prison overcrowding, decline in racial disparities in cannabis arrests, an increase in tax revenue and creation of new jobs (McGinty et al., 2016). However, the possible effect regulatory changes on cannabis may have on the extent of money laundering has been under-examined.

According to Schneider (2010), the volume of turnover of organised crime rose to USD 790 billion in 2006 compared to USD 595 billion in 2001 in OECD countries. As documented in the literature, money laundering is a typical element following illicit activities constituting organised crime. As a result, the rise in revenue generated out of organised crime increases the prominence of laundering. Further, among a range of illicit activities, the main contributor to the proceeds of organised crime is drug trafficking (Paoli, 2014; UNODC, 2011). Finally, among the various drugs available, the most widely-consumed illicit drug worldwide and in Australia is cannabis (AIHW, 2020; UNODC, 2019). Consequently, a critical implication more

often than not ignored in public policy debate around the effectiveness of decriminalisation could have been to assess the change in cannabis policies on the quantum of money laundering. A decriminalised drug market would result in eradication of illegality which so far has been paving the way for the need to launder funds. This is consistent with the economic approach of Becker (1968) to crime.

This chapter uses Walker's gravity model (Khan et al., 2018; Walker & Unger, 2009), to estimate the proportion of funds that could have potentially been laundered in Australia because of cannabis. It uses the prices of cannabis available from the Australian Criminal Intelligence Commission's (ACIC) illicit drug data reports and the UNODC database (ACIC, 2016, 2017, 2018, 2019; UNODC, 2020). The prices and the quantity of cannabis seized annually are combined to come up with a lower estimate of the proceeds of crime that would have been available for laundering resulting from cannabis had it not been detected. Once the proceeds available for laundering are known, the gravity model can be used to determine the proportion of funds that would have been laundered in Australia. The changes in cannabis regulations can be used to gauge the effect of such regulatory changes on the amount of funds laundered.

No study attempts to provide a foundation to focus on the effects of changes in cannabis policy explicitly on the amount of money being laundered. From the sellers' perspective, the prohibitory approach to cannabis sale encourages the sellers to look for alternatives to make illicit sales and consequently creates the need for laundering. Ceteris paribus, the primary thrust of rational choice theory, predicts that given a prohibitory approach to cannabis, the expected utility of mobilising channels to launder funds will be higher for illicit dealers (Gilmour, 2016b).

From the perspective of rational choice theory, the need to launder funds might decline. The regulatory changes play a critical role in assessing the need to launder the proceeds, and this is a relevant factor influencing the decision of sellers and suppliers (Clarke & Cornish, 1985; Piquero, Gibson & Tibbetts, 2002). Decriminalisation is situated between legal regulation and prohibition on the drug market legality continuum. The current cannabis regulatory developments across Australia as documented above have been towards decriminalisation.

From an economic perspective, the cannabis regulations focus on trade-offs between harms of drug consumption (which may be physical, mental, and social), perceived benefits of

consumption and harms from illegal markets. The harms from consumption are outweighed by the consumption benefits and harms from illegal markets, and this supports the need for behavioural policies instead of blanket prohibition (Rogeberg, 2018). A policy with optimal tax level would not leave the legal market outcompeted by the illegal market. Still, it would aid in reducing the incentive to launder funds and consequently would contribute to the actual assessment of the economy. The rationale is that since the prohibition makes illegal the revenue generated from cannabis consumption, a need to launder the proceeds arises. The perspectives considered in this chapter provide a theoretical argument on the possible results of changes in regulations from prohibition to decriminalisation and legalisation, and the amount of funds laundered.

6.1.6 Estimating cannabis proceeds available for money laundering

This chapter takes a step further to empirically evaluate the effects of changes in cannabis regulations on the amount of funds that could have been laundered in Australia. It considers the prices of cannabis from 2003 to 2017 to determine the proceeds of crime which would have been available for laundering had cannabis not been detected. The information on the per gram prices of cannabis was obtained from illicit drug data reports and the UNODC database (ACIC, 2016, 2017, 2018, 2019; UNODC, 2020). It is important to note that the price information provided in these reports was collected for all police jurisdictions in Australia and is based on information provided by covert police units and informants. There exists a lack of reporting standardisation as some reports contained price information per ounce while others reported price per gram, as provided in Table 16. It may result in a quantity discount factor not being taken into consideration. Hence, the quantity discount factor is used to derive the prices in case the price information per ounce is unavailable (for 2007). For ease of calculation, the purity levels in cannabis, different cannabis variants, and the purpose of usage (recreational or medicinal) are not taken into consideration.

Cannabis Type	**Original Unit of Reporting**	**Source of Information**	**Year**	**Price Information IDDR**	**Price Information UNODC**	**Effective Average Prices (IDDR)**	**Quantity Discount Ratio in IDDR Prices**
Outdoor	price per ounce	IDDR	2003	AUD 150 in NSW to AUD 250-360 in	-	9.05	

				Queensland per ounce			
Outdoor	price per ounce	IDDR	2004	AUD 150 in NSW to AUD 250-300 in Queensland per ounce	-	8.33	
Indoor	price per ounce plus price per gram	IDDR	2005	AUD 220 to AUD 400 per ounce and AUD 15 to AUD 60 per gram	-	11.07	
Outdoor	price per ounce	IDDR	2006	AUD 150 in NSW and SA to AUD 1000 in SA per ounce	-	20.54	
Outdoor	price per gram	IDDR	2007	AUD 20 to AUD 35, but price in remote location – Northern Territory is AUD 50 to AUD 100 per gram	-	9.31	
Outdoor	price per ounce plus price per gram	IDDR	2008	AUD 200 to AUD 500 per ounce, AUD 10 to AUD 50 per gram	-	12.50	
Outdoor	price per ounce plus price per gram	IDDR and UNODC	2009	AUD 180 to AUD 500 per ounce, AUD	AUD 17.0748 to AUD	12.14	3.911764706

				20 to AUD 75 per gram	29.88648 per gram		
Outdoor	price per ounce plus price per gram	IDDR and UNODC	2010	AUD 250 to AUD 700 per ounce, AUD 20 to AUD 75 per gram	AUD 19.877 to AUD 27.105 per gram; typical price is AUD 22.589	16.96	2.8
Indoor	price per ounce plus price per gram	IDDR and UNODC	2011	AUD 200 to AUD 700 per ounce, AUD 20 to AUD 100 per gram	AUD 20.622 to AUD 30.939 per gram; typical price is AUD 25.775	16.07	3.733333333
Indoor	price per ounce plus price per gram	IDDR and UNODC	2012	AUD 250 to AUD 450 per ounce, AUD 12 to AUD 50 per gram	AUD 19.792 to AUD 29.688 per gram; typical price is AUD 24.745	12.50	2.48
Indoor	price per ounce plus price per gram	IDDR and UNODC	2013	AUD 210 to AUD 450 per ounce, AUD 12 to AUD 50 per gram	Typical price is AUD 21.699	11.79	2.63030303
Indoor	price per ounce plus price per gram	IDDR and UNODC	2014	AUD 200 to AUD 450 per ounce, AUD 12 to AUD 50 per gram	AUD 13.299 to AUD 55.419 per gram; typical price is AUD 32.971	11.61	2.670769231
Indoor	price per ounce plus price per gram	IDDR and UNODC	2015	AUD 160 to AUD 450 per ounce, AUD 10 to AUD 50 per gram	-	10.89	2.754098361

Indoor	price per ounce plus price per gram	IDDR and UNODC	2016	AUD 200 to AUD 450 per ounce, AUD 10 to AUD 50 per gram	AUD 207.002 to AUD 465.759 per ounce; typical price is AUD 310.510 per ounce	11.61	2.584615385
Indoor	price per ounce plus price per gram	IDDR and UNODC	2017	AUD 200 to AUD 450 per ounce, AUD 20 to AUD 50 per gram	AUD 6.838 to AUD 48.818 per gram; typical price is AUD 19.527 per gram	11.61	3.015384615
						Average Discounting factor	**2.953363185**

Table 16. Per gram price estimates of cannabis in Australia

Once the price information is available, the amount of cannabis seized annually (ACIC, 2016, 2017, 2018, 2019) is used to come up with the amount of proceeds of crime from cannabis trafficking that would have been generated had it not been detected. It can be summarised using the formula below:

$$\textit{Proceeds of cannabis trafficking} = \textit{Price per gram of cannabis} \times \textit{Weight of cannabis seized (in grams)}$$

This chapter considers the weight of cannabis seized annually, considering that it would be difficult to ascertain the amount of annual cannabis production. The approach to derive the proceeds of crime involving a measurable commodity such as cannabis (in this case the proceeds that would have been available if not detected), based on the weight of cannabis and price per unit, is in line with the views of Unger et al. (2006). They state that proceeds of crime for a measurable commodity can be ascertained by multiplying the weight of commodity with their respective per unit price.

Once the proceeds of crime through cannabis trafficking that would have been derived had it not been detected are known, the next step is to compute the proceeds available for laundering. Not all proceeds of crime are available for laundering, and so it is essential to compute the percentage of the proceeds of crime that actually is available for laundering (Smekens & Verbruggen, 2004; Unger, 2007; Unger et al., 2006; Walker, 1999). Meloen et al. (2003), using case studies to examine the behaviour of money launderers caught, found that launderers of drug crimes laundered 80 per cent of the proceeds of their crime. These observations were in line with those of Walker (1999) and Unger (2007). As a result, based on past literature, to derive an estimate of the potential amount of funds available that would have been laundered, we estimate that 80 per cent of the proceeds of crime are available for laundering. An estimate of the potential amount of funds available that would have been laundered can be summarised using the formula below:

$$Amount\ available\ for\ laundering = Proceeds\ of\ crime\ from\ cannabis\ trafficking \times 0.80$$

Once the proceeds of crime, (and in this case it would be cannabis trafficking) available for money laundering are ascertained, the next step is to determine the proportion of funds that would be laundered in Australia. Using Walker's gravity model (Ene, 2014; Ferwerda et al., 2013; Khan et al., 2018; Walker, 1999; Walker & Unger, 2009), the proportion of funds laundered domestically can be ascertained. The equation for the Walker gravity model is as follows:

$$P(A, y_i) = \frac{\frac{attractiveness(y_i)}{dist(A,y_i)}}{\sum_{i=1}^{n} \frac{attractiveness(y_i)}{dist(A,y_i)}}$$

where P is the proportion of funds flowing from country A (Australia) to country y_i, which is again Australia in this case. The attractiveness and the distance component as specified in the literature (Ene, 2014; Ferwerda et al., 2013; Khan et al., 2018; Walker, 1999; Walker & Unger, 2009), are as follows:

$$Attractiveness = GDP^{*}\ (3^{*}BS + GA + SWIFT + FD - 3^{*}CF - CR - EG + 10)$$

where GDP is Gross Domestic Product, BS is banking secrecy, GA is government attitude, SWIFT is Society for Worldwide Interbank Financial Telecommunication (SWIFT) member, FD is financial deposits, CF is conflict, CR is corruption and EG is Egmont Group member.

$$Distance = Language + Trade + Colonial\ Background + Distance$$

As it is with Mayer and Zignago (2011), for the purpose of computing the proportion of funds laundered within a country the distance component for Australia from Australia is computed using the great circle formula.

Once the proportion of funds laundered in Australia is computed, they can be used in combination with proceeds available for laundering to determine the amount of funds that would have been laundered annually through cannabis trafficking had it not been detected[4]. The same can be summarised using the formula below:

$$Amount\ of\ cannabis\ laundering\ in\ Australia = Proceeds\ available\ for\ laundering \times Proportion\ of\ funds\ laundered\ in\ Australia$$

The annual prices of cannabis (per gram), weight seized (in kilograms), proceeds of crime available for laundering, the proportion of funds laundered in Australia, and the amount that would have been laundered had the cannabis not been detected are provided in Table 17 below.

Year	Weight Seized (in kilograms)	Price Estimates (Average prices from ounces to per gram as given in IDDR report and provided in table 16)	Proceeds of Crime Detected	Amount Available for Money Laundering	Proportion Laundered in Australia as per Walker Gravity Model	Guess Estimate of Amount Laundered
2003	9900	$ 9.05	$ 89,571,428.57	$ 71,657,142.86	20.49%	$14,681,832.00
2004	7600	$ 8.33	$ 63,333,333.33	$ 50,666,666.67	23.42%	$11,866,133.33
2005	4482.626	$ 11.07	$ 49,629,073.57	$ 39,703,258.86	23.79%	$9,445,405.28
2006	4781.9	$ 20.54	$ 98,199,732.14	$ 78,559,785.71	23.38%	$18,367,277.90

[4] The cannabis laundering proceeds have been computed up to 2017 because the World Bank's financial deposits data are currently only published up to that year.

Year	Weight Seized (in kilograms)	Price Estimates (Average prices from ounces to per gram as given in IDDR report and provided in table 16)	Proceeds of Crime Detected	Amount Available for Money Laundering	Proportion Laundered in Australia as per Walker Gravity Model	Guess Estimate of Amount Laundered
2007	5409	$ 9.31	$ 50,365,461.58	$ 40,292,369.26	26.53%	$10,689,565.57
2008	5573	$ 12.50	$ 69,662,500.00	$ 55,730,000.00	30.19%	$16,823,772.40
2009	5989	$ 12.14	$ 72,723,571.43	$ 58,178,857.14	21.25%	$12,363,007.14
2010	5452.4	$ 16.96	$ 92,496,071.43	$ 73,996,857.14	23.38%	$17,301,945.14
2011	7349.2	$ 16.07	$ 118,112,142.86	$ 94,489,714.29	26.71%	$25,238,202.69
2012	9344	$ 12.50	$ 116,800,000.00	$ 93,440,000.00	30.92%	$28,891,648.00
2013	7074	$ 11.79	$ 83,372,142.86	$ 66,697,714.29	32.98%	$21,996,906.17
2014	6004.7	$ 11.61	$ 69,697,410.71	$ 55,757,928.57	31.59%	$17,613,929.64
2015	6081.5	$ 10.89	$ 66,244,910.71	$ 52,995,928.57	24.62%	$13,047,597.61
2016	7547.8	$ 11.61	$ 87,608,392.86	$ 70,086,714.29	21.95%	$15,384,033.79
2017	8665.9	$ 11.61	$ 100,586,339.29	$ 80,469,071.43	21.29%	$17,131,865.31

Table 17. Annual estimates of money laundered through cannabis in Australia

6.1.7 Implications of cannabis regulations on prices and amount of money laundering

The highest prices per gram of cannabis are observed in 2006, 2010, and 2011. The lowest prices, after 2004, are observed in 2015 and 2016. The regulations in these years are critical in influencing cannabis prices. For instance, the price increase in 2006 could be attributed to policy changes such as increments in penalties for hydroponic cannabis in New South Wales, as provided in Table 1.

In addition, the price rise in 2010 and 2011 coincides with further prohibitory measures taken in ACT, South Australia, New South Wales, Northern Territory, and Tasmania. The low prices in 2015 and 2016 may be attributed to the steps being taken by the Federal Government to facilitate the medicinal use of cannabis in 2016 (Lintzeris et al., 2020). Such a correlation does direct attention towards empirically evaluating the extent to which regulations influence the prices.

There are data constraints around determining the amount of cannabis produced and consumed; as a result, this chapter tends to focus on the amount of cannabis seized annually. Once again, it is critical to note that cannabis seized is not a direct reflection on the amount of cannabis produced and consumed annually. Consideration is required of the presence of other factors for variation in cannabis seizures, as it would not be an accurate indicator reflecting the regulatory effects. Still, it needs to be considered in the absence of other reliable indicators. A substantial number of cannabis seizures is observed in the years 2003 and 2012, respectively. Before 2001, cannabis usage was decriminalized in three Australian states, namely, ACT, South Australia, and Northern Territory; however, since 2001, the cannabis policy changes in Australia have taken a more prohibitive and stricter turn (Ritter & Sotade, 2017). One outcome of such a prohibitory approach is the higher rate of seizures documented in the years 2003 and 2012. As seen in Table 15, in 2003 the Cannabis Control Act was introduced in Western Australia, while 2012 was marked by a ban on the sale of drug equipment in South Australia and Victoria, following a series of prohibitive measures in 2010 and 2011.

The cannabis regulations, affecting cannabis prices and seizures, did have an overall effect on the extent of revenue proceeds generated from cannabis trafficking. The years 2010 and 2011 witnessed the highest amount for proceeds of crime and funds available for money laundering, as seen in Table 17. Furthermore, an estimate for potential money laundering

resulting from cannabis within Australia between 2003 and 2017 has been provided in Figure 17, whereby 2006 and 2012 have witnessed a sharp rise followed by a sharp decline in 2015.

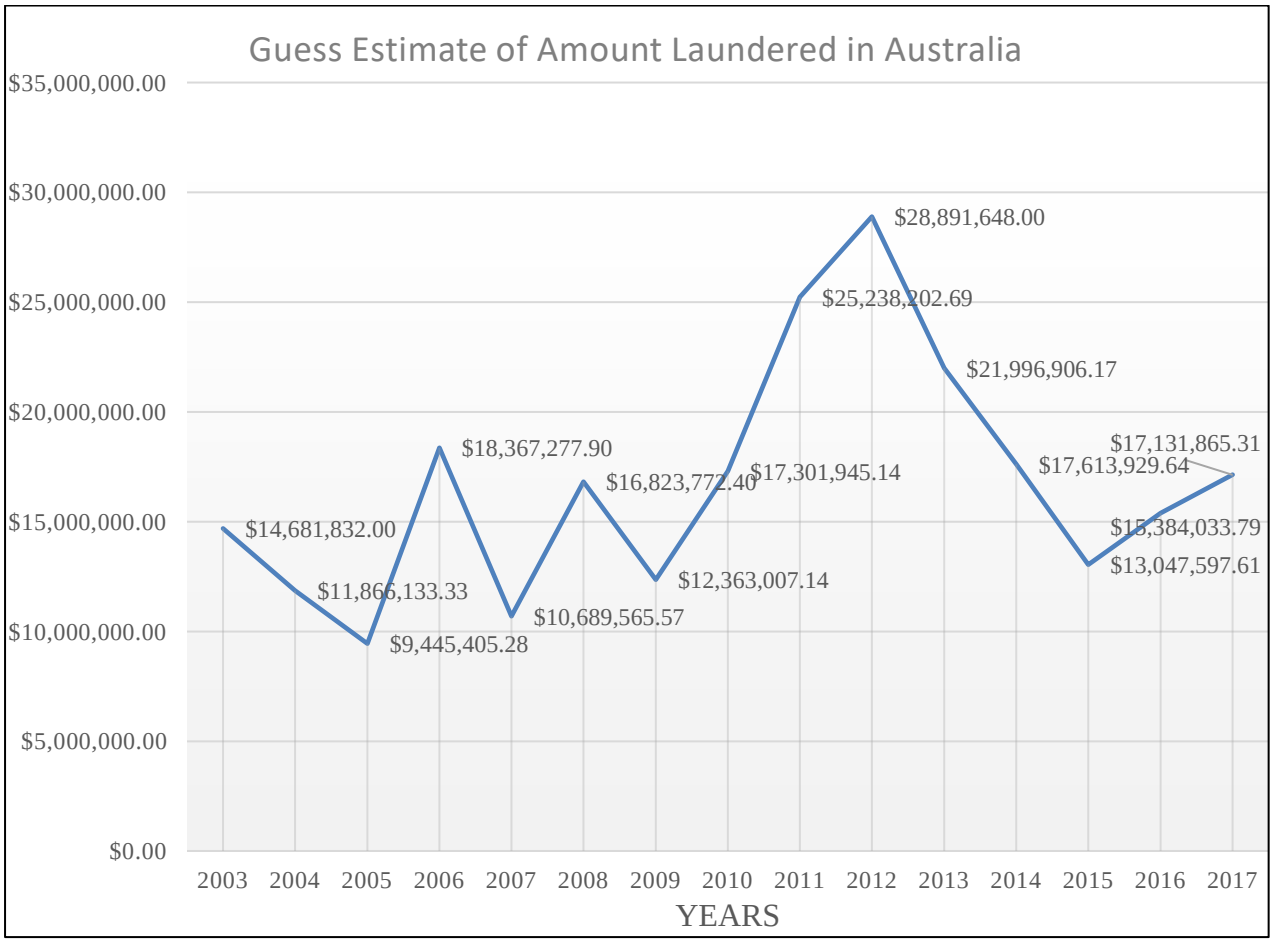

Figure 17: Annual estimates of potential money laundering as a result of cannabis in Australia

Regulatory changes, among other factors, often influence the weight and the price per unit, which in turn influences the proceeds of crime. It is important to note that the potential money-laundering amount estimated annually is dependent on the proceeds of crime, in this case, cannabis trafficking, which is influenced by the unit price and the weight of cannabis. The rational choice theory concerning the need to launder funds (Gilmour, 2016b) finds an empirical validation in the estimates documented in Table III. The need to launder funds becomes critical when a prohibitory approach towards cannabis is considered. This is evident from the highest amount estimated for the year 2012 (AUD 28.8 million), which would have been laundered had it not been seized. Consequently, the effect of regulatory changes on the

amount of funds being laundered or are made available for laundering is something that should be considered in more detail.

6.1.8 Conclusion

This chapter improves the understanding of the present state of cannabis policy reforms in Australia at the state and territory level. It highlights the discrepancy present in regulations at the state and territory level. Regulatory diversity is worth appreciating. However, when considering alternative metrics for policy effectiveness such as illicit income from drug trafficking as a proportion of national GDP (Werb et al., 2016), uniformity in cannabis regulations at the national level, such as exist in Uruguay, may be appropriate. It is essential to address such disparities in rules for effective policy implementation.

This chapter provides a theoretical grounding in the implications such a policy might have on the need to launder funds. It is in line with the views of Bewley-Taylor (2016), who argues for the use of measures of outcomes relevant to both individuals and communities when evaluating the effectiveness of a policy. This chapter uses theories in the literature to support the argument that a move from a prohibitory to harm-reduction approach about cannabis would aid in reducing the amount of funds being laundered and makes an attempt at empirical validation. It makes use of past literature and Walker's gravity model to do the same. No study in the past has used market prices or quantities of cannabis in assessment of a cannabis policy outcome except when determining potential tax revenue (Caulkins et al., 2015).

Such a conclusion could play a vital role in the debate around the legalisation of cannabis by providing an additional component for depicting harms from illegal markets. It may have implications for economies attempting to tackle the problem of money laundering by providing an avenue to consider the cannabis angle.

A prohibitory approach tends to increase drug prices, creates incentives for violence among drug dealers and generates illicit markets for consumption (Kleiman & Heussler, 2011). The argument provided in favour of the proliferation of cannabis accessibility laws is that it results in lowering of the drug's real and shadow price. However, in the context of Australia, the empirical evaluation of this argument becomes challenging because a broad range of per-unit prices of cannabis does not provide a clear picture of how prices have altered on account of changing regulations. For instance, according to the ACIC (2019), the price of one gram of

hydroponic cannabis head was between AUD 20 and AUD 50 in 2017-18, compared with AUD 10 to AUD 50 in 2016-17.

The chapter suffers from certain limitations in coming up with a lower estimate of the proceeds of crime that would have been available for laundering resulting from cannabis had it not been detected. First, the price information used is based on data provided by covert police units and informants lacking reporting standardisation. This led to the use of a quantity discount factor to acquire uniform prices. Secondly, for ease in calculation, aspects such as the purity levels in cannabis, different cannabis variants, and the purpose of usage (recreational or medicinal) are not taken into consideration. Finally, through lack of information about annual cannabis production, the chapter considers the weight of cannabis seized annually to ascertain the proceeds of cannabis trafficking.

Nevertheless, this chapter, drawing from the benefits of mixed methods research (MMR) (Lamprecht & Guetterman, 2019), attempts to evaluate the implication of regulatory changes on the amount of money laundered using Walker's gravity model. It is observed that the years with a stricter approach towards cannabis, stemming from regulations and annual seizures, namely 2006, 2008 and 2012, experience an increase in potential amounts of money laundering. Furthermore, the years leading to a more tolerant approach to cannabis consumption, that is, 2015 and 2016, witness a decline in potential money-laundering amounts. It is important to note that small price variations may be ignored because of lack of accuracy associated with price estimates; however, variations of significant magnitude do contribute to the understanding on the effect of regulations on money laundering.

As a result, the price obtained from consumers through survey responses is of paramount importance for researching the fluctuation of consumption from changes in prices. It becomes possible to obtain information about such transactions from those producing, selling and purchasing cannabis in the legal market (Kilmer & Pacula, 2017). The effect of cannabis regulations on the price of cannabis through changes in production costs and taxes will have crucial implications for consumption, government budgets and the size of illicit markets (Caulkins et al., 2015; Kilmer et al., 2010). According to Kilmer and Pacula (2017), there is a need for better data to use in the analysis of cannabis policy changes – for example, better measures about consumption such as total grams consumed or typical potency per dose – thereby validating self-report survey data and market transaction data.

This chapter outlines important future research directions. First, there is a need for a more advanced empirical assessment of the influence of cannabis regulation on the amount of funds being laundered. Quantifying this relationship would help inform policy makers. The changes occurring annually in response to changes in cannabis regulations could be measured by controlling for other factors using existing models (Ardizzi et al., 2014; Argentiero et al., 2008; Ferwerda et al., 2013; Hendriyetty & Grewal, 2017; Reuter & Greenfield, 2001; Schneider & Enste, 2000a, 2000b; Schneider & Linsbauer, 2016).

Secondly, it could be beneficial for public policy to use the knowledge derived from communication theories to understand factors responsible for changes in public attitudes towards cannabis. Apart from regulatory movements, the change in cannabis usage may be attributed to factors such as the purpose for which it was used, a decreased stigmatisation towards its use, availability of alternatives and the way it has been portrayed in the media (AIHW, 2014; Bresin & Mekawi, 2019; Hughes et al., 2011). As a result, a detailed analysis of factors responsible for the change in cannabis use could also be examined by future research.

Thirdly, it would be valuable for researchers to empirically evaluate the effect of differential regulations in a country on policy effectiveness. The diversity in drug policies should be viewed as a strength with scope for flexibility. In the presence of international conventions, policy innovations and diversity have thrived as seen in European countries (Chatwin, 2017). Cross-national policy diversity is encouraged; however, policy consistency at the national and sub-national levels is essential for policy effectiveness in light of a metric such as the amount of funds laundered. Uniformity in policy formulation and implementation may allow macroeconomic monitoring of the shadow economy and appropriately attribute changes to cannabis policies. Overall, the implications of any future policy changes must be monitored and analysed to inform policy makers.

After attempting to measure the magnitude of money laundering through cannabis trafficking, the thesis directs attention towards placing the complex phenomenon of money laundering appeal into a single composite indicator, one that might not only inform national strategies to prevent money laundering but provide an opportunity to use a similar approach to develop more localized hotspot maps that could move analysis at the sub-national level. This is discussed in the following chapter.

Chapter 7 Money-Laundering Appeal Index

***** This chapter is based on a conference paper presented at a conference, namely: Tiwari, M. 2020. Money Laundering: Ranking the countries attractive for money laundering to India. In *Online International Conference on 'Emerging Opportunities and Challenges in the Indian Economy: An Interdisciplinary Approach.'*

***** A version of this paper is published in a peer-reviewed journal, namely: Tiwari, M., A. Gepp, and K. Kumar. 2021. Global money laundering appeal index: application of principal component analysis. *Journal of Money Laundering Control*. https://doi.org/10.1108/JMLC-10-2021-0108

The literature review (see Section 2.2.4) and the previous chapter (Chapter 6) highlight the work on estimating the magnitude of money laundering. This results in the need to know the countries that would be attractive to launder funds. This chapter attempts to answer that by proposing a money-laundering appeal index (MLAI), determining a country's appeal as a destination for money laundering. It does so by using Principal Component Analysis (PCA) and finds four components relating to economic feasibility, financial liberty, government spending, and a tax regime to be critical in influencing a country's money-laundering appeal. This is the first attempt to use a statistical technique to understand the underlying components of a country's money-laundering appeal and could be used to develop more effective preventative strategies.

7.1 Introduction

Money laundering presents social, economic, and political harm to a country and the global economy by providing an opportunity to launder and reinvest criminal proceeds. Such opportunities lead to economic distortions, erosion of financial sectors, reduced government revenues, and other socioeconomic effects (Barone et al., 2018; Bhattacharjee, 2020; Degryse et al., 2019; Walker & Unger, 2009). The extent of economic and financial disruptions can be assessed based on Barone and Masciandaro (2011) estimates. They found money-laundering operations to produce legal assets worth USD 108.72 billion in Eastern Europe in 2009. As a result, efforts have been made to measure money-laundering flows, construct money-laundering risk indicators and uncover other such instances (Basel Institute on Governance, 2014; Collin, 2019; Ferwerda & Kleemans, 2019). Walker (1999) can be regarded as a pioneer in the domain. He postulated a range of factors contributing to the attractiveness of a destination for money laundering. The factors contributing to attractiveness have often been used to estimate the magnitude of money laundering, and there is often a debate around the accuracy of the generated estimates (Collin, 2019).

Efforts have been made to improve the proposed Walker Gravity model, and one such attempt in this regard was by Unger et al. (2006). The attractiveness component has been enhanced only through the addition or removal of variables. No attempts in the literature have been made to use quantitative techniques to develop an index of money-laundering appeal. This chapter contributes to the literature by presenting a standardised and replicable methodology, to condense into a single measure the complex and multifaceted phenomenon of a country's appeal as a destination for money laundering, thus avoiding the difficulty of precisely calculating illicit financial flows.

This chapter uses principal component analysis (PCA hereafter), with a mix of standardised and unstandardised components relating to attractiveness, economic freedom, and money-laundering risk (Basel Institute on Governance, 2014; Khan et al., 2018; Kim & Holmes, 2016) to come up with MLAI. Such an index would act as an additional tool to support policymakers and investigators in allocating relevant resources effectively and developing suitable preventative strategies; for banks and professionals, the indicator would improve due-diligence operations. Such efforts would combat the phenomenon of money laundering

responsible for the stagnation of economic growth through tax evasion, corruption, and the creation of non-competitive markets.

7.2 Data and methodology

The data on 30 variables incorporated for analysis in the chapter have been collected for 150 countries. The year 2014 is chosen for analysis to facilitate comparison with the results of an earlier study that used the traditional gravity model to develop the attractiveness of money laundering for countries. In the case of missing variables, the variable information available for the most recent year, past or present, is considered for analysis. Finally, in order to avoid excluding countries from analysis when variable information is unavailable for them, the variable value is recorded as 0 for that country. (The entire dataset is available upon request).

Table 18 below provides the list of variables used for analysis:

Variables	**Source**	**Description**
Per Capital Gross Domestic Product (GDP), Government Expenditure, Tariff Rate, Income Tax Rate, Corporate Tax Rate, Tax Burden (% GDP), Public Debt (% GDP), FDI Inflows (in millions), Unemployment, Inflation (%), Financial Deposits	The World Bank (2020)	Assessment of country's macroeconomy
Basel AML Score	Basel Institute on Governance (2014)	Assessment of countries' risk associated with money laundering or terrorist financing, to develop Basel Anti-money Laundering (AML) Risk Index
Economic Freedom Score, Business Freedom, Financial Freedom, Fiscal Freedom, Government Spending, Labor Freedom, Monetary Freedom, Trade Freedom	Kim and Holmes (2016)	Assessment of economic freedom available to a country's population to produce the Index of Economic Freedom
Attractiveness Score, Banking Secrecy (BS), Conflict (C), Corruption (COR), Member of Egmont Group (EG), Government Attitude (AG), Swift Member	Khan et al. (2018); Walker and Unger (2009)	Estimate of the magnitude of money laundering for countries depending upon how attractive they are to launderers

Table 18. List of variables

The use of variables for accessing countries' attractiveness has been limited to estimating the magnitude of money laundering. The current work presents an opportunity to develop an index of a country's appeal as a destination for it. The rationale to incorporate additional variables stems from works directing attention towards the link between money laundering and economic cycles, economic growth, and taxes (Barone et al., 2018; Johannesen et al., 2016). Such an index would differ from the Basel AML Risk Index and other similar indices that do not measure the country's actual money-laundering activity. These indices' focus has been to assess the risk level based on adherence to AML/CTF (Countering Terrorism Financing) standards and other such risk categories. The rankings of such global indices are more suitable in a probabilistic rather than economic sense.

This chapter uses PCA to reduce a large number of variables into fewer components (Ferwerda & Kleemans, 2019; Iwasokun et al., 2019; OECD & JRC, 2008; Riccardi et al., 2018) representing a specific phenomenon: in this case, money-laundering appeal. This construction is a linear combination of the observable variables and it takes the form of an index.

The number of components is selected based on accepted standards – the Kaiser-Harris criterion and parallel analysis. The unrotated components are subject to rotation to ensure the pattern of loadings is easier to interpret. The components are then extracted to be normalised and combined in a composite indicator using the proportion of variance explained by each component as weights (Ferwerda & Kleemans, 2019; Watkins, 2006).

7.3 Results

The suitability of the data for PCA is assessed by using a Kaiser-Meyer-Olkin Measure of Sampling Adequacy (KMO), and Bartlett's Test of Sphericity (Kaiser, 1960). A KMO value of 0.768, and a significant sphericity test as presented in Table 19, suggest the data are suitable for PCA.

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0.768
Bartlett's Test of Sphericity	Approx. Chi-Square	4931.351
	df	435

	Sig.	0.000

Table 19. KMO and Bartlett's Test of Sphericity

The decision of the number of components to be extracted is based on a mix of Kaiser-criterion (components with eigenvalues > 1) and parallel analysis (Watkins, 2006). The comparison of eigenvalues obtained from Kaiser-criterion and parallel analysis (Table 20) is presented below and it suggests that four components should be extracted:

	Initial Eigenvalues			**Random Data Eigenvalues (Parallel Analysis)**	
Component	**Total**	**% of variance**		**Total**	**Decision**
1	10.922	36.406		2.067	Accept
2	3.063	10.210		1.916	Accept
3	1.996	6.654		1.779	Accept
4	1.878	6.260		1.679	Accept
5	1.390	4.633		1.595	Reject

Table 20. Comparison of eigenvalues from Kaiser-criterion and Parallel Analysis

The extracted components were subject to varimax rotation to ensure suitable factorisation. The output is presented in Table 21 and Table 22 below:

	Component			
	1	**2**	**3**	**4**
Attractiveness	0.817			
FD	0.791			
Freedom from Corruption	0.789			
Property Rights	0.780			
COR	-0.755			
Economic Freedom Score	0.723	0.608		
Business Freedom	0.678			
GDP	0.670			
FDI Inflows in millions	0.561			
Labor Freedom				
Public Debt as percent of GDP				
C				
AG				
Unemployment				
Monetary Freedom		0.808		
Inflation in percentage		-0.725		
Investment Freedom		0.699		
Financial Freedom	0.553	0.657		
Trade Freedom		0.606		
Tariff Rate		-0.504		
BS				
Basel AML Score				
EG				
Government Expenditure			0.916	
Government Spending			-0.913	
Tax Burden as percent of GDP			0.665	
Swift				
Income Tax Rate				0.903
Fiscal Freedom				-0.888
Corporate Tax Rate				0.774

Table 21. Rotated component matrix

Component	Variance		
		% of variance	Cumulative %
1		22.949	22.949
2		14.859	37.809
3		12.228	50.037
4		9.494	59.530

Table 22. Variance explained by components

The first component (1) comprised the set of variables related to a country's economic feasibility and explained 22.9 % of the overall variance. The second component (2) explained 14.85% of the overall variance and included proxies for financial liberty. The expenditure incurred and income source to support it by a country's government are grouped in the third component (3) and explain 12.22% of the overall variance. Finally, the fourth component (4) relates to a country's tax regime and explains 9.49% of the overall variance. Consequently, a country's appeal for money laundering can be explained as follows:

$$Money\ Laundering\ Appeal = f(E, F, G, T)$$

Where,

E = Economic feasibility of a country to invest in

F = Financial liberty available to people to transact and do business

G = Government spending

T = Tax regime

Each principal component's variance is used as a fraction of the model's overall variance as a weight to obtain the index. The index is normalised using the Min-Max criterion and is expressed as follows:

$$Global\ Money\ Laundering\ Appeal\ Index$$

$$= \sum_{j=1}^{4} (S_{ij} * w_j) = (S_{1i} * w_1) + (S_{2i} * w_2) + (S_{3i} * w_3) + (S_{4i} * w_4)$$

Where the subscript i indicates the country (150 in total), j is the component and w_j is the proportion of variance explained by each component, that is, $w_1 = 22.9\%, w_2 = 14.85\%$, $w_3 = 12.22\%$, and $w_4 = 9.49\%$, respectively. S_{ij} is the relevant value from the PCA for each component. According to the index, for 2014 the most appealing countries for money laundering were Denmark, Sweden and the United States, and the least appealing countries were Sudan, Iran and Iraq (ranking results are available for 150 countries in the Appendix including the underlying data). It should be noted that rankings will vary if fewer or additional countries are included in the sample.

7.4 Conclusion

This chapter proposes a quantitative methodology for ranking countries' money-laundering appeal, tests it on data from 150 countries and attempts to advance the research on illicit financial flows. The use of PCA instead of a more theoretical approach is assessed against money-laundering related information about the top destinations in the public domain. Denmark's being found an appealing destination for money laundering in 2014 aligns with a Danish bank's involvement in one of the largest scandals around the same time (Bjerregaard & Kirchmaier, 2019). Similarly, the attractiveness of the US as another destination is documented through the HSBC money-laundering scandal (Huang, 2015). Finally, concerns about whether a low Basel AML Risk score (Manning et al., 2020) results in lower chances of money laundering are also addressed through this chapter. It is found that a low Basel AML Risk score does not necessarily eliminate the chances of a country being chosen as an appealing destination for money laundering.

It is critical to score and rank countries based on their appeal for money laundering. Illicit financial flows from developing countries have a considerable effect, particularly for those that struggle to maintain essential social services and functioning institutions. For such economies, revenue losses will be more damaging and may further give rise to underlying activities that generate them, such as corrupt practices and drug trafficking (Collin, 2019). In the light of current circumstances where a considerable amount of funds is being drained out

of developing economies, the ranking mechanism proposed in this chapter can assist in identifying preferable destinations for money launderers to launder funds. It may allow regulatory authorities to be proactive. Careful monitoring of transactions and the movement of funds from developing countries to economies found appealing for money laundering may help stop the launderers from damaging these more vulnerable countries.

Consequently, such an index might not only inform national strategies to prevent money laundering but may provide an opportunity to use a similar approach to create more localised hot-spot maps that could move analysis to the sub-national level, subject to availability of accurate regional data. It would offer a more robust tool for identifying the appeal of geographies as a destination for money laundering.

Robust results can leave the way open for future work, and this may include incorporating more variables. The chapter provides several aspects that can be considered in future research. Another element that could be focused upon is to address the regulatory framework that makes countries, identified through this approach, into an attractive destination for money laundering. To determine its accuracy, the ranking results of 2014 through this method can be compared with the publicly available information on money laundering for the top ten countries. The chapter, consistent with views of Riccardi et al. (2018), can benefit studies beyond the AML field, for instance, in ranking countries according to their efforts against the financing of terrorism, corruption and tax evasion.

Chapter 8 Overall Conclusion and Future Work

Money laundering presents social, economic and political harms to a country and the global economy by providing an opportunity to launder and reinvest criminal proceeds. Such opportunities lead to economic distortions, erosion of financial sectors, reduced government revenues and other socioeconomic effects (Barone et al., 2018; Degryse et al., 2019; Loayza et al., 2019; Manning et al., 2020; Unger, 2007; Walker & Unger, 2009). This thesis makes an effort to improve the understanding around money laundering and means to detect it. The key stakeholders to benefit from such research work would be legal and compliant professionals and government officials, especially tax officials and anti-corruption NGOs.

The major conclusions and contributions of this research are presented next, followed by suggestions for future work.

8.1 Conclusions and contributions of this research

In line with the aims of the project, this research has advanced the field of financial crimes, money laundering and means of detecting it through:

- Developing a framework to detect possible money-laundering techniques that may be used by a launderer
- Developing a graph database schema to identify hidden patterns and relationships among entities
- Using hybrid techniques to come up with detection models to uncover shell companies
- Documenting the emergence of a new opportunity to commit fraud and pave the way to launder funds
- Empirically assessing the effect of regulations on money laundering in Australia
- Identifying the critical factors contributing to a country's appeal as a destination for laundered funds.

The new framework model was presented which could be used to educate forensic professionals in coming up with proactive approaches to identify possible techniques being used to launder funds. Moreover, the empirical assessment of regulatory changes on money laundering may guide policymakers in the future to keep in mind the possible effect the changes they propose may have on the magnitude of money being laundered within the country. All this may be helpful in tackling the global problem of money laundering. The contribution of this research is strengthened because:

- There is a lack of understanding about the reasons underlying a launderer's choice of techniques, which this research proposes to address
- It is the first study to develop models to detect illicit shell companies using publicly available information quantitatively; and
- It is the first study to empirically assess the effect of regulations on the amount of funds being laundered.

The following subsections discuss the main findings according to the six main research questions driving this research.

8.1.1 Research Question 3 (RQ1)

RQ 1: *What factors may influence a launderer's choice of technique to launder funds?*

While the forensic accounting education curriculum directs some attention towards money laundering, there is a lack of understanding about the reasons underlying a launderer's choice of techniques. Drawing on existing literature and theories, a new framework is developed in this research to provide insights into the techniques a launderer may adopt to wash funds among a range of available options. It is found that the actors involved, predicate crime, the purpose for laundering, and technological innovations each play a role in explaining the choice of techniques. The APPT framework comprising the factors as described earlier could increase the forensic accounting educational content value and be of benefit to educational institutions offering such courses and to personnel undertaking them.

8.1.2 Research Question 2 (RQ2)

RQ 2: *Does the presence of data related to entities on a graph database platform aid in revealing hidden patterns and relationships?*

This chapter focuses on explaining the set-up of the data structure to investigate a network of illicit companies identified in cases of money laundering schemes through a graph database platform. Data on a list of such companies, as provided by TIUK, are collected through OpenCorporates, cleansed through OpenRefine, and transported to a graph database platform – Neo4J. On querying the graph database of corporate entities through a combination of search queries and pathfinding algorithms, it was found that 51 companies in the dataset had an ultimate beneficial owner, 16 companies were located at the same postal address, and the same individuals named were directors in 139 and 610 entities, respectively. The move to adopt a graph database structure for storing information related to corporate entities will helps in the identification of hidden links among entities to deter activities of corruption and money laundering.

8.1.3 Research Question 3 (RQ3)

RQ 3: *Are combinations of graph analysis algorithms and supervised-learning modelling techniques successful in detecting illicit shell companies?*

Shell companies are used to launder dirty money to make it appear legitimate and hide information about the actual beneficial owners. Illegal arms dealers, drug cartels, corrupt politicians, terrorists and cyber-criminals have become some of the frequent users of these shell companies. This research developed models for detection of shell companies being used to launder illicit proceeds of crime using hybrid techniques. The results showed that on using three classification algorithms, namely Decision Trees, TreeNet, and Random Forests, for the combination of various graph algorithms, the classification accuracy achieved was within the range of 88.17 % and 97.85 %, respectively. The key stakeholders to benefit from such models would be legal and compliant professionals and government officials, especially tax officials and anti-corruption NGOs.

8.1.4 Research Question 4 (RQ4)

RQ 4: *How have the changes in technology enhanced the opportunity to commit fraudulent acts?*

Over one billion US dollars were invested in blockchain in 2016. The potential application of blockchain extends far beyond cryptocurrencies. One use of blockchain is an Initial Coin Offering (ICO), a digital method of raising finance involving issuance of tokens in exchange for cryptocurrencies or fiat money. It is a cheaper, easier and quicker way to raise funds compared with traditional public offerings. However, it has raised a new opportunity for fraud. An estimated ten percent of ICO funds were lost to fraud. Using case-study analysis, this research determined characteristics of such fraud schemes and the regulatory changes made in response to them. The study revealed key lessons for investors in terms of proactive steps that could be taken to protect themselves from being victims, for issuers to ensure awareness and take steps to secure investors' trust, and for regulators to promote a safe environment. It was the first attempt to document the effect of ICO fraud schemes on the regulatory environment, which is going through a series of amendments to provide protection against such fraudulent schemes.

8.1.5 Research Question 5 (RQ5)

RQ 5: *How do the changes in cannabis regulations affect money laundering in Australia?*

Cannabis is the most often used drug in Australia. In the past decade, the country has witnessed a shift in cannabis policy regulations from prohibition towards decriminalisation and eventual legalisation at the state and territory level. As a result, understanding the changes in cannabis policy regulations and possible implication of such changes on the quantum of money laundering in Australia can be value-additional. A review of published secondary data sources is conducted to document the changes in cannabis policy regulations. Through the use of theoretical concepts of rational choice, individual decision-making and utility, this chapter provides a high-level view of the possible policy implications on money laundering. It then attempts to provide empirical validation. This research lays down the implication of such policy changes in the amount of money being laundered. It finds some support for the argument that prohibitive measures towards cannabis use do contribute to an increase in the need to launder the proceeds generated.

8.1.6 Research Question 6 (RQ6)

RQ 2: *What factors may make a country appealing as a destination to launder funds?*

This research uses principal component analysis (PCA), with a mix of standardised and unstandardised components relating to attractiveness, economic freedom and money-laundering risk to come up with an index of money-laundering appeal. Four components relating to economic feasibility, financial liberty, government spending and tax regime are critical in influencing a country's money-laundering appeal. It was an attempt to use a standardised and replicable methodology to condense into a single measure the complex and multifaceted phenomenon of a country's appeal as a destination for money laundering, thus avoiding the difficulty associated with precisely calculating illicit financial flows. The ranking system could be used to determine the destinations attractive for laundering money. Such information can be used to come up with more effective preventative strategies to combat phenomena responsible for the stagnation of economic growth through tax evasion, corruption and creation of non-competitive markets.

8.2 Future work

The ultimate goal is to have an increased understanding of money laundering, its related aspects and models that are able to detect such illicit activities with good accuracy. There is always scope for future research in directions that could improve model development and an overall understanding of money laundering. Specific suggestions have been made in different sections of the dissertation for future works.

Chapter 3 provides scope for future research. It offers an opportunity for the development of a more detail-oriented framework to be incorporated in practice. The future work could consider whether the value-addition provided by such a framework is greater on the education curriculum offered by tertiary institutions or certification organizations. On similar lines, more frameworks could be incorporated concerning other financial crimes. A detailed understanding of the motivation behind the participation of non-criminal actors in the act of money laundering could also be value-additional in coming up with a better framework. All of these aspects could be considered in future research.

Chapter 4 presents opportunities to come up with alternative network topologies to identify hidden patterns and relationships and to come up with better detection models.

Chapter 5 lays a foundation for future research to analyse further ICO cases and develop a detailed best-practice guide in relation to ICOs for all stakeholders.

Chapter 6 outlines important future research directions. First, there is a need for a more advanced empirical assessment of the influence of cannabis regulation on the amount of funds being laundered. Quantifying this relationship would help inform policy makers. Secondly, it could be beneficial for public policy to use the knowledge derived from communication theories to understand factors responsible for changes in public attitudes towards cannabis. Thirdly, it would be valuable for researchers to empirically evaluate the effect of differential regulations in a country on policy effectiveness. Overall, the implications of any future policy changes must be monitored and analysed to inform policy makers.

The robust results as presented in Chapter 7 can be considered suitable for future work, along with the incorporation of more variables. The research in this section provides several aspects that can be considered as part of future research. An element that could be focused upon is to address the regulatory framework that makes the countries identified through this approach into an attractive destination for money laundering. Through this method the ranking

results of 2014 can be compared with the publicly available information on money laundering for the top ten countries to determine its accuracy. The chapter, consistent with views of Riccardi et al. (2018), can benefit studies beyond the AML field, for instance, in ranking countries according to their efforts against the financing of terrorism, corruption and tax evasion.

Bibliography

ACC. (2015). *Organised crime in Australia 2015*. Retrieved from https://apo.org.au/sites/default/files/resource-files/2015-05/apo-nid54772.pdf

ACCA. (2018). ICOs: Real deal or token gestures? Retrieved from http://www.accaglobal.com/content/dam/ACCA_Global/professional-insights/Initial-coin-offerings/pi-initial-coin-offerings.pdf

ACIC. (2016). *Illicit Drug Data Report 2014–15*. Retrieved from https://www.acic.gov.au/sites/default/files/2016/08/acic-iddr-2014-15.pdf?v=1561619004

ACIC. (2017). *Illicit Drug Data Report 2015–16*. Retrieved from https://www.acic.gov.au/sites/default/files/2017/06/illicit_drug_data_report_2015-16_full_report.pdf?v=1561618955

ACIC. (2018). *Illicit Drug Data Report 2016–17*. Retrieved from https://www.acic.gov.au/sites/default/files/iddr_2016-17_050718.pdf?v=1561090189

ACIC. (2019). *Illicit Drug Data Report 2017–18*. Retrieved from https://www.acic.gov.au/sites/default/files/illicit_drug_data_report_2017-18.pdf?v=1564727746

ACT. (2019). *Drugs of Dependence (Personal Cannabis Use) Amendment Act 2019*. Retrieved from Australia: https://www.legislation.act.gov.au/a/2019-34/

ACT. (2020). Cannabis. Retrieved from https://www.act.gov.au/cannabis/home

Adamic, L. A., & Adar, E. (2003). Friends and neighbors on the Web. *Social Networks, 25*(3), 211-230. doi:https://doi.org/10.1016/S0378-8733(03)00009-1

Aggarwal, C. C. (2015). Outlier analysis. In *Data mining* (pp. 237-263): Springer, Cham.

AIHW. (2014). *National drug strategy household survey detailed report 2013*. Retrieved from Canberra: https://www.aihw.gov.au/reports/illicit-use-of-drugs/2013-ndshs-detailed/summary

AIHW. (2017). *National drug strategy household survey detailed report 2016*. Retrieved from Canberra: https://www.aihw.gov.au/about-our-data/our-data-collections/national-drug-strategy-household-survey/2016-national-drug-strategy-household-survey

AIHW. (2020). *Alcohol, tobacco & other drugs in Australia*. Retrieved from Canberra: https://www.aihw.gov.au/reports/alcohol/alcohol-tobacco-other-drugs-australia

Ainsworth, P. (2013). *Offender profiling and crime analysis*. Hoboken: Taylor and Francis.

Aitken, R. (2018). U.S. SEC Halts Alleged Crypto ICO Scam From 'Decentralized' Bank Seeking $1 Billion. Retrieved from https://www.forbes.com/sites/rogeraitken/2018/01/30/u-s-sec-halts-alleged-crypto-ico-scam-from-decentralized-bank-seeking-1-billion

Akhigbe, A., McNulty, J. E., & Stevenson, B. A. (2017). Additional evidence on transparency and bank financial performance. *Review of Financial Economics, 32*(1), 1-6. doi:10.1016/j.rfe.2016.09.001

Al Hasan, M., Chaoji, V., Salem, S., & Zaki, M. (2006). *Link prediction using supervised learning*. Paper presented at the SDM06: Workshop on link analysis, counter-terrorism and security.

Alberto, G. S. (2016). Spain: financial ownership file and money laundering prevention. *Journal of Money Laundering Control, 19*(3), 238-248. doi:10.1108/JMLC-10-2014-0030

Albrecht, W. S., Romney, M. B., & Howe, K. R. (1984). *Deterring fraud : the internal auditor's perspective*. Altamonte Springs, Florida: Institute of Internal Auditors Research Foundation.

Aldhous, P. (2012). 'Specialist knowledge is not only useless, it's unhelpful'. *New Scientist, 216*(2893), 28-29. doi:https://doi.org/10.1016/S0262-4079(12)63065-6

Aleta, A., & Moreno, Y. (2019). Multilayer networks in a nutshell. *Annual Review of Condensed Matter Physics, 10*, 45-62.

Ali, R., Barrdear, J., Clews, R., & Southgate, J. (2014). The economics of digital currencies. *Bank of England Quarterly Bulletin*, Q3.

Allred, B. B., Findley, M. G., Nielson, D., & Sharman, J. C. (2017). Anonymous Shell Companies: A Global Audit Study and Field Experiment in 176 Countries. *Journal of International Business Studies, 48*(5), 596-619.

Alstadsæter, A., Johannesen, N., & Zucman, G. (2018). Who owns the wealth in tax havens? Macro evidence and implications for global inequality. *Journal of Public Economics, 162*, 89-100. doi:10.1016/j.jpubeco.2018.01.008

AMF. (2017). L'AMF lance une consultation sur les Initial Coin Offerings et initie son programme UNICORN. Retrieved from http://www.amf-france.org/Actualites/Communiques-de-presse/AMF/annee-2017?docId=workspace%3A%2F%2FSpacesStore%2F5097c770-e3f7-40bb-81ce-db2c95e7bdae

Anand, A. I. (2011). Combating Terrorist Financing: Is Canada's Legal Regime Effective? *University of Toronto Law Journal, 61*(1), 59-71. doi:10.1353/tlj.2011.0004

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., . . . Savage, S. (2013). Measuring the cost of cybercrime. In *The economics of information security and privacy* (pp. 265-300): Springer.

Andon, P., Free, C., Jidin, R., Monroe, G., & Turner, M. (2018). The Impact of Financial Incentives and Perceptions of Seriousness on Whistleblowing Intention. *Journal of Business Ethics, 151*(1), 165-178. doi:10.1007/s10551-016-3215-6

Ardizzi, G., Petraglia, C., Piacenza, M., Schneider, F., & Turati, G. (2014). Money Laundering as a Crime in the Financial Sector: A New Approach to Quantitative Assessment, with an Application to Italy. *Journal of Money, Credit and Banking, 46*(8), 1555-1590. doi:10.1111/jmcb.12159

Argentiero, A., Bagella, M., & Busato, F. (2008). Money laundering in a two-sector model: using theory for measurement. *European Journal of Law and Economics, 26*(3), 341-359. doi:10.1007/s10657-008-9074-6

Arnold, L., Brennecke, M., Camus, P., Fridgen, G., Guggenberger, T., Radszuwill, S., . . . Urbach, N. (2019). Blockchain and Initial Coin Offerings: Blockchain's Implications for Crowdfunding. In *Business Transformation through Blockchain* (pp. 233-272): Springer.

Ashby, W. R. (1961). *An introduction to cybernetics*: Chapman & Hall Ltd.

ASIC. (2017). Initial coin offerings. Retrieved from http://asic.gov.au/regulatory-resources/digital-transformation/initial-coin-offerings/

ATODA. (2020). *Briefing Paper: The ACT's new personal cannabis use, possession and cultivation legislation*. Retrieved from http://www.atoda.org.au/wp-content/uploads/2020/01/Personal-cannabis-use-legislative-changes.pdf

Aurasu, A., & Aspalella, A. R. (2018). Forfeiture of criminal proceeds under anti-money laundering laws: A comparative analysis between Malaysia and United Kingdom (UK).

Journal of Money Laundering Control, 21(1), 104-111. doi:10.1108/JMLC-04-2017-0016; 23

10.1108/JMLC-04-2017-0016

AUSTRAC. (2014). *Terrorism financing in Australia*. Retrieved from Australia: https://www.austrac.gov.au/sites/default/files/2019-07/terrorism-financing-in-australia-2014.pdf

AUSTRAC. (2018). Draft AML/CTF Rules. Retrieved from http://www.austrac.gov.au/draft-aml-ctf-rules

AUSTRAC. (2019). Global crime syndicate used underground banking to launder drug profits. Retrieved from https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/global-crime-syndicate-used-underground-banking-launder-drug-profits

Australian, T. (2018). Swiss town Zug aims to become crypto-safe haven.

AWS. (2018). AWS Blockchain Partners: Accelerating your distributed ledger journey. Retrieved from https://aws.amazon.com/partners/blockchain/

Aydogdu, M., Shekhar, C., & Torbey, V. (2007). Shell companies as IPO alternatives: an analysis of trading activity around reverse mergers. *Applied Financial Economics, 17*(16), 1335.

Azran, A. (2007). The rendezvous algorithm: Multiclass semi-supervised learning with Markov random walks. In (Vol. 227, pp. 49-56).

Baader, G., & Krcmar, H. (2018). Reducing false positives in fraud detection: Combining the red flag approach with process mining. *International Journal of Accounting Information Systems, 31*, 1-16. doi://doi.org/10.1016/j.accinf.2018.03.004

Backhouse, J., Demetis, D., Dye, R., Canhoto, A., & Nardo, M. (2005). *Spotlight: new approaches to fighting money-laundering*. Retrieved from London: http://www.spotlight.uk.com/

Backstrom, L., & Leskovec, J. (2011). *Supervised Random Walks: Predicting and Recommending Links in Social Networks.* Paper presented at the Proceedings of the fourth ACM international conference on Web search and data mining Hong Kong, China.

Bahnsen, A. C., Aouada, D., Stojanovic, A., & Ottersten, B. (2016). Feature engineering strategies for credit card fraud detection. *Expert Systems with Applications, 51*, 134-142. doi:https://doi.org/10.1016/j.eswa.2015.12.030

Bailey, M. (2018). Melbourne start-up Konkrete to 'tokenise' property with ASIC-compliant coin offering. Retrieved from https://www.afr.com/technology/crypto-property-20180924-h15st5

Bajada, C. (2017). Money laundering activities in Australia—an examination of the push and pull factors driving money flows. In M. dela Rama & C. Rowley (Eds.), *The Changing Face of Corruption in the Asia Pacific* (pp. 127-147): Elsevier.

Baker, J., & Goh, D. (2004). *The cannabis cautioning scheme three years on: an implementation and outcome evaluation*: New South Wales Bureau of Crime Statistics and Research Sydney, Australia.

Baker, W. E., & Faulkner, R. R. (1993). The Social Organization of Conspiracy: Illegal Networks in the Heavy Electrical Equipment Industry. *American Sociological Review, 58*(6), 837-860. doi:10.2307/2095954

Balakina, O., D'Andrea, A., & Masciandaro, D. (2017). Bank secrecy in offshore centres and capital flows: Does blacklisting matter? *Review of Financial Economics, 32*, 30-57. doi:https://doi.org/10.1016/j.rfe.2016.09.005

Baldwin, R., & Black, J. (2008). Really responsive regulation. *The modern law review, 71*(1), 59-94.

Baluja, S., Seth, R., Sivakumar, D. S., Jing, Y., Yagnik, J., Kumar, S., . . . Aly, M. (2008). Video suggestion and discovery for you tube: Taking random walks through the view graph. In (pp. 895-904).

Bangcharoensap, P., Kobayashi, H., Shimizu, N., Yamauchi, S., & Murata, T. (2015). *Two step graph-based semi-supervised learning for online auction fraud detection.* Paper presented at the Machine Learning and Knowledge Discovery in Databases, Cham.

Bannister, F., & Connolly, R. (2014). ICT, public values and transformative government: A framework and programme for research. *Government Information Quarterly, 31*(1), 119-128. doi:10.1016/j.giq.2013.06.002

Bantekas, I. (2003). The international law of terrorist financing. *The American Journal of International Law, 97*(2), 315-333.

Barabasi, & Albert. (1999). Emergence of scaling in random networks. *Science (New York, N.Y.), 286*(5439), 509. doi:10.1126/science.286.5439.509

Barabási, A.-L. (2009). Scale-free networks: a decade and beyond. *Science (New York, N.Y.), 325*(5939), 412. doi:10.1126/science.1173299

Barabási, A.-L. (2013). Network science. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 371*(1987), 20120375.

Barnes, P., & Oloruntoba, R. (2005). Assurance of security in maritime supply chains: Conceptual issues of vulnerability and crisis management. *Journal of International Management, 11*(4), 519-540. doi:https://doi.org/10.1016/j.intman.2005.09.008

Barone, R., Delle Side, D., & Masciandaro, D. (2018). Drug trafficking, money laundering and the business cycle: Does secular stagnation include crime? *Metroeconomica, 69*(2), 409-426. doi:10.1111/meca.12193

Barone, R., & Masciandaro, D. (2011). Organized crime, money laundering and legal economy: theory and simulations. *European Journal of Law and Economics, 32*(1), 115-142. doi:10.1007/s10657-010-9203-x

Barone, R., & Schneider, F. G. (2018). Shedding Light on Money Laundering. Is It a Damping Wave? *SSRN Electronic Journal*. doi:10.2139/ssrn.3204289

Barratt, M. J. (2012). Silk Road: EBay for Drugs. *Addiction, 107*(3), 683-684. doi:10.1111/j.1360-0443.2011.03709.x

Basel Institute on Governance. (2014). *Basel AML Index 2014 Report*. Retrieved from

Bateman, L. R. (2016). *Shell companies: A regulatory and legal framework.* (M.S.), Utica College, ProQuest Dissertations Publishing, . Retrieved from https://search.proquest.com/docview/1836098499?accountid=26503

Battaglia, P. W., Hamrick, J. B., Bapst, V., Sanchez-Gonzalez, A., Zambaldi, V., Malinowski, M., . . . Pascanu, R. (2018). Relational inductive biases, deep learning, and graph networks. *arXiv e-prints*. Retrieved from https://ui.adsabs.harvard.edu/abs/2018arXiv180601261B

Beaulieu, T., Sarker, S., & Sarker, S. (2015). A Conceptual Framework for Understanding Crowdfunding. *CAIS, 37*, 1.

Becerra-Fernandez, I., Murphy, K. E., & Simon, S. J. (2000). Enterprise resource planning: integrating ERP in the business school curriculum. *Communications of the ACM, 43*(4), 39-41. doi:10.1145/332051.332066

Becker, G. S. (1968). Crime and Punishment: An Economic Approach. *Journal of Political Economy, 76*(2), 169-217. doi:10.1086/259394

Beer, S. (1985). *Diagnosing the system for organizations*: John Wiley & Sons Inc.

Bell, R. E. (2002). An introductory who's who for money laundering investigators. *Journal of Money Laundering Control, 5*(4), 287-295. doi: https://doi.org/10.1108/eb027309

Benson, K. (2016). *The facilitation of money laundering by legal and financial professionals: roles, relationships and response.* (Ph.D.), The University of Manchester (United Kingdom), Retrieved from https://search.proquest.com/docview/1837033760?accountid=26503

Berry, F. S., & Berry, W. D. (2018). Innovation and Diffusion Models in Policy Research. In *Theories of the policy process* (pp. 263-308): Routledge.

Bewley-Taylor, D. (2016). Towards metrics that measure outcomes that matter. *Policy Brief, 10*.

Bhagat, S., Cormode, G., & Muthukrishnan, S. (2011). Node Classification in Social Networks. In C. C. Aggarwal (Ed.), *Social Network Data Analytics* (pp. 115-148). Boston, MA: Springer.

Bhattacharjee, G. (2020, Oct 17). Tax on Agricultural Income: Holy Cow of the Indian Economy. *Economic and Political Weekly, 55*.

Bhattacharya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. *Decision Support Systems, 50*(3), 602-613. doi:http://dx.doi.org/10.1016/j.dss.2010.08.008

Biagioli, A. (2008). Financial crime as a threat to the wealth of nations. *Journal of Money Laundering Control, 11*(1), 88-95. doi:10.1108/13685200810844523

Bichler, G., Malm, A., & Cooper, T. (2017a). Drug supply networks: a systematic review of the organizational structure of illicit drug trade. *Crime Science, 6*(1), 1-23. doi:http://dx.doi.org/10.1186/s40163-017-0063-3

Bichler, G., Malm, A., & Cooper, T. (2017b). Drug supply networks: a systematic review of the organizational structure of illicit drug trade. *Crime Science, 6*(1), 2. doi:10.1186/s40163-017-0063-3

Bidabad, B. (2017). Money laundering detection system (MLD) (a complementary system of Rastin banking). *Journal of Money Laundering Control, 20*(4), 354-366. doi:10.1108/JMLC-04-2016-0016

Bjerregaard, E., & Kirchmaier, T. (2019). The Danske Bank Money Laundering Scandal: A Case Study. *Available at SSRN 3446636*.

Black, J., & Baldwin, R. (2010). Really Responsive Risk-Based Regulation. *Law & Policy, 32*(2), 181-213. doi:10.1111/j.1467-9930.2010.00318.x

Blankstein, A., Winter, T., & Schapiro, R. (2020). COVID-19 is costing drug cartels millions of dollars. Retrieved from https://www.nbcnews.com/news/crime-courts/covid-19-costing-drug-cartels-millions-dollars-n1213181

Bogdanoski, T. (2010). Accommodating the medical use of marijuana: surveying the differing legal approaches in Australia, the United States and Canada. *Journal of law and medicine, 17*(4), 508-531.

Bolton, R., & Hand, D. (2002). Statistical fraud detection: A review. *Statistical Science, 17*(3), 235-249. doi:10.1214/ss/1042727940

Borak, M. (2018). The final crackdown? China moves to completely ban and block cryptocurrency trading at home and abroad. Retrieved from https://technode.com/2018/02/05/china-ban-block-cryptocurrency-trading-at-home-abroad/

Botes, V., & Saadeh, A. (2018). Exploring evidence to develop a nomenclature for forensic accounting. *Pacific Accounting Review, 30*(2), 135-154. doi:10.1108/PAR-12-2016-0117

Bozhilova, K. (2018). [European Union: European Commission Proposes New Anti-Money Laundering Directives].

Breiman, L. (1996). Bagging Predictors. *Machine Learning, 24*(2), 123-140. doi:10.1023/A:1018054314350

Breiman, L. (2001). Random Forests. *Machine Learning, 45*(1), 5-32. doi:10.1023/a:1010933404324
Breiman, L., Friedman, J. H., Olshen, R., & Stone, C. J. (1984). *Classification and Regression Trees*: Wadsworth & Brooks.
Bresin, K., & Mekawi, Y. (2019). Do marijuana use motives matter? Meta-analytic associations with marijuana use frequency and problems. *Addictive Behaviors, 99*, 106102. doi:https://doi.org/10.1016/j.addbeh.2019.106102
Bright, D., Hughes, C., & Chalmers, J. (2012). Illuminating dark networks: a social network analysis of an Australian drug trafficking syndicate. *Crime, Law and Social Change, 57*(2), 151-176. doi:10.1007/s10611-011-9336-z
Bright, S., & Bartle, J. (2020). ACT cannabis laws come into effect on Friday, but they may not be what you hoped for. Retrieved from https://theconversation.com/act-cannabis-laws-come-into-effect-on-friday-but-they-may-not-be-what-you-hoped-for-130050
Broidy, L. M. (2001). A TEST OF GENERAL STRAIN THEORY*. *Criminology, 39*(1), 9-36. doi:10.1111/j.1745-9125.2001.tb00915.x
Brzoska, M. (2016). Consequences of Assessments of Effectiveness for Counterterrorist Financing Policy. *Administration & Society, 48*(8), 911-930. doi:10.1177/0095399714532272
Buchanan, B. (2004). Money laundering—a global obstacle. *Research in International Business and Finance, 18*(1), 115-127. doi:10.1016/j.ribaf.2004.02.001
Burden, K., & Palmer, C. (2003). Internet crime: Cyber Crime — A new breed of criminal? *Computer Law & Security Review, 19*(3), 222-227. doi:https://doi.org/10.1016/S0267-3649(03)00306-6
Cahill, M. H., Lambert, D., Pinheiro, J. C., & Sun, D. X. (2002). Detecting fraud in the real world. In *Handbook of massive data sets* (pp. 911-929): Springer.
Camdessus, M. (1998, February 10). *Money laundering: the importance of international countermeasures.* Paper presented at the Plenary Meeting of the Financial Action Task Force on Money Laundering, Paris.
Canhoto, A. I., & Backhouse, J. (2007). Profiling under conditions of ambiguity—An application in the financial services industry. *Journal of Retailing and Consumer Services, 14*(6), 408-419. doi:https://doi.org/10.1016/j.jretconser.2007.02.006
Carliner, H., Brown, Q. L., Sarvet, A. L., & Hasin, D. S. (2017). Cannabis use, attitudes, and legal status in the U.S.: A review. *Preventive Medicine, 104*, 13-23. doi:https://doi.org/10.1016/j.ypmed.2017.07.008
Carlson, S., & Seely, A. (2017). Using OpenRefine's Reconciliation to Validate Local Authority Headings. *Cataloging & Classification Quarterly, 55*(1), 1-11. doi:10.1080/01639374.2016.1245693
Castells, M. (2011). *The power of identity* (Vol. 14): John Wiley & Sons.
Catalini, C., & Gans, J. S. (2017). Some Simple Economics of the Blockchain. *Rotman School of Management Working Paper No. 2874598; MIT Sloan Research Paper No. 5191-16., Available at SSRN: https://ssrn.com/abstract=2874598*.
Cattuto, C., Quaggiotto, M., Panisson, A., & Averbuch, A. (2013). *Time-varying social networks in a graph database: a Neo4j use case*. Paper presented at the First International Workshop on Graph Data Management Experiences and Systems, New York, New York.
Caulkins, J. P., Kilmer, B., Kleiman, M., MacCoun, R. J., Midgette, G., Oglesby, P., . . . Reuter, P. H. (2015). *Considering marijuana legalization: Insights for Vermont and other jurisdictions*: Rand Corporation.
Chaikin, D. (2009). How effective are suspicious transaction reporting systems? *Journal of Money Laundering Control, 12*(3), 238-253. doi:10.1108/13685200910973628

Chan, G. C. K., & Hall, W. (2020). Estimation of the proportion of population cannabis consumption in Australia that is accounted for by daily users using Monte Carlo Simulation. *Addiction, n/a*(n/a). doi:10.1111/add.14909

Chan, G. C. K., Leung, J., Quinn, C., Weier, M., & Hall, W. (2018). Socio-economic differentials in cannabis use trends in Australia. *Addiction, 113*(3), 454-461. doi:10.1111/add.14010

Chan, P. K., Fan, W., Prodromidis, A. L., & Stolfo, S. J. (1999). Distributed Data Mining in Credit Card Fraud Detection. *IEEE Intelligent Systems and Their Applications, 14*(6), 67-74. doi:10.1109/5254.809570

Chance, C. (2018). Initial Coin Offerings – Asking The Right Regulatory Questions. Retrieved from https://talkingtech.cliffordchance.com/content/micro-cctech/en/fintech/initial-coin-offerings/_jcr_content/text/parsysthumb/download/file.res/Initial%20Coin%20Offerings.pdf

Chang, R., Lee, A., Ghoniem, M., Kosara, R., Ribarsky, W., Yang, J., . . . Sudjianto, A. (2008). Scalable and Interactive Visual Analysis of Financial Wire Transactions for Fraud Detection. *Information Visualization, 7*(1), 63-76. doi:10.1057/palgrave.ivs.9500172

Chang, T. Y., & Jacobson, M. (2017). Going to pot? The impact of dispensary closures on crime. *Journal of Urban Economics, 100*, 120-136. doi:https://doi.org/10.1016/j.jue.2017.04.001

Chapple, L., Dunstan, K., & Truong, T. P. (2018). Corporate governance and management earnings forecast behaviour: Evidence from a low private litigation environment. *Pacific Accounting Review, 30*(2), 222-242. doi:10.1108/PAR-09-2016-0081; 16

10.1108/PAR-09-2016-0081

Chatwin, C. (2017). UNGASS 2016: Insights from Europe on the development of global cannabis policy and the need for reform of the global drug policy regime. *International Journal of Drug Policy, 49*, 80-85. doi:https://doi.org/10.1016/j.drugpo.2015.12.017

Chen, D., Lü, L., Shang, M.-S., Zhang, Y.-C., & Zhou, T. (2012). Identifying influential nodes in complex networks. *Physica A: Statistical Mechanics and its Applications, 391*(4), 1777-1787. doi:10.1016/j.physa.2011.09.017

Chen, K. C., Cheng, Q., Lin, Y. C., Lin, Y. C., & Xiao, X. (2016). Financial reporting quality of Chinese reverse merger firms: The reverse merger effect or the weak country effect? *Accounting Review, 91*(5), 1363-1390. doi:10.2308/accr-51376

Chen, Y., & Soileau, J. S. (2014). Does pedigree matter? Earnings quality of U.S. listed domestic firms via reverse mergers. *Journal of Accounting and Public Policy, 33*(6), 573-595. doi://doi.org/10.1016/j.jaccpubpol.2014.08.003

Choo, K. K. R. (2015). Cryptocurrency and Virtual Currency: Corruption and Money Laundering/Terrorism Financing Risks? In *Handbook of Digital Currency* (pp. 283-307). San Diego: Academic Press.

Christensen, J. (2011). The looting continues: tax havens and corruption. *Critical Perspectives on International Business, 7*(2), 177-196. doi://dx.doi.org/10.1108/17422041111128249

Christensen, J. (2012). The hidden trillions: Secrecy, corruption, and the offshore interface. *Crime, Law and Social Change, 57*(3), 325-343. doi://dx.doi.org/10.1007/s10611-011-9347-9

Christin, N. (2012). Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace.

Chu, H., Lai, C. C., & Cheng, C. C. (2015). Tax Havens, Growth, and Welfare. *Journal of Public Economic Theory, 17*(6), 802-823.

Chu, Y.-W. L., & Gershenson, S. (2018). High times: The effect of medical marijuana laws on student time use. *Economics of Education Review, 66*, 142-153. doi:https://doi.org/10.1016/j.econedurev.2018.08.003
Chu, Y.-W. L., & Townsend, W. (2019). Joint culpability: The effects of medical marijuana laws on crime. *Journal of Economic Behavior & Organization, 159*, 502-525. doi:https://doi.org/10.1016/j.jebo.2018.07.003
Clarke, R. V. (1983). Situational Crime Prevention: Its Theoretical Basis and Practical Scope. *Crime and Justice, 4*, 225-256.
Clarke, R. V., & Cornish, D. B. (1985). Modeling Offenders' Decisions: A Framework for Research and Policy. *Crime and Justice, 6*, 147-185.
Clarke, R. V. G., & Felson, M. (1993). *Routine activity and rational choice* (Vol. 5): Transaction publishers.
Clarke, R. V. G., & Webb, B. (1999). *Hot products: Understanding, anticipating and reducing demand for stolen goods* (Vol. 112): Citeseer.
Clauset, A., Moore, C., & Newman, M. E. J. (2008). Hierarchical structure and the prediction of missing links in networks. *Nature, 453*(7191), 98. doi:10.1038/nature06830
CMC. (2005). *Money Laundering,Background Intelligence Briefing*. Retrieved from Queensland, Australia:
Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review, 44*(4), 588. doi:10.2307/2094589
Colladon, A. F., & Remondi, E. (2017). Using social network analysis to prevent money laundering. *Expert Systems with Applications, 67*, 49-58. doi:10.1016/j.eswa.2016.09.029
Collin, M. (2019). Illicit Financial Flows: Concepts, Measurement, and Evidence. *World Bank Research Observer, 35*(1), 44-86. doi:10.1093/wbro/lkz007
Compin, F. (2008). The role of accounting in money laundering and money dirtying. *Critical Perspectives on Accounting, 19*(5), 591-602. doi:10.1016/j.cpa.2007.01.001
Congress, T. L. L. o. (2018a). *Regulation of Cryptocurrency Around the World*. Retrieved from https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf
Congress, T. L. L. o. (2018b). Regulation of Cryptocurrency: China. Retrieved from https://www.loc.gov/law/help/cryptocurrency/china.php
Cooley, A., Heathershaw, J., & Sharman, J. C. (2018). Laundering Cash, White Washing Reputations. *Journal of Democracy, 29*(1), 39-53. doi:10.1353/jod.2018.0003
Cornish, D. B., & Clarke, R. V. (1987). Understanding Crime Displacement: An Application of Rational Choice Theory. *Criminology (Beverly Hills), 25*(4), 933-948. doi:10.1111/j.1745-9125.1987.tb00826.x
Cortes, C., Pregibon, D., & Volinsky, C. (2003). Computational Methods for Dynamic Graphs. *Journal of Computational and Graphical Statistics, 12*(4), 950-970. doi:10.1198/1061860032742
Cowdock, B. (2017). *Hiding in Plain Sight: How UK Companies are used to launder corrupt wealth*. Retrieved from United Kingdom: http://www.transparency.org.uk/publications/hiding-in-plain-sight/#.WwInj3eFO70
Cowdock, B., & Simeone, G. (2019). *At Your Service- Investigating how UK businesses and institutions help corrupt indivduals and regimes launder their money and reputations*. Retrieved from United Kingdom: https://www.transparency.org.uk/uncovered-uk-businesses-corruption-money-laundering-cases/
Cunliffe, J., Martin, J., Décary-Hétu, D., & Aldridge, J. (2017). An island apart? Risks and prices in the Australian cryptomarket drug trade. *International Journal of Drug Policy, 50*, 64-73. doi:https://doi.org/10.1016/j.drugpo.2017.09.005

Dalby, D., & Wilson-Chapman, A. (2019). Panama Papers Helps Recover More Than $1.2 Billion Around The World. Retrieved from https://www.icij.org/investigations/panama-papers/panama-papers-helps-recover-more-than-1-2-billion-around-the-world/

Dalins, J., Wilson, C., & Carman, M. (2018). Criminal motivation on the dark web: A categorisation model for law enforcement. *Digital Investigation, 24*, 62-71. doi:https://doi.org/10.1016/j.diin.2017.12.003

Davis, C., Farrell, R., & Ogilby, S. (2010). Characteristics and skills of the Forensic Accountant. *American Institute of Certified Public Accountants*.

Degenhardt, L., Whiteford, H. A., Ferrari, A. J., Baxter, A. J., Charlson, F. J., Hall, W. D., . . . Vos, T. (2013). Global burden of disease attributable to illicit drug use and dependence: findings from the Global Burden of Disease Study 2010. *The Lancet, 382*(9904), 1564-1574. doi:https://doi.org/10.1016/S0140-6736(13)61530-5

Degryse, H., Karas, A., & Schoors, K. (2019). Relationship lending during a trust crisis on the interbank market: A friend in need is a friend indeed. *Economics Letters, 182*, 1-4. doi:https://doi.org/10.1016/j.econlet.2019.03.019

Demetis, D. S. (2018). Fighting money laundering with technology: A case study of Bank X in the UK. *Decision Support Systems, 105*, 96-107. doi:https://doi.org/10.1016/j.dss.2017.11.005

Deng, X., Joseph, V. R., Sudjianto, A., & Wu, C. F. J. (2009). Active Learning Through Sequential Design, With Applications to Detection of Money Laundering. *Journal of the American Statistical Association, 104*(487), 969-981. doi:10.1198/jasa.2009.ap07625

Derrig, R. A., & Francis, L. A. (2008). Distinguishing the Forest from the TREES: A Comparison of Tree-Based Data Mining Methods. *Variance, 2*(2), 184-208.

DeVoe, R. (2018). Benebit – The Biggest ICO Exit Scam In History Nets Up to $4 Million. Retrieved from https://www.coinbureau.com/ico/benebit-biggest-ico-exit-scam-history-nets-4-million/

Dharmapala, D., & Hines, J. R. (2009). Which countries become tax havens? *Journal of Public Economics, 93*(9), 1058-1068. doi:10.1016/j.jpubeco.2009.07.005

Didimo, W., Liotta, G., Montecchiani, F., & Palladino, P. (2011). An advanced network visualization system for financial crime detection. In (pp. 203-210).

Digabriele, J. A. (2008). An Empirical Investigation of the Relevant Skills of Forensic Accountants. *Journal of Education for Business, 83*(6), 331-338. doi:10.3200/JOEB.83.6.331-338

Ding, C. H. Q., He, X., Zha, H., Gu, M., & Simon, H. D. (2001, 29 Nov.-2 Dec. 2001). *A min-max cut algorithm for graph partitioning and data clustering.* Paper presented at the Proceedings 2001 IEEE International Conference on Data Mining.

Does de Willebois, E. v. d., Halter, E. M., Harrison, R. A., Park, J. W., & Sharman, J. C. (2011). *The Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do About It*. Washington D.C.: The World Bank.

Dostov, V., & Shust, P. (2014). Cryptocurrencies: an unconventional challenge to the AML/CFT regulators? *Journal of Financial Crime, 21*(3), 249-263.

Dowers, K., & Palmreuther, S. (2003). Developing an international consensus to combat money laundering and terrorism financing. *Infrastructure and Financial Markets Review, 9*(1), 1-7.

Dragone, D., Prarolo, G., Vanin, P., & Zanella, G. (2019). Crime and the legalization of recreational marijuana. *Journal of Economic Behavior & Organization, 159*, 488-501. doi:https://doi.org/10.1016/j.jebo.2018.02.005

Drakopoulos, G., Baroutiadi, A., & Megalooikonomou, V. (2015). *Higher order graph centrality measures for Neo4j*. Paper presented at the 2015 6th International Conference on Information, Intelligence, Systems and Applications (IISA).

Drayton, F. R. (2002). Dirty Money, Tax and Banking: Recent Developments Concerning Mutual Legal Assistance and Money Laundering in the Caribbean Region and the Region's Responses. *Journal of Money Laundering Control, 5*(4), 338-344. doi:10.1108/eb027316

Drezewski, R., Sepielak, J., & Filipkowski, W. (2012). System supporting money laundering detection. *Digital Investigation, 9*(1), 8-21. doi:10.1016/j.diin.2012.04.003

Dunstan, K., & Gepp, A. (2018). Guest editorial. *Pacific Accounting Review, 30*(2), 130-134. doi:doi:10.1108/PAR-01-2018-0009

Eifrem, E. (2019). How graph technology can map patterns to mitigate money-laundering risk. *Computer Fraud & Security, 2019*(10), 6-8. doi:https://doi.org/10.1016/S1361-3723(19)30105-8

Elkan, C. (2001). Magical thinking in data mining: Lessons from CoIL challenge 2000. In F. Provost, R. Srikant, M. Schkolnick, & D. Lee (Eds.), (pp. 426-431).

Emerson, R. M. (1962). Power-dependence relations. *American Sociological Review*, 31-41.

Ene, C. M. (2014). Measuring Money Laundering Using "The Walker Gravity Model". *Annales Universitatis Apulensis Series Oeconomica, 2*(16), 1-13.

Ernst & Young. (2017). EY research: initial coin offerings (ICOs). Retrieved from http://www.ey.com/Publication/vwLUAssets/ey-research-initial-coin-offerings-icos/$File/ey-research-initial-coin-offerings-icos.pdf

Ernst & Young. (2018). Big risks in ICO market: flawed token valuations, unclear regulations, heightened hacker attention and congested networks. Retrieved from http://www.ey.com/Publication/vwLUAssets/ey-research-initial-coin-offerings-icos/$File/ey-research-initial-coin-offerings-icos.pdf

ESMA. (2017). ESMA highlights ICO risks for investors and firms [Press release]. Retrieved from https://www.esma.europa.eu/sites/default/files/library/esma71-99-649_press_release_ico_statements.pdf

Europol. (2019). Multi-million Euro cryptocurrency laundering service Bestmixer.io taken down [Press release]. Retrieved from https://www.europol.europa.eu/newsroom/news/multi-million-euro-cryptocurrency-laundering-service-bestmixerio-taken-down

Ezawa, K. J., & Norton, S. W. (1996). Constructing Bayesian networks to predict uncollectible telecommunications accounts. *IEEE Expert-Intelligent Systems and their Applications, 11*(5), 45-51. doi:10.1109/64.539016

Fakhraei, S., Foulds, J., Shashanka, M., & Getoor, L. (2015). Collective spammer detection in evolving multi-relational social networks. In (Vol. 2015-, pp. 1769-1778): Association for Computing Machinery.

FATF. (2012). The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. *Financial Action Task Force*.

Fawcett, T. (2003). "In vivo" spam filtering: a challenge problem for KDD. *ACM Sigkdd Explorations Newsletter, 5*(2), 140. doi:10.1145/980972.980990

Fawcett, T., & Provost, F. J. (1999). *Activity Monitoring: Noticing Interesting Changes in Behavior*. Paper presented at the KDD.

FCA. (2017). Distributed Ledger Technology: Feedback Statement on Discussion Paper 17/03. Retrieved from https://www.fca.org.uk/publication/feedback/fs17-04.pdf

Fei, L., Zhang, Q., & Deng, Y. (2018). Identifying influential nodes in complex networks based on the inverse-square law. *Physica A: Statistical Mechanics and its Applications, 512*, 1044-1059. doi:https://doi.org/10.1016/j.physa.2018.08.135

Felson, M., & Boba, R. (2010). *Crime and everyday life*: SAGE Publications Inc.

Ferwerda, J. (2009). The economics of crime and money laundering: Does anti-money laundering policy reduce crime? *Review of Law and Economics, 5*(2), 903-929. doi:10.2202/1555-5879.1421

Ferwerda, J., Kattenberg, M., Chang, H. H., Unger, B., Groot, L., & Bikker, J. A. (2013). Gravity models of trade-based money laundering. *Applied Economics, 45*(22), 3170-3182. doi:10.1080/00036846.2012.699190

Ferwerda, J., & Kleemans, E. R. (2019). Estimating Money Laundering Risks: An Application to Business Sectors in the Netherlands. *European Journal on Criminal Policy and Research, 25*(1), 45-62. doi:10.1007/s10610-018-9391-4

Ferwerda, J., van Saase, A., Unger, B., & Getzner, M. (2020). Estimating money laundering flows with a gravity model-based simulation. *Scientific Reports, 10*(1), 18552. doi:10.1038/s41598-020-75653-x

Findley, M. G., Nielson, D. L., & Sharman, J. C. (2013). Using field experiments in international relations: A randomized study of anonymous incorporation. *International Organization, 67*(4), 657-693. doi:10.1017/S0020818313000271

Findley, M. G., Nielson, D. L., & Sharman, J. C. (2015). Causes of noncompliance with international law: A field experiment on anonymous incorporation. *American Journal of Political Science, 59*(1), 146-161. doi:10.1111/ajps.12141

FINMA. (2017). FINMA Guidance 04/2017 Regulatory treatment of initial coin offerings. Retrieved from https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20170929-finma-aufsichtsmitteilung-04-2017.pdf?la=en

FINMA. (2018). *Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)*. Retrieved from

Fitina, L., Imbal, J., Uiari, V., Murki, N., & Goodyear, E. (2010). An application of minimum spanning trees to travel planning. *Contemporary PNG Studies, 12*, 1.

Fleming, L., & Sorenson, O. (2016). Financing by and for the Masses: An Introduction to the Special Issue on Crowdfunding. *California Management Review, 58*(2), 5-19. doi:10.1525/cmr.2016.58.2.5

Floros, I. V., & Sapp, T. R. A. (2011). Shell games: On the value of shell companies. *Journal of Corporate Finance, 17*(4), 850-867. doi:10.1016/j.jcorpfin.2011.03.004

Floyd, D. (2018). Vietnam Investigates ICO Fraud After $660 Million in Losses Reported. Retrieved from https://www.coindesk.com/vietnam-investigates-ico-fraud-660-million-losses-reported/

Foster, D. P., & Stine, R. A. (2004). Variable Selection in Data Mining: Building a Predictive Model for Bankruptcy. *Journal of the American Statistical Association, 99*(466), 303-313. doi:10.1198/016214504000000287

Friedman, J. (1999). *Greedy function approximation: a gradient boosting machine*. Technical Report, Department of Statistics, Stanford University.

Friedman, J. (2002). Stochastic gradient boosting. *Computational Statistics and Data Analysis, 38*(4), 367-378. doi:10.1016/s0167-9473(01)00065-2

Fritsche, I. (2005). Predicting Deviant Behavior by Neutralization: Myths and Findings. *Deviant Behavior, 26*(5), 483-510. doi:10.1080/016396290968489

FSI. (2019). *ICO Survey Results and Future Direction*. Retrieved from South Korea: http://www.fsc.go.kr/info/ntc_news_view.jsp?bbsid=BBS0030&page=1&sch1=&sword=&r_url=&menu=7210100&no=32932

Gansner, E. R., & North, S. C. (2000). An open graph visualization system and its applications to software engineering. *Software: Practice and Experience, 30*(11), 1203-1233. doi:10.1002/1097-024X(200009)30:11<1203::AID-SPE338>3.0.CO;2-N

Gao, Z. (2009). *Application of cluster-based local outlier factor algorithm in anti-money laundering.* Paper presented at the Proceedings - International Conference on Management and Service Science, MASS 2009.

Gao, Z., & Ye, M. (2007). A framework for data mining-based anti-money laundering research. *Journal of Money Laundering Control, 10*(2), 170-179. doi:10.1108/13685200710746875

Garside, J. (2019). Q&A: What is the 'Troika Laundromat' and how did it work? Retrieved from https://www.theguardian.com/world/2019/mar/04/qa-what-is-the-troika-laundromat-and-how-did-it-work

Garvey, P. (2018). Blockchain-backed gold: Mint's answer to bitcoin.

Gepp, A. (2015). *Financial statement fraud detection using supervised learning methods.* Bond University, Gold Coast, Queensland.

Gepp, A. (2016). Addressing the problem of financial statement fraud: Better detection through improved models. In *8th Asia-Pacific Interdisciplinary Research in Accounting (APIRA) Conference*. Melbourne, Australia.

Gepp, A., Kumar, K., & Bhattacharya, S. (2010). Business failure prediction using decision trees. *Journal of Forecasting, 29*(6), 536-555. doi:10.1002/for.1153

Gepp, A., Linnenluecke, M. K., O'Neill, T. J., & Smith, T. (2018). Big data techniques in auditing research and practice: Current trends and future opportunities. *Journal of Accounting Literature, 40*, 102-115. doi:https://doi.org/10.1016/j.acclit.2017.05.003

Ghosh, S., & Reilly, D. L. (1994). Credit card fraud detection with a neural-network. In (Vol. 3, pp. 621-630): Publ by IEEE.

Ghosh, T. S., Vigil, D. I., Maffey, A., Tolliver, R., Van Dyke, M., Kattari, L., . . . Wolk, L. (2017). Lessons learned after three years of legalized, recreational marijuana: The Colorado experience. *Preventive Medicine, 104*, 4-6. doi:https://doi.org/10.1016/j.ypmed.2017.02.021

Gilbert, J. A., & Sharman, J. C. (2016). Turning a Blind Eye to Bribery: Explaining Failures to Comply with the International Anti-corruption Regime. *Political Studies, 64*(1), 74-89. doi:10.1111/1467-9248.12153; 20

10.1111/1467-9248.12153

Gilmour, N. (2015). Understanding the practices behind money laundering – A rational choice interpretation. *International Journal of Law, Crime and Justice, 44*(C). doi:10.1016/j.ijlcj.2015.03.002

Gilmour, N. (2016a). Preventing money laundering: a test of situational crime prevention theory. *Journal of Money Laundering Control, 19*(4), 376-396. doi:http://dx.doi.org/10.1108/JMLC-10-2015-0045

Gilmour, N. (2016b). Understanding the practices behind money laundering – A rational choice interpretation. *International Journal of Law, Crime and Justice, 44*, 1-13. doi:https://doi.org/10.1016/j.ijlcj.2015.03.002

Gilmour, N. (2017). Blindingly obvious and frequently exploitable- Money laundering through the purchasing of high-value portable commodities. *Journal of Money Laundering Control, 20*(2), 105-115. doi:10.1108/JMLC-08-2016-0035

Gleason, K. C., Rosenthal, L., & Wiggins, R. A. (2005). Backing into being public: an exploratory analysis of reverse takeovers. *Journal of Corporate Finance, 12*(1), 54-79. doi:10.1016/j.jcorpfin.2004.08.001

Gleasure, R., & Feller, J. (2016). Emerging technologies and the democratisation of financial services: A metatriangulation of crowdfunding research. *Information and Organization, 26*(4), 101-115.

Global Drug Survey. (2015). Global Drug Survey Findings. Retrieved from https://www.globaldrugsurvey.com/the-global-drug-survey-2015-findings/

Goyal, P., & Ferrara, E. (2018). Graph embedding techniques, applications, and performance: A survey. *Knowledge-Based Systems, 151*, 78-94. doi:https://doi.org/10.1016/j.knosys.2018.03.022

Gup, B. E., & Beekarry, N. (2009). Limited liability companies (LLCs) and financial crimes. *Journal of Money Laundering Control, 12*(1), 7-18. doi://dx.doi.org/10.1108/13685200910922615

Hao, W., Zhisong, P., Guyu, H., Liangliang, Z., Haimin, Y., Xin, L., & Xingyu, Z. (2018). Identifying influential nodes based on network representation learning in complex networks. *PloS one, 13*(7), e0200091. doi:10.1371/journal.pone.0200091

Harding, L. (2016). What are the Panama Papers? A guide to history's biggest data leak. *The Guardian*. Retrieved from http://www.theguardian.com/news/2016/apr/03/what-you-need-to-know-about-the-panama-papers

Harvey, J. (2008). Just How Effective is Money Laundering Legislation? *Security Journal, 21*(3), 189-211. doi:10.1057/palgrave.sj.8350054

Hassan, M., & Schneider, F. (2016a). Modelling the Egyptian Shadow Economy: A MIMIC model and A Currency Demand approach. *Journal of Economics and Political Economy, 3*(2), 309-339.

Hassan, M., & Schneider, F. (2016b). Size and Development of the Shadow Economies of 157 Worldwide Countries: Updated and New Measures from 1999 to 2013. *Journal of Global Economics, 04*(03). doi:10.4172/2375-4389.1000218

Hawking, P., McCarthy, B., & Stein, A. (2005). Integrating ERP's second wave into higher education curriculum. *PACIS 2005 Proceedings*, 83.

Helms, K. (2019). France Adopts New Crypto Regulation. Retrieved from https://news.bitcoin.com/france-cryptocurrency-regulation/

Hendriyetty, N., & Grewal, B. S. (2017). Macroeconomics of money laundering: effects and measurements. *Journal of Financial Crime, 24*(1), 65-81. doi:10.1108/JFC-01-2016-0004

Herman, I., Melancon, G., & Marshall, M. S. (2000). Graph visualization and navigation in information visualization: A survey. *Ieee Transactions On Visualization And Computer Graphics, 6*(1), 24-43. doi:10.1109/2945.841119

Hill, K. M. (2016). In search of useful collection metadata: using openrefine to create accurate, complete, and clean title-level collection information. *Serials Review, 42*(3), 222-228.

Hite, J. M., Williams, E. J., & Baugh, S. C. (2005). Multiple networks of public school administrators: An analysis of network content and structure. *International Journal of Leadership in Education, 8*(2), 91-122. doi:10.1080/1360312042000329086

Ho, J. K. S. (2017). Disclosure of beneficial ownership of companies in Hong Kong. *Common Law World Review, 46*(4), 251-268. doi:10.1177/1473779517731749; 20

10.1177/1473779517731749

Hobbs, D., Hadfield, P., Lister, S., & Winlow, S. (2005). Violence and control in the night-time economy. *European Journal of Crime, Criminal Law and Criminal Justice, 13*(1), 89-102. doi:10.1163/1571817053558310

Hoffman, A. N., Stearns, T. M., & Shrader, C. B. (1990). Structure, context, and centrality in interorganizational networks. *Journal of Business Research, 20*(4), 333-347. doi:10.1016/0148-2963(90)90010-B

Hoiberg, P. (1999). Accounting in the New Millennium. *Pacific Accounting Review, 11*(1-2), 131-136. doi:10.1108/eb037934

Holtz, L., & Sarlo Neto, A. (2014). Effects of Board of Directors' Characteristics on the Quality of Accounting Information in Brazil. *Revista Contabilidade & Finanças, 25*(66), 255-266. doi:10.1590/1808-057x201412010

Houlder, V. (2017). [UK shell companies linked to £80bn money laundering].

Hout, M. C. V., & Bingham, T. (2013). Silk Road, the virtual drug marketplace: A single case study of user experiences. *International Journal of Drug Policy, 24*(5), 385-391. doi:10.1016/j.drugpo.2013.01.005

Howieson, B. (2005). Can we teach auditors and accountants to be more ethically competent and publicly accountable. *Ethics and Auditing*, 265-288.

Howieson, B. (2018). What is the 'good' forensic accountant? A virtue ethics perspective. *Pacific Accounting Review, 30*(2), 155-167. doi:10.1108/PAR-01-2017-0005

Huang, H., & Dong, Z. (2013). *Research on architecture and query performance based on distributed graph database neo4j*. Paper presented at the 2013 3rd International Conference on Consumer Electronics, Communications and Networks.

Huang, J. Y. (2015). Effectiveness of US anti-money laundering regulations and HSBC case study. *Journal of Money Laundering Control, 18*(4), 525-532. doi:10.1108/JMLC-05-2015-0018; 23

10.1108/JMLC-05-2015-0018

Hubbs, R. C. (2018). Anonymous Shell Companies Rising. *Fraud Magazine*.

Huber, W. (2017). Forensic accounting, fraud theory, and the end of the fraud triangle. *Journal of Theoretical Accounting Research, 12*(2).

Hughes, C. (2020). *The Australian (illicit) Drug Policy Timeline: 1985-2019*. Retrieved from Australia: https://ndarc.med.unsw.edu.au/sites/default/files/ndarc/resources/Australian%20Illicit%20Drug%20Policy%20Timeline%20-%201985-2019%20-%20FINAL.pdf

Hughes, C. E., Bright, D. A., & Chalmers, J. (2017). Social network analysis of Australian poly-drug trafficking networks: How do drug traffickers manage multiple illicit drugs? *Social Networks, 51*, 135-147. doi:https://doi.org/10.1016/j.socnet.2016.11.004

Hughes, C. E., Chalmers, J., Bright, D. A., & McFadden, M. (2016). Poly-drug trafficking: Estimating the scale, trends and harms at the Australian border. *International Journal of Drug Policy, 31*, 80-89. doi:https://doi.org/10.1016/j.drugpo.2016.01.005

Hughes, C. E., Lancaster, K., & Spicer, B. (2011). How do Australian news media depict illicit drug issues? An analysis of print media reporting across and between illicit drugs, 2003–2008. *International Journal of Drug Policy, 22*(4), 285-291. doi:https://doi.org/10.1016/j.drugpo.2011.05.008

Hughes, C. E., Ritter, A., Lancaster, K., & Hoppe, R. (2017). Understanding policy persistence—The case of police drug detection dog policy in NSW, Australia. *International Journal of Drug Policy, 44*, 58-68. doi:https://doi.org/10.1016/j.drugpo.2017.03.007

IBM. (2018). Maersk and IBM to Form Joint Venture Applying Blockchain to Improve Global Trade and Digitize Supply Chains. Retrieved from https://www-03.ibm.com/press/us/en/pressrelease/53602.wss

Ienco, D., Meo, R., & Botta, M. (2008). Using PageRank in feature selection. In (pp. 93-100).

International Consortium of Investigative Journalists. ICIJ offshore leaks database. Retrieved from https://offshoreleaks.icij.org/#_ga=1.90578010.1932562669.1464270097
Irwin, A. S. M., Kim-Kwang, R. C., & Liu, L. (2012). An analysis of money laundering and terrorism financing typologies. *Journal of Money Laundering Control, 15*(1), 85-111. doi://dx.doi.org/10.1108/13685201211194745
Iwasokun, G. B., Akinyede, R. O., Fadamiro, C. F., & Bello, O. A. (2019). Factor analysis of financial crime-related issues. *Journal of Financial Crime, 26*(1), 113-130. doi:10.1108/JFC-11-2017-0120
Jacobs, B. A., & Wright, R. (2006). *Street justice: Retaliation in the criminal underworld*: Cambridge University Press.
Jacques, S., Rosenfeld, R., Wright, R., & van Gemert, F. (2016). Effects of Prohibition and Decriminalization on Drug Market Conflict. *Criminology & Public Policy, 15*(3), 843-875. doi:10.1111/1745-9133.12218
Jacques, S., & Wright, R. (2013). How victimized drug traders mobilize police. *Journal of Contemporary Ethnography, 42*(5), 545-575.
Jakobi, A. P. (2018). Governing illicit finance in transnational security spaces: the FATF and anti-money laundering. *Crime, Law and Social Change, 69*(2), 173-190. doi:10.1007/s10611-017-9750-y
Jancsics, D. (2017). Offshoring at Home? Domestic Use of Shell Companies for Corruption. *Public Integrity, 19*(1), 4-21. doi:10.1080/10999922.2016.1200412
JCBA. (2019). *Recommendation on New ICO Regulation*. Retrieved from https://cryptocurrency-association.org/news/main-info/20190308-001/
JFSA. (2017). Details of Screening for New Registration Application as Virtual Currency Exchange Service Provider Retrieved from https://www.fsa.go.jp/en/news/2017/20170930-1/02.pdf
Johannesen, N., Tørsløv, T., & Wier, L. (2016). Are less developed countries more exposed to multinational tax avoidance? Method and evidence from micro-data. *The World Bank Economic Review*.
Ju, C., & Zheng, L. (2009). *Research on Suspicious Financial Transactions Recognition Based on Privacy-Preserving of Classification Algorithm.* Paper presented at the 2009 First International Workshop on Education Technology and Computer Science.
Kaiser, H. F. (1960). The application of electronic computers to factor analysis. *Educational and psychological measurement, 20*(1), 141-151.
Kamps, J., & Kleinberg, B. (2018). To the moon: defining and detecting cryptocurrency pump-and-dumps. *Crime Science, 7*(1), 18. doi:10.1186/s40163-018-0093-5
Katz, L. (1953). A new status index derived from sociometric analysis. *Psychometrika, 18*(1), 39-43. doi:10.1007/BF02289026
Kennedy, J. (2016). $1.4bn investment in blockchain start-ups in last 9 months, says PwC expert. Retrieved from https://www.siliconrepublic.com/start-ups/blockchain-pwc-investment
Kenno, S. A., & Free, C. (2018). Fostering and forcing uses of accounting: Labour-management negotiations in the automotive crisis in Canada 2008–2009. *Management Accounting Research, 39*, 17-34. doi://doi.org/10.1016/j.mar.2017.06.001
Kersten, A. (2002). Financing of Terrorism—A Predicate Offence to Money Laundering? In *Financing Terrorism* (pp. 49-56): Springer.
Khaled, H., Kuldeep, K., & Adrian, G. (2018). Using Cutting-Edge Tree-Based Stochastic Models to Predict Credit Risk. *Risks, 6*(2), 55. doi:10.3390/risks6020055
Khan, W. A., Jawaid, S. T., & Arif, I. (2018). Where does a nation's wealth go? Evidence from a third world country. *Journal of Money Laundering Control, 21*(3), 426-476. doi:10.1108/JMLC-01-2017-0005

Kharpal, A. (2018). [Bank of England's Carney calls for more regulation around the 'speculative mania' of cryptocurrencies]. Web Page.
Khatri, Y. (2019). South Korea Will Maintain ICO Ban After Finding Token Projects Broke Rules. Retrieved from https://www.coindesk.com/south-korea-will-maintain-ico-ban-after-finding-token-projects-broke-rules
Kido, G. S., Igawa, R. A., & Barbon, S. (2016). Topic modeling based on louvain method in online social networks. In (pp. 353-360): Universidade Federal de Santa Catarina, Florianopolis - UFSC/Departamento de Informatica e Estatistica.
Kihara, T. (2018). [Hong Kong to tighten cryptocurrency rules]. Web Page.
Kilmer, B., Caulkins, J. P., Pacula, R. L., MacCoun, R. J., & Reuter, P. (2010). *Altered state? Assessing how marijuana legalization in California could influence marijuana consumption and public budgets*: RAND Santa Monica, CA.
Kilmer, B., & Pacula, R. L. (2017). Understanding and learning from the diversification of cannabis supply laws. *Addiction, 112*(7), 1128-1135. doi:10.1111/add.13623
Kim, A. B., & Holmes, K. R. (2016). 2014 Index of economic freedom. *The Heritage Foundation in Partnership with Wall Street Journal*.
Kim, Y. (2017). Behind South Korea's Cryptocurrency Boom. Retrieved from https://www.technologyreview.com/s/609561/behind-south-koreas-cryptocurrency-boom/
Kingdon, J. W., & Stano, E. (1984). *Agendas, alternatives, and public policies* (Vol. 45): Little, Brown Boston.
Kleiman, M. A. R., & Heussler, L. (2011). Crime-minimizing drug policy. *Journal of Criminal Justice, 39*(3), 286-288. doi:https://doi.org/10.1016/j.jcrimjus.2011.04.002
Knight, W. (2017). The Technology Behind Bitcoin Is Shaking Up Much More Than Money. Retrieved from https://www.technologyreview.com/s/604148/the-technology-behind-bitcoin-is-shaking-up-much-more-than-money/
Knust, S., & Stewart, A. L. (2002). Risk-Taking Behaviour and Criminal Offending: An Investigation of Sensation Seeking and the Eysenck Personality Questionnaire. *International Journal of Offender Therapy and Comparative Criminology, 46*(5), 586-602. doi:10.1177/030662402236742
Koh, J.-m. (2006). *Suppressing terrorist financing and money laundering*: Springer Science & Business Media.
Kotabe, M. (2005). Global security risks and international competitiveness. *Journal of International Management, 11*(4), 453-455. doi:https://doi.org/10.1016/j.intman.2005.09.004
Kranacher, M.-J., Riley, R., & Wells, J. T. (2011). *Forensic accounting and fraud examination*. New York, NY: John Wiley & Sons.
Krauth, O. (2018). 5 companies using blockchain to drive their supply chain. Retrieved from https://www.techrepublic.com/article/5-companies-using-blockchain-to-drive-their-supply-chain/
Krebs, V. E. (2002). Mapping networks of terrorist cells. *Connections, 24*(3), 43-52.
Krieger, T., & Meierrieks, D. (2011). Terrorist financing and money laundering. *Available at SSRN 1860069*.
Kshetri, N. (2005). Pattern of global cyber war and crime: A conceptual framework. *Journal of International Management, 11*(4), 541-562. doi:https://doi.org/10.1016/j.intman.2005.09.009
Kübler, D. (2001). Understanding policy change with the advocacy coalition framework: an application to Swiss drug policy. *Journal of European Public Policy, 8*(4), 623-641. doi:10.1080/13501760110064429

Kubzansky, C. (2018). Nine essential tools from ICIJ's data journalists and programmers. In *ICIJ*: International Consortium of Investigative Journalists.

Kumar, K., & Bhattacharya, S. (2006). Artificial neural network vs linear discriminant analysis in credit ratings forecast. *Review of Accounting and Finance, 5*(3), 216-227. doi:10.1108/14757700610686426

Kumar, K., Bhattacharya, S., & Hicks, R. (2018). Employee perceptions of organization culture with respect to fraud – where to look and what to look for. *Pacific Accounting Review, 30*(2), 187-198. doi:10.1108/PAR-05-2017-0033; 16

10.1108/PAR-05-2017-0033

Kumar, K., & Haynes, J. D. (2003). Forecasting credit ratings Using ANN and statistical techniques.

Kusumasari, T. F. (2016). *Data profiling for data quality improvement with OpenRefine.* Paper presented at the 2016 International Conference on Information Technology Systems and Innovation (ICITSI).

LabCFTC. (2017). A CFTC Primer on Virtual Currencies. Retrieved from https://www.cftc.gov/sites/default/files/idc/groups/public/documents/file/labcftc_primercurrencies100417.pdf

Lagarde, C. (2017). Central Banking and Fintech—A Brave New World? In *Bank of England conference, London*. https://www.imf.org/en/News/Articles/2017/09/28/sp092917-central-banking-and-fintech-a-brave-new-world (accessed 25 February 2018): International Monetary Fund.

Lamprecht, C., & Guetterman, T., C. (2019). Mixed methods in accounting: a field based analysis. *Meditari Accountancy Research, 27*(6), 921-938. doi:10.1108/MEDAR-11-2018-0403

Lancaster, K., & Ritter, A. (2014a). Examining the construction and representation of drugs as a policy problem in Australia's National Drug Strategy documents 1985–2010. *International Journal of Drug Policy, 25*(1), 81-87. doi:https://doi.org/10.1016/j.drugpo.2013.07.002

Lancaster, K., & Ritter, A. (2014b). Making change happen: A case study of the successful establishment of a peer-administered naloxone program in one Australian jurisdiction. *International Journal of Drug Policy, 25*(5), 985-991. doi:https://doi.org/10.1016/j.drugpo.2014.02.003

Langton, L., & Piquero, N. L. (2007). Can general strain theory explain white-collar crime? A preliminary investigation of the relationship between strain and select white-collar offenses. *Journal of Criminal Justice, 35*(1), 1-15. doi:10.1016/j.jcrimjus.2006.11.011

Larsson, P. (2013). Evaluation of open source data cleaning tools: Open refine and data wrangler. *University of Washington.*

Lasslett, K. (2019). Breaking with the past? Conflicts of interest and transparency. In: The Corruption and Human Rights Initiative (CHRI).

Lavrač, N., Motoda, H., Fawcett, T., Holte, R., Langley, P., & Adriaans, P. (2004). Introduction: Lessons Learned from Data Mining Applications and Collaborative Problem Solving. *Machine Learning, 57*(1), 13-34. doi:10.1023/B:MACH.0000035516.74817.51

Lee, A., & Palstra, N. (2018). *The Companies We Keep: What The UK's Open Data Register Actually Tells Us About Company Ownership*. Retrieved from United Kingdom: https://www.globalwitness.org/en/press-releases/groundbreaking-analysis-owners-uk-companies-uncovers-serious-money-laundering-risks/

Lee, C. C., Li, K. K., & Zhang, R. (2015). Shell games: The long-term performance of Chinese reverse-merger firms. *Accounting Review, 90*(4), 1547-1589. doi:10.2308/accr-50960

Lee, N., & Bartle, J. (2019). Home grown cannabis to be legal in the ACT. Now what? Retrieved from https://theconversation.com/home-grown-cannabis-to-be-legal-in-the-act-now-what-124268

Lenton, S., Humeniuk, R., Heale, P., & Christie, P. (2000). Infringement versus conviction: The social impact of a minor cannabis offence in South Australia and Western Australia. *Drug and Alcohol Review, 19*(3), 257-264.

Leukfeldt, E. R. (2014). Cybercrime and social ties. *Trends in Organized Crime, 17*(4), 231-249. doi:10.1007/s12117-014-9229-5

Levi, M., Doig, A., Gundur, R., Wall, D., & Williams, M. (2016). *The implications of economic cybercrime for policing. City of London Corporation*. Retrieved from

Levi, M., Doig, A., Gundur, R., Wall, D., & Williams, M. (2017). Cyberfraud and the implications for effective risk-based responses: themes from UK research. *Crime, Law and Social Change, 67*(1), 77-96. doi:10.1007/s10611-016-9648-0

Levi, M., & Reuter, P. (2006). Money laundering. *Crime and Justice, 34*(1), 289-375.

Levi, M., & Reuter, P. (2009). Money Laundering. In M. Tonry (Ed.), *The Oxford Handbook of Crime and Public Policy* (pp. 356-380). Oxfords: Oxford University Press.

Lewis, J., Ossowski, S., Hicks, J., Errami, M., & Garner, H. R. (2006). Text similarity: an alternative way to search MEDLINE. *Bioinformatics, 22*(18), 2298-2304. doi:10.1093/bioinformatics/btl388

Liben-Nowell, D., & Kleinberg, J. (2007). The link-prediction problem for social networks. *Journal of the American Society for Information Science and Technology, 58*(7), 1019-1031. doi:10.1002/asi.20591

Lintzeris, N., Mills, L., Suraev, A., Bravo, M., Arkell, T., Arnold, J. C., & Melissa, J. (2020). Medical cannabis use in the Australian community following introduction of legal access: The 2018-2019 Online Cross-Sectional Cannabis as Medicine Survey (CAMS-18). *Harm Reduction Journal*.

Liss, C., & Sharman, J. C. (2015). Global corporate crime-fighters: Private transnational responses to piracy and money laundering. *Review of International Political Economy, 22*(4), 693-718. doi:10.1080/09692290.2014.936482

Little, B. B., Johnston Jr, W. L., Lovell, A. C., Rejesus, R. M., & Steed, S. A. (2002). Collusion in the U.S. crop insurance program: Applied data mining. In (pp. 594-598).

Liu, D., Nie, H., & Zhang, B. (2018). A novel method for identifying influential nodes in complex networks based on multiple attributes. *International Journal of Modern Physics B, 32*(28), 1850307. doi:10.1142/S0217979218503071

Liu, J., Bier, E., Wilson, A., Guerra-Gomez, J. A., Honda, T., Sricharan, K., . . . Davies, D. (2016). Graph analysis for detecting fraud, waste, and abuse in healthcare data. *AI Magazine, 37*(2), 33-46.

Livingston, M., Holmes, J., Oldham, M., Vashishtha, R., & Pennay, A. (2020). Trends in the sequence of first alcohol, cannabis and cigarette use in Australia, 2001–2016. *Drug and Alcohol Dependence, 207*, 107821. doi:https://doi.org/10.1016/j.drugalcdep.2019.107821

Loayza, N., Villa, E., & Misas, M. (2019). Illicit activity and money laundering from an economic growth perspective: A model and an application to Colombia. *Journal of Economic Behavior & Organization, 159*, 442-487. doi:https://doi.org/10.1016/j.jebo.2017.10.002

Lu, D. (2019). *Submission to the Treasury's review into Initial Coin Offerings (ICOs)*. Retrieved from https://treasury.gov.au/sites/default/files/2019-04/c2019-t353604-256_ventures.pdf

Lü, L., Chen, D., Ren, X.-L., Zhang, Q.-M., Zhang, Y.-C., & Zhou, T. (2016). Vital nodes identification in complex networks. *Physics reports, 650*(C), 1-63. doi:10.1016/j.physrep.2016.06.007

Luhmann, N., Baecker, D., & Gilgen, P. (2013). *Introduction to systems theory*: Polity Cambridge.

Luna, D. K., Palshikar, G. K., Apte, M., & Bhattacharya, A. (2018). *Finding shell company accounts using anomaly detection*. Paper presented at the Proceedings of the ACM India Joint International Conference on Data Science and Management of Data, Goa, India.

Lv, Z., Zhao, N., Xiong, F., & Chen, N. (2019). A novel measure of identifying influential nodes in complex networks. *Physica A: Statistical Mechanics and its Applications, 523*, 488-497. doi:https://doi.org/10.1016/j.physa.2019.01.136

Lyman, M. D. (2011). Drugs and Crime. In M. D. Lyman (Ed.), *Drugs in Society (Sixth Edition)* (pp. 197-230). Boston: Anderson Publishing, Ltd.

Malinick, T. E., Tindall, D. B., & Diani, M. (2013). Network centrality and social movement media coverage: A two-mode network analytic approach. *Social Networks, 35*(2), 148-158. doi:https://doi.org/10.1016/j.socnet.2011.10.005

Malm, A., & Bichler, G. (2013). Using friends for money: the positional importance of money-launderers in organized crime. *Trends in Organized Crime, 16*(4), 365-381. doi:10.1007/s12117-013-9205-5

Manning, M., Wong, G. T., & Jevtovic, N. (2020). Investigating the relationships between FATF recommendation compliance, regulatory affiliations and the Basel Anti-Money Laundering Index. *Security Journal*.

Mansfield-Devine, S. (2017). Beyond Bitcoin: using blockchain technology to provide assurance in the commercial world. *Computer Fraud & Security, 2017*(5), 14-18. doi:https://doi.org/10.1016/S1361-3723(17)30042-8

Marteache, N., Viollaz, J., & Petrossian, G. A. (2015). Factors influencing the choice of a safe haven for offloading illegally caught fish: a comparative analysis of developed and developing economies. *Crime Science, 4*(1), 1-13. doi:http://dx.doi.org/10.1186/s40163-015-0045-2

Martin, J. (2014). Lost on the Silk Road: Online drug distribution and the 'cryptomarket'. *Criminology & Criminal Justice, 14*(3), 351-367. doi:10.1177/1748895813505234

Martini, M., Constantino, F., & France, G. (2019). *Who is behind the wheel? Fixing the global standards on company ownership*. Retrieved from

MAS. (2017a). Consumer Advisory on Investment Schemes Involving Digital Tokens (Including Virtual Currencies). Retrieved from http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/Consumer-Advisory-on-Investment-Schemes-Involving-Digital-Tokens.aspx

MAS. (2017b). A Guide to Digital Token Offerings. Retrieved from https://www.iosco.org/library/ico-statements/Singapore%20-%20MAS%20-%20A%20Guide%20to%20Digital%20Token%20Offerings.pdf

MAS. (2018). *Monetary Authority Of Singapore: A Guide to Digital Token Offerings*. Retrieved from http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulations%20Guidance%20and%20Licensing/Securities%20Futures%20and%20Fund%20Management/Regulations%20Guidance%20and%20Licensing/Guidelines/A%20Guide%20to%20Digital%20Token%20Offerings%20last%20updated%20on%2030%20Nov%202018.pdf

Masciandaro, D. (1998). Money Laundering Regulation: The Micro Economics. *Journal of Money Laundering Control, 2*(1), 49-58. doi:10.1108/eb027170

Masciandaro, D. (2008). Offshore financial centres: the political economy of regulation. *European Journal of Law and Economics, 26*(3), 307-340. doi:10.1007/s10657-008-9075-5

Masciandaro, D., & Portolano, A. (2003). It takes two to tango: international financial regulation and offshore centres. *Journal of Money Laundering Control, 6*(4), 311-330. doi:10.1108/13685200310809635

Maturana, H. R., & Varela, F. J. (1987). *The tree of knowledge: The biological roots of human understanding*: New Science Library/Shambhala Publications.

Mayer, T., & Zignago, S. (2011). Notes on CEPII's distances measures: The GeoDist database.

McCarthy, K. J., van Santen, P., & Fiedler, I. (2015). Modeling the money launderer: Microtheoretical arguments on anti-money laundering policy. *International Review of Law & Economics, 43*, 148-155. doi:10.1016/j.irle.2014.04.006

McGinty, E. E., Niederdeppe, J., Heley, K., & Barry, C. L. (2017). Public perceptions of arguments supporting and opposing recreational marijuana legalization. *Preventive Medicine, 99*, 80-86. doi:https://doi.org/10.1016/j.ypmed.2017.01.024

McGinty, E. E., Samples, H., Bandara, S. N., Saloner, B., Bachhuber, M. A., & Barry, C. L. (2016). The emerging public discourse on state legalization of marijuana for recreational use in the US: Analysis of news media coverage, 2010–2014. *Preventive Medicine, 90*, 114-120. doi:https://doi.org/10.1016/j.ypmed.2016.06.040

Medina, L., & Schneider, F. (2018). *Shadow Economies Around the World*. International Monetary Fund. Washington, D. C.

Meloen, J., Landman, R., De Miranda, H., Van Eekelen, J., Van Soest, S., Van Duyne, P., & Van Tilburg, W. (2003). Buit en besteding: Een empirisch onderzoek naar de omvang, de kenmerken en de besteding van misdaadgeld. *Den Haag: Reed Business Information, 186*, 380-396.

Memon, B. R., & Wiil, U. K. (2014). Predicting links in multi-relational networks. In (pp. 107-114): Institute of Electrical and Electronics Engineers Inc.

Miller, J. J. (2013). *Graph database applications and concepts with Neo4j*. Paper presented at the Proceedings of the Southern Association for Information Systems Conference, Atlanta, GA, USA.

Mitchell, A., Sikka, P., & Willmott, H. (1998a). *The Accountants' Laundromat*: Basildon: Association for Accountancy & Business Affairs.

Mitchell, A., Sikka, P., & Willmott, H. (1998b). Sweeping it under the carpet: The role of accountancy firms in moneylaundering. *Accounting, Organizations and Society, 23*(5), 589-607. doi:10.1016/S0361-3682(98)00010-5

Mollick, E., & Nanda, R. (2015). Wisdom or madness? Comparing crowds with expert evaluation in funding the arts. *Management Science, 62*(6), 1533-1553.

Mondaq. (2019). ICOs and ICO Regulations in Malta. Retrieved from http://www.mondaq.com/x/800132/fin+tech/ICOs+And+ICO+Regulations+In+Malta

Mondragon, R. J., Iacovacci, J., & Bianconi, G. (2018). Multilink communities of multiplex networks. *PloS one, 13*(3), e0193821.

Monge, A., & Elkan, C. (1997). An efficient domain-independent algorithm for detecting approximately duplicate database records.

Moore, D. A. (2017). How to Improve the Accuracy and Reduce the Cost of Personnel Selection. *California Management Review, 60*(1), 8-17. doi:10.1177/0008125617725288

Morselli, C., & Roy, J. (2008). BROKERAGE QUALIFICATIONS IN RINGING OPERATIONS*. *Criminology, 46*(1), 71-98. doi:10.1111/j.1745-9125.2008.00103.x

Mumford, E. (1998). Problems, knowledge, solutions: solving complex problems. *Journal of Strategic Information Systems, 7*(4), 255-269. doi:10.1016/S0963-8687(99)00003-7

Murphy, P. R., & Free, C. (2016). Broadening the Fraud Triangle: Instrumental Climate and Fraud. *Behavioral Research in Accounting, 28*(1), 41-56. doi:10.2308/bria-51083; 07

10.2308/bria-51083

Murray, D. (2018). Protecting Our Elections: Examining Shell Companies and Virtual Currencies as Avenues for Foreign Interference. In. USA: Financial Integrity Network.

Murray, K. (2016). In the shadow of the dark twin – proving criminality in money laundering cases. *Journal of Money Laundering Control, 19*(4), 447-458. doi:http://dx.doi.org/10.1108/JMLC-02-2016-0009

Murray, K. (2018). The cost of not wanting to know – the professions, money laundering and organised crime. *Journal of Financial Crime, 25*(1), 218-229. doi:10.1108/JFC-11-2016-0071

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf

Nakamura, Y., & Kim, S. (2017). Cryptocurrencies Drop as South Korea Bans ICOs, Margin Trading. Retrieved from https://www.bloomberg.com/news/articles/2017-09-29/cryptocurrencies-drop-as-south-korea-bans-icos-margin-trading

Ndofor, H., Wesley, C., & Priem, R. (2015). Providing CEOs With Opportunities to Cheat: The Effects of Complexity-Based Information Asymmetries on Financial Reporting Fraud. *Journal Of Management, 41*(6), 1774-1797. doi:10.1177/0149206312471395

Needham, M., & Hodler, A. (2019). *Graph Algorithms: Practical Examples in Apache Spark & Neo4J* (1 ed.): O'Reilly Media, Inc.

Neu, D., Everett, J., Rahaman, A. S., & Martinez, D. (2013). Accounting and networks of corruption. *Accounting, Organizations and Society, 38*(6-7), 505-524. doi:10.1016/j.aos.2012.01.003

Newman, L. (2007). Making the Most of Anti-money Laundering Systems. *The Journal of Superannuation Management, 1*(2), 31-34.

Newman, M., & Girvan, M. (2004). Finding and evaluating community structure in networks. *Physical Review E, 69*(2). doi:10.1103/PhysRevE.69.026113

Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems, 50*(3), 559-569. doi:https://doi.org/10.1016/j.dss.2010.08.006

Niels, J., & Gabriel, Z. (2014). The End of Bank Secrecy? An Evaluation of the G20 Tax Haven Crackdown. *American Economic Journal: Economic Policy, 6*(1), 65-91. doi:10.1257/pol.6.1.65

Norton, S. D. (2018). Suspicion of money laundering reporting obligations: Auditor compliance, or sceptical failure to engage? *Critical Perspectives on Accounting, 50*, 56-66. doi:10.1016/j.cpa.2017.09.003

Nougayrède, D. (2019). After the Panama Papers: A Private Law Critique of Shell Companies. *The International Lawyer, 51*(3).

Obermayer, B., Ryle, G., Guevara, M. W., Hudson, M., Bernstein, J., Fitzgibbon, W., . . . Chittum, R. (2016). Giant leak of offshore financial records exposes global array of crime and corruption. *OCCRP. The International Consortium of Investigative Journalists*.

OCCRP. (2017). The Azerbaijani Laundromat. Retrieved from https://www.occrp.org/en/azerbaijanilaundromat/

OCCRP. (2019). The Troika Laundromat. Retrieved from https://www.occrp.org/en/troikalaundromat/

OECD, & JRC. (2008). *Handbook on constructing composite indicators: methodology and user guide*: Joint Research Centre of the European Commission.
OpenCorporates. (2019a). OpenRefine Reconciliation API. Retrieved from https://api.opencorporates.com/documentation/Open-Refine-Reconciliation-API
OpenCorporates. (2019b). The White Box Data Revolution. In: OpenCorporates.
Pacini, C. J., Sinclair, D. T., & Hopwood, W. S. (2016). Domestic Asset Tracing: Identifying, Locating and Freezing Stolen and Hidden Assets. *Journal of Forensic Accounting Research, 1*(1), A42-A65.
Paoli, L. (2014). Types of Organized Crime. In G. Bruinsma & D. Weisburd (Eds.), *Encyclopedia of Criminology and Criminal Justice* (pp. 3376-3387). New York, NY: Springer New York.
Pardo, B. (2014). Cannabis policy reforms in the Americas: A comparative analysis of Colorado, Washington, and Uruguay. *International Journal of Drug Policy, 25*(4), 727-735. doi:https://doi.org/10.1016/j.drugpo.2014.05.010
Paternoster, R., & Mazerolle, P. (1994). General Strain Theory and Delinquency: A Replication and Extension. *Journal of Research in Crime and Delinquency, 31*(3), 235-263. doi:10.1177/0022427894031003001
Pellegrina, L. D., & Masciandaro, D. (2009). The risk-based approach in the New European anti-money laundering legislation: A law and economics view. *Review of Law and Economics, 5*(2), 931-952. doi:10.2202/1555-5879.1422
Perols, J. (2011a). Financial Statement Fraud Detection: An Analysis of Statistical and Machine Learning Algorithms. *AUDITING: A Journal of Practice & Theory, 30*(2), 19-50. doi:10.2308/ajpt-50009
Perols, J. (2011b). Financial statement fraud detection: An analysis of statistical and machine learning algorithms. *Auditing, 30*(2), 19-50. doi:10.2308/ajpt-50009
Perryer, S. (2019). Troika Laundromat: inside Europe's latest money laundering scandal. Retrieved from https://www.europeanceo.com/finance/troika-laundromat-inside-europes-latest-money-laundering-scandal/
Peslak, A. R. (2005). A twelve-step, multiple course approach to teaching enterprise resource planning. *Journal of Information Systems Education, 16*(2), 147.
Philippson, S. (2001). Money laundering on the internet. *Computers & security, 20*(6), 485-485.
Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A Comprehensive Survey of Data Mining-based Fraud Detection Research. *arXiv preprint arXiv:1009.6119*. Retrieved from https://arxiv.org/ftp/arxiv/papers/1009/1009.6119.pdf doi:10.1016/j.chb.2012.01.002
Picard, P. M., & Pieretti, P. (2011). Bank secrecy, illicit money and offshore financial centers. *Journal of Public Economics, 95*(7), 942-955. doi://doi.org/10.1016/j.jpubeco.2011.01.004
Piquero, A. R., Gibson, C. L., & Tibbetts, S. G. (2002). Does self-control account for the relationship between binge drinking and alcohol-related behaviours? *Criminal Behaviour and Mental Health, 12*(2), 135-154. doi:10.1002/cbm.492
Pivo, G., Henry, A. D., & Berger, L. (2020). Essential elements at play in local environmental policy change: A guide for the perplexed. *Environmental Science & Policy, 106*, 240-249. doi:https://doi.org/10.1016/j.envsci.2020.01.023
Pol, R. (2018a). Anti-money laundering effectiveness: assessing outcomes or ticking boxes? *Journal of Money Laundering Control, 21*(2), 215-230. doi:10.1108/JMLC-07-2017-0029
Pol, R. (2018b). Uncomfortable truths? ML=BS and AML= BS2. *Journal of Financial Crime, 25*(2), 294-308. doi:10.1108/JFC-08-2017-0071

Poulsen, A. B., & Stegemoller, M. (2008). Moving from Private to Public Ownership: Selling Out to Public Firms versus Initial Public Offerings. *Financial Management, 37*(1), 81-101. doi:10.1111/j.1755-053X.2008.00005.x

Quirk, P. (1997). Macroeconomic implications of money laundering. *Trends in Organized Crime, 2*(3), 10-14. doi:10.1007/BF02901593

Raghavan, U. N., Albert, R., & Kumara, S. (2007). Near linear time algorithm to detect community structures in large-scale networks. *Physical Review E, 76*(3). doi:10.1103/PhysRevE.76.036106

Ravenda, D., Argilés-Bosch, J. M., & Valencia-Silva, M. M. (2015). Detection Model of Legally Registered Mafia Firms in Italy. *European Management Review, 12*(1), 23-39. doi:10.1111/emre.12039; 08

10.1111/emre.12039

Ravenda, D., Valencia-Silva, M. M., Argiles-Bosch, J. M., & García-Blandón, J. (2018). Money laundering through the strategic management of accounting transactions. *Critical Perspectives on Accounting*. doi://doi.org/10.1016/j.cpa.2018.08.003

Ravenda, D., Valencia, M. M., Josep, M. A., & Josep, G. B. (2017). Accrual management as an indication of money laundering through legally registered Mafia firms in Italy. *Accounting, Auditing & Accountability Journal, 31*(1), 286-317. doi:10.1108/AAAJ-12-2015-2329; 23

10.1108/AAAJ-12-2015-2329

Ray, A. (2015). *Emerging Solutions in Anti-Money Laundering Technology*. Retrieved from http://celent.com/reports/emerging-solutions-anti-money-laundering-technology

Raychaudhuri, A., Mallick, S., Sircar, A., & Singh, S. (2020, 2020//). *Identifying Influential Nodes Based on Network Topology: A Comparative Study*. Paper presented at the Information, Photonics and Communication, Singapore.

Regan, S., Adams, H., Guiral, P., & Chouri, S. (2017). Evolving AML Journey - Leveraging Machine Learning Within Anti-Money Laundering Transaction Monitoring. In: Accenture Consulting.

Reuter, P., & Greenfield, V. (2001). Measuring global drug markets. *World economics, 2*(4), 159-173.

Reuter, P., & Truman, E. (2004). *Chasing Dirty Money: The Fight Against Anti-Money Laundering*. Washington DC: Peterson Institute for International Economics.

Riccardi, M., Milani, R., & Camerini, D. (2018). Assessing Money Laundering Risk across Regions. An Application in Italy. *European Journal on Criminal Policy and Research, 25*(1), 21-43. doi:10.1007/s10610-018-9399-9

Richet, J. L. (2013). *Laundering Money Online: a review of cybercriminals methods*. Retrieved from https://arxiv.org/ftp/arxiv/papers/1310/1310.2368.pdf

Ritter, A., Lancaster, K., Grech, K., & Reuter, P. (2011). *An assessment of illicit drug policy in Australia (1985 to 2010): Themes and trends*: National Drug and Alcohol Research Centre.

Ritter, A., & Lee, N. (2016). Australia's recreational drug policies aren't working, so what are the options for reform? Retrieved from http://theconversation.com/australias-recreational-drug-policies-arent-working-so-what-are-the-options-for-reform-55493

Ritter, A., & Sotade, O. (2017). Explaining the declining rates of past year cannabis use in Australia: A first pass. *Drug and Alcohol Review, 36*(5), 602-608. doi:10.1111/dar.12553

Rodriguez, M. A., & Shinavier, J. (2010). Exposing multi-relational networks to single-relational network analysis algorithms. *Journal of Informetrics, 4*(1), 29-41. doi:https://doi.org/10.1016/j.joi.2009.06.004

Rogeberg, O. (2018). Prohibition, regulation or laissez faire: The policy trade-offs of cannabis policy. *International Journal of Drug Policy, 56*, 153-161. doi:https://doi.org/10.1016/j.drugpo.2018.03.024

Rokach, L., & Maimon, O. (2015). Introduction to Decision Trees. In *Data Mining with Decision Trees: Theory and Applications* (2nd ed., pp. 1-16). Singapore: World Scientific Publishing.

Romera, P., & Gallego, C. S. (2018). How ICIJ deals with massive data leaks like the Panama Papers and Paradise Papers. Retrieved from https://www.icij.org/blog/2018/07/how-icij-deals-with-massive-data-leaks-like-the-panama-papers-and-paradise-papers/

Rose, A. K., & Spiegel, M. M. (2007). Offshore Financial Centres: Parasites or Symbionts? *Economic Journal, 117*(523), 1310-1335. doi:10.1111/j.1468-0297.2007.02084.x

Rose, J., Skiftenes Flak, L., & Sæbø, Ø. (2018). Stakeholder theory for the E-government context: Framing a value-oriented normative core. *Government Information Quarterly, 35*(3), 362-374. doi:10.1016/j.giq.2018.06.005

Rosenfeld, R., Jacobs, B. A., & Wright, R. (2003). Snitching and the code of the street. *British Journal of Criminology, 43*(2), 291-309.

Rothstein, H., Huber, M., & Gaskell, G. (2006). A theory of risk colonization: The spiralling regulatory logics of societal and institutional risk. *Economy and Society, 35*(1), 91-112. doi:10.1080/03085140500465865

Ruhnau, B. (2000). Eigenvector-centrality — a node-centrality? *Social Networks, 22*(4), 357-365. doi:https://doi.org/10.1016/S0378-8733(00)00031-9

Rusanov, G., & Pudovochkin, Y. (2018). Money laundering and predicate offenses: models of criminological and legal relationships. *Journal of Money Laundering Control, 21*(1), 22-32. doi:10.1108/JMLC-12-2016-0048; 23

10.1108/JMLC-12-2016-0048

Sabatier, P. A., & Weible, C. M. (2014). *Theories of the Policy Process* (3rd ed. ed.). Boulder: Westview Press.

Sahin, Y., Bulkan, S., & Duman, E. (2013). A cost-sensitive decision tree approach for fraud detection. *Expert Systems with Applications, 40*(15), 5916-5923. doi://doi.org/10.1016/j.eswa.2013.05.021

Salavati, C., Abdollahpouri, A., & Manbari, Z. (2019). Ranking nodes in complex networks based on local structure and improving closeness centrality. *Neurocomputing, 336*, 36-45. doi:https://doi.org/10.1016/j.neucom.2018.04.086

Samantha Maitland Irwin, A., Raymond Choo, K.-K., & Liu, L. (2012). Modelling of money laundering and terrorism financing typologies. *Journal of Money Laundering Control, 15*(3), 316-335. doi:10.1108/13685201211238061

Sathya, R., & Abraham, A. (2013). Comparison of Supervised and Unsupervised Learning Algorithms for Pattern Classification. *International Journal of Advanced Research in Artificial Intelligence, 2*(2), 34-38.

Savage, D. (2017). *Detection of Illicit Behaviours and Mining for Contrast Patterns.* (Dissertation/Thesis), RMIT University,

Savage, D., Wang, Q., Chou, P., Zhang, X., & Yu, X. (2016). Detection of money laundering groups using supervised learning in networks.

Schechter, H. (2004). *The serial killer files: The who, what, where, how, and why of the world's most terrifying murderers*: Random House Digital, Inc.

Scheufele, D. A., & Tewksbury, D. (2007). Framing, Agenda Setting, and Priming: The Evolution of Three Media Effects Models. *Journal of Communication, 57*(1), 9-20. doi:10.1111/j.0021-9916.2007.00326.x

Schneider, F. (2010). Turnover of organized crime and money laundering: some preliminary empirical findings. *Public Choice, 144*(3), 473-486. doi:10.1007/s11127-010-9676-8
Schneider, F. (2017a). The Dark Side: Crime Has Gone Global. *A Closer Look at Globalization–The Positive Facets and the Dark Faces of a Complex Notion, Gütersloh*.
Schneider, F. (2017b). *Restricting or Abolishing Cash: An Effective Instrument for Fighting the Shadow Economy, Crime and Terrorism?* Paper presented at the International Cash Conference 2017–War on Cash: Is there a Future for Cash?
Schneider, F., & Enste, D. H. (2000a). *Shadow Economies Around the World-Size, Causes, and Consequences*. Retrieved from imf.org/external/pubs/ft/wp/2000/wp0026.pdf
Schneider, F., & Enste, D. H. (2000b). Shadow Economies: Size, Causes, and Consequences. *Journal of Economic Literature, 38*(1), 77-114. doi:10.1257/jel.38.1.77
Schneider, F., & Linsbauer, K. (2016). *The Financial Flows of Transnational Crime and Tax Fraud: How much cash is used and what do we (not) know?* Paper presented at the Cash on Trial.
Schneider, F., & Windischbauer, U. (2008). Money laundering: some facts. *European Journal of Law and Economics, 26*(3), 387-404. doi:10.1007/s10657-008-9070-x
Scholl, H. J. (2001). Applying stakeholder theory to e-government: Benefits and limits. In (Vol. 74, pp. 735-747): Springer New York LLC.
Scholl, H. J. (2004). Involving Salient Stakeholders: Beyond the Technocratic View on Change. *Action Research, 2*(3), 277-304. doi:10.1177/1476750304045940
Scholl, H. J., & Bolívar, M. P. R. (2019). Regulation as both enabler of technology use and global competitive tool: The Gibraltar case. *Government Information Quarterly, 36*(3), 601-613. doi:https://doi.org/10.1016/j.giq.2019.05.003
Schott, P. A. (2006). *Reference guide to anti-money laundering and combating the financing of terrorism*: The World Bank.
Schwarz, P. (2011). Money launderers and tax havens: Two sides of the same coin? *International Review of Law & Economics, 31*(1), 37-47. doi:10.1016/j.irle.2010.12.001
Schweitzer, F., Fagiolo, G., Sornette, D., Vega-Redondo, F., Vespignani, A., & White, D. R. (2009). Economic networks: the new challenges. *Science (New York, N.Y.), 325*(5939), 422. doi:10.1126/science.1173644
Schweizer, A., Schlatt, V., Urbach, N., & Fridgen, G. (2017). Unchaining Social Businesses–Blockchain as the Basic Technology of a Crowdlending Platform.
Schwienbacher, A., & Larralde, B. (2010). Crowdfunding of small entrepreneurial ventures.
SEC. (2017a). Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO. Retrieved from https://www.sec.gov/litigation/investreport/34-81207.pdf
SEC. (2017b). SEC V. PLEXCORPS (a/k/a and d/b/a PLEXCOIN and SIDEPAY.CA), DOMINIC LACROIX and SABRINA PARADIS-ROYER. Retrieved from https://www.sec.gov/litigation/complaints/2017/comp-pr2017-219.pdf
SEC. (2017c). SEC V. RECOIN GROUP FOUNDATION, LLC, DRC : COMPLAINT WORLD INC. a/k/a DIAMOND RESERVE CLUB,: and MAKSIM ZASLAVSKIY. Retrieved from https://www.sec.gov/litigation/complaints/2017/comp-pr2017-185.pdf
SEC. (2018). SEC V. ARISEBANK, JARED RICE SR., and STANLEY FORD. Retrieved from https://www.sec.gov/litigation/complaints/2018/comp-pr2018-8.pdf
SEC. (2019). SEC Staff to Hold Fintech Forum to Discuss Distributed Ledger Technology and Digital Assets [Press release]. Retrieved from https://www.sec.gov/news/press-release/2019-35

Sedgwick, K. (2018). Benebit ICO Does a Runner with $2.7 Million of Investor Funds. Retrieved from https://news.bitcoin.com/benebit-ico-runner-2-7-million-investor-funds/

Seifoddini, H., & Hsu, C.-P. (1994). Comparative study of similarity coefficients and clustering algorithms in cellular manufacturing. *Journal of Manufacturing Systems, 13*(2), 119-127. doi:https://doi.org/10.1016/0278-6125(94)90027-2

Semenenko, I. (2011). Reverse merger waves, market timing and managerial behavior. *International Research Journal of Applied Finance, 2*(12), 1453-1481.

SFC. (2018). SFC warns of cryptocurrency risks. Retrieved from https://www.sfc.hk/edistributionWeb/gateway/EN/news-and-announcements/news/doc?refNo=18PR13

Shanahan, M., Gerard, K., & Ritter, A. (2014). Preferences for policy options for cannabis in an Australian general population: A discrete choice experiment. *International Journal of Drug Policy, 25*(4), 682-690. doi:https://doi.org/10.1016/j.drugpo.2014.03.005

Shao, B., Wang, H., & Xiao, Y. (2012). *Managing and mining large graphs: systems and implementations*. Paper presented at the Proceedings of the 2012 ACM SIGMOD International Conference on Management of Data, Scottsdale, Arizona, USA.

Sharma, A., & Panigrahi, P. K. (2012). A Review of Financial Accounting Fraud Detection based on Data Mining Techniques. *International Journal of Computer Applications, 39*(1), 37-47.

Sharman, J. (2012). *Tackling shell companies: Limiting the opportunities to hide proceeds of corruption*. Retrieved from https://www.cmi.no/publications/4664-tackling-shell-companies

Sharman, J. (2013). *Preventing the misuse of shell companies by regulating corporate service providers*. Retrieved from https://www.u4.no/publications/preventing-the-misuse-of-shell-companies-by-regulating-corporate-service-providers.pdf

Shin, L. (2017). $15 Million ICO Halted By SEC For Being Alleged Scam. Retrieved from https://www.forbes.com/sites/laurashin/2017/12/04/15-million-ico-halted-by-sec-for-being-alleged-scam/#63e741d51569

Shome, A. (2018). Benebit ICO Scammed Investors for At Least $2.7 Million. Retrieved from https://www.financemagnates.com/cryptocurrency/news/benebit-ico-scammed-investors-least-2-7-million/

Sikka, P., & Willmott, H. (2010). The dark side of transfer pricing: Its role in tax avoidance and wealth retentiveness. *Critical Perspectives on Accounting, 21*(4), 342-356. doi://doi.org/10.1016/j.cpa.2010.02.004

Siklos-Whillans, J., Bacchus, A., & Manwell, L. A. (2020). A Scoping Review of the Use of Cannabis and Its Extracts as Potential Harm Reduction Strategies: Insights from Preclinical and Clinical Research. *International Journal of Mental Health and Addiction*. doi:10.1007/s11469-020-00244-w

Singh, D. (2010). Incorporating with fraudulent intentions: A Study of Various Differentiating Attributes of Shell Companies in India. *Journal of Financial Crime, 17*(4), 459-484. doi:10.1108/13590791011082805

Singh, K., & Best, P. (2016). Interactive visual analysis of anomalous accounts payable transactions in SAP enterprise systems. *Managerial Auditing Journal, 31*(1), 35-63. doi:10.1108/MAJ-10-2014-1117

Singh, K., & Best, P. (2019). Anti-Money Laundering: Using data visualization to identify suspicious activity. *International Journal of Accounting Information Systems*. doi:https://doi.org/10.1016/j.accinf.2019.06.001

Sjostrom, W. K. (2008). The truth about reverse mergers. *Entrepreneurial Business Law Journal, 2*(2), 743-759.

Smekens, M., & Verbruggen, M. (2004). De illegale Economie in Nederland. *Centraal Bureau voor de Statistiek, 20*.
Song, X., Hu, Z., Du, J., & Sheng, Z. (2014). Application of Machine Learning Methods to Risk Assessment of Financial Statement Fraud: Evidence from China. *Journal of Forecasting, 33*(8), 611-626.
Sood, A., Bonsal, R., & Enbody, R. (2013). Cybercrime: Dissecting the State of Underground Enterprise. *Ieee Internet Computing, 17*(1), 60-68. doi:10.1109/MIC.2012.61
Soudijn, M. (2012). Removing excuses in money laundering. *Trends in Organized Crime, 15*(2), 146-163. doi:10.1007/s12117-012-9161-5
Soudijn, M., & Been, W. (2020). *Law enforcement and money laundering: Big data is coming*.
Soudijn, M. R. J. (2019). Using Police Reports to Monitor Money Laundering Developments. Continuity and Change in 12 Years of Dutch Money Laundering Crime Pattern Analyses. *European Journal on Criminal Policy and Research, 25*(1), 83-97. doi:10.1007/s10610-018-9379-0
Sparrow, M. K. (1991). The application of network analysis to criminal intelligence: An assessment of the prospects. *Social Networks, 13*(3), 251-274.
Speer, D. L. (2000). Redefining borders: The challenges of cybercrime. *Crime, Law and Social Change, 34*(3), 259-273. doi:10.1023/A:1008332132218
Srinivas, S., & Rajendran, C. (2019). Community detection and influential node identification in complex networks using mathematical programming. *Expert Systems with Applications, 135*, 296-312. doi:https://doi.org/10.1016/j.eswa.2019.05.059
Stack, G. (2015a). Baltic shells: on the mechanics of trade-based money-laundering in the former Soviet space. *Journal of Money Laundering Control, 18*(1), 81-98. doi:10.1108/JMLC-10-2013-0040
Stack, G. (2015b). Money laundering in Ukraine. *Journal of Money Laundering Control, 18*(3), 382-394.
Stack, G. (2015c). Shell companies, Latvian-type correspondent banking, money laundering and illicit financial flows from Russia and the former Soviet Union. *Journal of Money Laundering Control, 18*(4), 496-512. doi:10.1108/JMLC-06-2014-0020
Steinberg, D. CART vs. The Clones. Retrieved from https://www.salford-systems.com/blog/dan-steinberg/item/9-cart%C2%AE-vs-the-clones
Stevens, E., & Churchman, C. W. (1975). The Design of Inquiring Systems: Basic Concepts of Systems and Organization. In (Vol. 12): American Educational Research Association.
Stewart, G., & Rosemann, M. (2001). Industry-oriented design of ERP-related curriculum - an Australian initiative. *Business Process Management Journal, 7*(3), 234-242. doi:10.1108/14637150110392719
Stuhlmiller, L. (2013). *Mitigating virtual money laundering: An analysis of virtual worlds and virtual currencies.* (M.S.), Utica College, United States -- New York. Retrieved from https://search.proquest.com/docview/1449374093?accountid=26503
Sudjianto, A., Yuan, M., Kern, D., Nair, S., Zhang, A., & Cela-Diaz, F. (2010). Statistical methods for fighting financial crimes. *Technometrics, 52*, 5-19.
Sullivan, C., & Burger, E. (2017). E-residency and blockchain. *Computer Law & Security Review, 33*(4), 470-481. doi:https://doi.org/10.1016/j.clsr.2017.03.016
Sutton, C. D. (2005). Classification and Regression Trees, Bagging, and Boosting. In E. J. W. C.R. Rao & J. L. Solka (Eds.), *Handbook of statistics* (Vol. Volume 24, pp. 303-329): Elsevier.
Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review, 22*(6), 664-670.

Tanzi, V. (1996). *Money Laundering and the International Financial System*. IMF Working Papers. International Monetary Fund.
Tapscott, D., & Tapscott, A. (2017). How Blockchain Will Change Organizations. *MIT Sloan Management Review, 58*(2), 10.
Tashiro, M. (2019). [Japan's Crypto Association issues ICO regulation recommendations Brave New Coin]. Web Page.
Teichmann, F. (2020). Recent trends in money laundering. *Crime, Law and Social Change, 73*(2), 237-247. doi:10.1007/s10611-019-09859-0
Tew, J. A., & Freedman, D. (1973). In Support of SEC v. W.J. Howey Co.: A Critical Analysis of the Parameters of the Economic Relationship Between an Issuer of Securities and the Securities Purchaser. *University of Miami Law Review, 27*, 407-450.
The Lancet. (2016). Reforming international drug policy. *The Lancet, 387*(10026), 1347. doi:https://doi.org/10.1016/S0140-6736(16)30115-5
The World Bank. (2020). World Bank Open Data. Retrieved from https://data.worldbank.org/
Theocharidis, A., Dongen, S. V., Enright, A. J., & Freeman, T. C. (2009). Network visualization and analysis of gene expression data using BioLayout Express3D. *Nature Protocols, 4*(10), 1535. doi:10.1038/nprot.2009.177
Thomas, J. J., & Cook, K. A. (2006). A Visual Analytics Agenda. *IEEE Computer Graphics and Applications, 26(1):10-13, 26*(1). doi:10.1109/MCG.2006.5
Thoumi, F. E. (2005). The numbers game: let's all guess the size of the illegal drug industry! *Journal of Drug Issues, 35*(1), 185-200.
TimeBase. (2019). ACT Passes Legislation for Personal Cannabis Use and New Cannabis Offences. Retrieved from http://www.timebase.com.au/news/2018/AT04949-article.html
Tiwari, M., Gepp, A., & Kumar, K. (2019). The future of raising finance - a new opportunity to commit fraud: a review of initial coin offering (ICOs) scams. *Crime, Law and Social Change*. doi:10.1007/s10611-019-09873-2
Tiwari, M., Gepp, A., & Kumar, K. (2020). A review of money laundering literature: the state of research in key areas. *Pacific Accounting Review, 32*(2), 271-303. doi:10.1108/PAR-06-2019-0065
Top ICO List. (2018). Benebit ICO. Retrieved from https://topicolist.com/ico/benebit
Townsend, B., Strazdins, L., Harris, P., Baum, F., & Friel, S. (2020). Bringing in critical frameworks to investigate agenda-setting for the social determinants of health: Lessons from a multiple framework analysis. *Social Science & Medicine, 250*, 112886. doi:https://doi.org/10.1016/j.socscimed.2020.112886
Tracy, S., Stewart, G., Boykin, R., Najm, M., Rosemann, M., & Carpinetti, L. (2001). SAP student marketplace for the advancement of research and teaching (SAP Smart). *AMCIS 2001 Proceedings*, 195.
Turner, A., & Irwin, A. S. M. (2018). Bitcoin transactions: a digital discovery of illicit activity on the blockchain. *Journal of Financial Crime, 25*(1), 109-130. doi:doi:10.1108/JFC-12-2016-0078
Twizeyimana, J. D., & Andersson, A. (2019). The public value of E-Government: A literature review. In (Vol. 36, pp. 167-178): Elsevier.
Underhill, J. (2018). Initial coin offerings: Fraudsters use new technology to perpetrate old schemes. Retrieved from https://www.fraud-magazine.com/article.aspx?id=4295000887&Site=ACFEWEB
Unger, B. (2007). *The scale and impacts of money laundering*. Cheltenham, UK ;: Edward Elgar.
Unger, B. (2013). Can Money Laundering Decrease? *Public Finance Review, 41*(5), 658-676. doi:10.1177/1091142113483353

Unger, B., Ferwerda, J., Nelen, H., & Ritzen, L. (2011). *Money laundering in the real estate sector: Suspicious properties*. Cheltenham: Edward Elgar.
Unger, B., Ferwerda, J., Van Der Broek, M., & Deleanu, I. (2014). *The economic and legal effectiveness of the european union's anti-money laundering policy*. Cheltenham, England; Northampton, Massachusetts: Edward Elgar.
Unger, B., & Hertog, J. (2012). Water always finds its way: Identifying new forms of money laundering. *Crime, Law and Social Change, 57*(3), 287-304. doi:10.1007/s10611-011-9352-z
Unger, B., Siegel, M., Ferwerda, J., de Kruijf, W., Busuioic, M., Wokke, K., & Rawlings, G. (2006). The amounts and the effects of money laundering. *Report for the Ministry of Finance, 16*.
UNODC. (2004). *United Nations Convention Against Transnational Organized Crime and the Protocols Thereto*. Retrieved from Vienna:
UNODC. (2011). *Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes*. Retrieved from Vienna, Austria: https://www.unodc.org/unodc/en/data-and-analysis/WDR-2011.html
UNODC. (2015). *World Drug Report 2015*. Retrieved from Vienna: https://www.unodc.org/wdr2015/
UNODC. (2016). Outcome document of the 2016 United Nations General Assembly special session on the world drug problem. In: United Nations Office on Drugs and Crime New York, NY.
UNODC. (2019). *World Drug Report 2019*. Retrieved from Vienna: https://wdr.unodc.org/wdr2019/
UNODC. (2020). *DATA UNODC*. Retrieved from: https://dataunodc.un.org/data/drugs/Retail%20drug%20price%20and%20purity%20level
Vail, N. (2018). Cracking Shells: The Panama Papers and Looking to the European Union's Anti-Money Laundering Directive as a Framework for Implementing Multilateral Agreement to Combat the Harmful Effects of Shell Companies. *Texas A&M Law Review, 5*(1), 133-153.
Van Akkeren, J., Buckby, S., & Tarr, J.-A. (2016). Forensic accounting: Professional regulation of a multi-disciplinary field. *Australian Business Law Review, 44*, 204-2015.
Van Bruggen, R. (2014). *Learning Neo4j*: Packt Publishing Ltd.
Van Duyne, P. (2003). Money Laundering Policy: Fears and Facts. In *Criminal Finances and Organizing Crime in Europe* (pp. 72-109). Nijmegen: Wolf Legal Publishers.
Van Duyne, P., & Levi, M. (2005). *Drugs and money managing the drug trade and crime-money in Europe*. London; New York: Routledge.
Van Vlasselaer, V., Eliassi-Rad, T., Akoglu, L., Snoeck, M., & Baesens, B. (2017). GOTCHA! Network-Based Fraud Detection for Social Security Fraud. *Manage. Sci., 63*(9), 3090-3110. doi:10.1287/mnsc.2016.2489
Vaughan, G. (2018). [Shell companies, the role of company and trust service providers, and alternative banking platforms highlighted in NZ Police money laundering report].
Vedrenne, G. (2019). Takedown of Cryptocurrency Mixer a Hard Blow for Money Launderers. Retrieved from https://www.moneylaundering.com/news/a-major-cryptocurrencies-mixer-dismantled-a-hard-blow-for-launderers/
Vitali, S., Glattfelder, J. B., & Battiston, S. (2011). The network of global corporate control. *PloS one, 6*(10), e25995.
Vittori, J. (2011). *Terrorist financing and resourcing*: Springer.
Von Altrock, C. (1996). *Fuzzy logic and neurofuzzy applications in business and finance*: Prentice-Hall, Inc.

Von Hoffmann, J. (2016). The international dimension of drug policy reform in Uruguay. *International Journal of Drug Policy, 34*, 27-33. doi:10.1016/j.drugpo.2016.04.015
Walker, J. (1999). How Big is Global Money Laundering? *Journal of Money Laundering Control, 3*(1), 25-37. doi:10.1108/eb027208
Walker, J., & Unger, B. (2009). Measuring global money laundering. *Review of Law and Economics, 5*(2), 821-853. doi:10.2202/1555-5879.1418
Walker, J. L. (1969). The Diffusion of Innovations among the American States. *American Political Science Review, 63*(3), 880-899. doi:10.1017/S0003055400258644
Walters, J., Budd, C., Smith, R. G., Choo, K. K. R., McCusker, R., & Rees, D. (2012). *Anti-money laundering and counter-terrorism financing across the globe: A comparative study of regulatory action*. Retrieved from Australia: https://aic.gov.au/publications/rpp/rpp113
Walters, R., & Bradley, T. (2019). *Introduction to criminological thought*: Pearson Education.
Wang, G. S., Davies, S. D., Halmo, L. S., Sass, A., & Mistry, R. D. (2018). Marijuana Legalization and Adolescent Health. *Journal of Adolescent Health, 63*(3), 367. doi:https://doi.org/10.1016/j.jadohealth.2018.06.018
Wang, G. S., Heard, K., & Roosevelt, G. (2017). The Unintended Consequences of Marijuana Legalization. *The Journal of Pediatrics, 190*, 12-13. doi:https://doi.org/10.1016/j.jpeds.2017.08.023
Wang, Y., Xu, D., Wang, H., Ye, K., & Gao, S. (2007). *Agent-oriented ontology for monitoring and detecting money laundering process*. Paper presented at the Proceedings of the 2nd international conference on Scalable information systems, Suzhou, China.
Watkins, M. W. (2006). Determining parallel analysis criteria. *Journal of modern applied statistical methods, 5*(2), 344-346.
Watson, E. E., & Schneider, H. (1999). Using ERP Systems in Education. *Communications of the Association for Information Systems, 1*. doi:10.17705/1CAIS.00109
Weatherburn, D., & Jones, C. (2001). *Does prohibition deter cannabis use?* Retrieved from https://www.bocsar.nsw.gov.au/Publications/CJB/cjb58.pdf
Wedge, R., Kanter, J. M., Rubio, S. M., Perez, S. I., & Veeramachaneni, K. (2017). Solving the" false positives" problem in fraud prediction. *arXiv preprint arXiv:1710.07709*.
Werb, D., Wood, E., Strathdee, S., Kazatchkine, M., des Jarlais, D., & Hankins, C. (2016). Open letter to the United Nations: A call for a reprioritisation of metrics to evaluate illicit drug policy. In: Tornto, Canada: International Centre for Science in Drugs Policy.
White, H. C., Boorman, S. A., & Breiger, R. L. (1976). Social Structure from Multiple Networks. I. Blockmodels of Roles and Positions. *American Journal of Sociology, 81*(4), 730-780.
Whiting, D. G., Hansen, J. V., McDonald, J. B., Albrecht, C., & Albrecht, W. S. (2012). Machine Learning Methods For Detecting Patterns Of Management Fraud. *Computational Intelligence, 28*(4), 505-527. doi:10.1111/j.1467-8640.2012.00425.x
Williams, G. J. (1999). Evolutionary hot spots data mining: An architecture for exploring for interesting discoveries. In (Vol. 1574, pp. 184-193): Springer Verlag.
Williams, R. (2019). ICO Regulations- Which are the Countries with Restrictions? In *CryptoNewsZ*.
Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud.
Wu, J., Shen, J., Zhou, B., Zhang, X., & Huang, B. (2019). General link prediction with influential node identification. *Physica A: Statistical Mechanics and its Applications, 523*, 996-1007. doi:https://doi.org/10.1016/j.physa.2019.04.205
Wu, S.-y., Zhang, Q., Xue, C.-y., & Liao, X.-y. (2019). Cold-start link prediction in multi-relational networks based on network dependence analysis. *Physica A: Statistical*

Mechanics and its Applications, 515, 558-565. doi:https://doi.org/10.1016/j.physa.2018.09.082
Xu, X., Yuruk, N., Feng, Z., & Schweiger, T. A. J. (2007). SCAN: A structural clustering algorithm for networks. In (pp. 824-833).
Yakubowski, M. (2019). [Japan: Crypto Industry Trade Group JCBA Issues Guidelines for ICO Regulation]. Web Page.
Yang, S., Xie, H., & Chen, L. Y. (2018). Renren to Scrap ICO After Talks With China Regulators, Sources Say. Retrieved from https://www.bloomberg.com/news/articles/2018-01-09/renren-is-said-to-scrap-ico-after-talks-with-china-regulators
Yao, Y., Zhang, R., Yang, F., Tang, J., Yuan, Y., & Hu, R. (2018). Link prediction in complex networks based on the interactions among paths. *Physica A: Statistical Mechanics and its Applications, 510*, 52-67. doi:https://doi.org/10.1016/j.physa.2018.06.051
Zahra, E., Darke, S., Degenhardt, L., & Campbell, G. (2020). Rates, characteristics and manner of cannabis-related deaths in Australia 2000–2018. *Drug and Alcohol Dependence*, 108028. doi:https://doi.org/10.1016/j.drugalcdep.2020.108028
Zdanowicz, J. S. (2004a). Detecting money laundering and terrorist financing via data mining. *Communications of the ACM, 47*(5), 53-55. doi:10.1145/986213.986239
Zdanowicz, J. S. (2004b). *U.S. Trade with the World and Al Qaeda Watch List Countries - 2001: An Estimate of Money Moved Out of and Into the U.S. Due to Suspicious Pricing in International Trade*. Retrieved from https://business.fiu.edu/pdf/PrintJun2007/tfml.pdf
Zdanowicz, J. S. (2009). Trade-based money laundering and terrorist financing. *Review of Law and Economics, 5*(2), 855-878. doi:10.2202/1555-5879.1419
Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Ffhr, L. (2017). The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators. *SSRN Electronic Journal*. doi:10.2139/ssrn.3072298
Zhang, T. (2014). A Novel Method of Identifying Influential Nodes in Complex Networks Based on Random Walks. *Journal of Information and Computational Science, 11*(18), 6735-6740. doi:10.12733/jics20105091
Zhang, Z., Salerno, J. J., & Yu, P. S. (2003). *Applying data mining in investigating money laundering crimes.* Paper presented at the Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining.
Zhou, Y., Cheng, H., & Yu, J. X. (2009). Graph clustering based on structural/attribute similarities. *Proceedings of the VLDB Endowment, 2*(1), 718-729. doi:10.14778/1687627.1687709
Zmudzinski, A. (2019). Dubai Real Estate Giant Emaar to Launch ETH Token, Considers ICO in Europe. Retrieved from https://cointelegraph.com/news/local-media-dubai-real-estate-giant-emaar-to-launch-eth-token-considers-ico-in-europe
Zucman, G., Fagan, T. L., & Piketty, T. (2015). *The Hidden Wealth of Nations : The Scourge of Tax Havens*. Chicago, IL: University of Chicago Press.
Zuo, X.-N., Ehmke, R., Mennes, M., Imperati, D., Castellanos, F. X., Sporns, O., & Milham, M. P. (2012). Network Centrality in the Human Functional Connectome. *Cerebral Cortex, 22*(8), 1862-1875. doi:10.1093/cercor/bhr269

Appendices

Appendix A. Model Error Measures for Decision Tree for Combination 1 Algorithms.

	Name	Learn	Test
	Average Log Likelihood (Negative)	0.20944	0.49529
	ROC (Area Under Curve)	0.95044	0.92947
	Variance of ROC (Area Under Curve)	0.02643	0.00027
	Lower Confidence Limit ROC	0.63182	0.89754
	Upper Confidence Limit ROC	1.00000	0.96140
	Lift	1.91265	1.92771
	K-S Stat	0.87670	0.83868
	Misclass Rate Overall (Raw)	0.06250	0.08125
	Balanced Error Rate (Simple Average over classes)	0.06165	0.08066
	Class. Accuracy (Baseline threshold)	0.93750	0.91875
	Relative Cost	0.12330	0.16132

Appendix B. Confusion Matrix for Decision Tree for Combination 1 Algorithms.

	Actual Class	Total Class	Percent Correct	Predicted Classes	
				0 N = 160	1 N = 160
	0	154	93.51%	144	10
	1	166	90.36%	16	150
	Total:	320			
	Average:		91.93%		
	Overall % Correct:		91.88%		
	Specificity		93.51%		
	Sensitivity/Recall		90.36%		
	Precision		93.75%		
	F1 statistic		92.02%		

Appendix C. Prediction Statistics for Decision Tree for Combination 1 Algorithms.

	Name	Score Result
	Mean Score	0.89114
	Log Likelihood	-35.07919
	Average Log Likelihood (Negative)	0.18860
	ROC (Area Under Curve)	0.95093
	Lift	1.71962
	D for binary models	0.83306

Appendix D. Confusion Matrix for Testing data for Decision Tree for Combination 1 Algorithms.

	Actual Class	Total Class	Percent Correct	Predicted Classes	
				0 N = 53	1 N = 40
	0	50	98.00%	49	1
	1	43	90.70%	4	39
	Total:	93			
	Average:		94.35%		
	Overall % Correct:		94.62%		
	Specificity		98.00%		
	Sensitivity/Recall		90.70%		
	Precision		97.50%		
	F1 statistic		93.98%		

Appendix E. Model Error Measures for Random Forests for Combination 1 Algorithms.

	Name	OOB
	Average Log Likelihood (Negative)	2.37788
	ROC (Area Under Curve)	0.95181
	Variance of ROC (Area Under Curve)	0.00017
	Lower Confidence Limit ROC	0.92618
	Upper Confidence Limit ROC	0.97743
	Lift	1.86930
	K-S Stat	0.83868
	Misclass Rate Overall (Raw)	0.08438
	Balanced Error Rate (Simple Average over classes)	0.08066
	Class. Accuracy (Baseline threshold)	0.91875

Appendix F. Confusion Matrix for Random Forests for Combination 1 Algorithms.

	Actual Class	Total Class	Percent Correct	Predicted Classes	
				0 N = 160	1 N = 160
	0	154	93.51%	144	10
	1	166	90.36%	16	150
	Total:	320			
	Average:		91.93%		
	Overall % Correct:		91.88%		
	Specificity		93.51%		
	Sensitivity/Recall		90.36%		
	Precision		93.75%		
	F1 statistic		92.02%		

Appendix G. Prediction Statistics for Random Forests for Combination 1 Algorithms.

	Name	Score Result
	Mean Score	0.89185
	Log Likelihood	-52.46400
	Average Log Likelihood (Negative)	0.28206
	ROC (Area Under Curve)	0.95558
	Variance of ROC (Area Under Curve)	0.00055
	Lower Confidence Limit ROC	0.90968
	Upper Confidence Limit ROC	1.00000
	K-S Stat	0.90698
	D for binary models	4.93434

Appendix H. Confusion Matrix for Testing data for Random Forest for Combination 1 Algorithms.

	Actual Class	Total Class	Percent Correct	Predicted Classes	
				0 N = 52	1 N = 41
	0	50	96.00%	48	2
	1	43	90.70%	4	39
	Total:	93			
	Average:		93.35%		
	Overall % Correct:		93.55%		
	Specificity		96.00%		
	Sensitivity/Recall		90.70%		
	Precision		95.12%		
	F1 statistic		92.86%		

Appendix I. Model Error Measures for TreeNet for Combination 1 Algorithms.

	Name	Learn	Test	Learn Sampled
	Average Log Likelihood (Negative)	0.23868	0.16940	0.23809
	ROC (Area Under Curve)	0.97335	0.98561	0.97426
	Variance of ROC (Area Under Curve)	0.00008	0.00021	n/a
	Lower Confidence Limit ROC	0.95604	0.95739	n/a
	Upper Confidence Limit ROC	0.99066	1.00000	n/a
	Lift	2.00752	1.60606	2.03030
	K-S Stat	0.87252	0.96970	0.88102
	Misclass Rate Overall (Raw)	0.07116	0.01887	0.06716
	Balanced Error Rate (Simple Average over classes)	0.07120	0.01515	n/a
	Class. Accuracy (Baseline threshold)	0.92884	0.98113	n/a
	Fraction Data Used after influence trimming	0.41948	n/a	n/a

Appendix J. Confusion Matrix for TreeNet for Combination 1 Algorithms.

	Actual Class	Total Class	Percent Correct	Predicted Classes	
				0 N = 21	1 N = 32
	0	20	100.00%	20	0
	1	33	96.97%	1	32
	Total:	53			
	Average:		98.48%		
	Overall % Correct:		98.11%		
	Specificity		100.00%		
	Sensitivity/ Recall		96.97%		
	Precision		100.00%		

	F1 statistic		98.46%		

Appendix K. Prediction Statistics for TreeNet for Combination 1 Algorithms.

	Name	Score Result
	Mean Score	0.85011
	Log Likelihood	-36.91108
	Average Log Likelihood (Negative)	0.19845
	ROC (Area Under Curve)	0.98953
	Variance of ROC (Area Under Curve)	0.00004
	Lower Confidence Limit ROC	0.97698
	Upper Confidence Limit ROC	1.00000
	Lift	2.16279
	K-S Stat	0.90698
	D for binary models	1.02033

Appendix L. Confusion Matrix for Testing data for TreeNet for Combination 1 Algorithms.

	Actual Class	Total Class	Percent Correct	Predicted Classes	
				0 N = 52	1 N = 41
	0	50	96.00%	48	2
	1	43	90.70%	4	39
	Total:	93			
	Average:		93.35%		
	Overall % Correct:		93.55%		
	Specificity		96.00%		
	Sensitivity/Recall		90.70%		

	Precision		95.12%		
	F1 statistic		92.86%		

Appendix M. Model Error Measures for Decision Tree for Combination 2 Algorithms.

	Name	Learn	Test
	Average Log Likelihood (Negative)	0.16013	0.42662
	ROC (Area Under Curve)	0.95740	0.93235
	Variance of ROC (Area Under Curve)	0.01932	0.00028
	Lower Confidence Limit ROC	0.68496	0.89937
	Upper Confidence Limit ROC	1.00000	0.96532
	Lift	1.92771	1.91442
	K-S Stat	0.90917	0.89063
	Misclass Rate Overall (Raw)	0.04688	0.05625
	Balanced Error Rate (Simple Average over classes)	0.04542	0.05469
	Class. Accuracy (Baseline threshold)	0.95313	0.94375
	Relative Cost	0.09083	0.10937

Appendix N. Confusion Matrix for Decision Tree for Combination 2 Algorithms.

	Actual Class	Total Class	Percent Correct	Predicted Classes	
				0 N = 168	1 N = 152
	0	154	98.70%	152	2
	1	166	90.36%	16	150
	Total:	320			
	Average:		94.53%		
	Overall % Correct:		94.38%		
	Specificity		98.70%		

	Sensitivity/Recall		90.36%		
	Precision		98.68%		
	F1 statistic		94.34%		

Appendix O. Prediction Statistics for Decision Trees for Combination 2 Algorithms.

	Name	Score Result
	Mean Score	0.93284
	Log Likelihood	-174.00948
	Average Log Likelihood (Negative)	0.93553
	ROC (Area Under Curve)	0.97791
	Lift	1.82280
	D for binary models	5.20575

Appendix P. Confusion Matrix for Testing Data for Decision Trees for Combination 2 Algorithms.

	Actual Class	Total Class	Percent Correct	Predicted Classes	
				0 N = 50	1 N = 43
	0	50	98.00%	49	1
	1	43	97.67%	1	42
	Total:	93			
	Average:		97.84%		
	Overall % Correct:		97.85%		
	Specificity		98.00%		
	Sensitivity/ Recall		97.67%		
	Precision		97.67%		
	F1 statistic		97.67%		

Appendix Q. Model Error Measures for Random Forest for Combination 2 Algorithms.

	Name	OOB
	Average Log Likelihood (Negative)	2.31673
	ROC (Area Under Curve)	0.96759
	Variance of ROC (Area Under Curve)	0.00010
	Lower Confidence Limit ROC	0.94825
	Upper Confidence Limit ROC	0.98693
	Lift	1.92771
	K-S Stat	0.89712
	Misclass Rate Overall (Raw)	0.05938
	Balanced Error Rate (Simple Average over classes)	0.05492
	Class. Accuracy (Baseline threshold)	0.94375

Appendix R. Confusion Matrix for Random Forest for Combination 2 Algorithms.

	Actual Class	Total Class	Percent Correct	Predicted Classes	
				0 N = 166	1 N = 154
	0	154	98.05%	151	3
	1	166	90.96%	15	151
	Total:	320			
	Average:		94.51%		
	Overall % Correct:		94.38%		
	Specificity		98.05%		
	Sensitivity/ Recall		90.96%		
	Precision		98.05%		
	F1 statistic		94.38%		

Appendix S. Prediction Statistics for Random Forest for Combination 2 Algorithms.

	Name	Score Result
	Mean Score	0.94224
	Log Likelihood	-177.10237
	Average Log Likelihood (Negative)	0.95216
	ROC (Area Under Curve)	0.97349
	Variance of ROC (Area Under Curve)	0.00035
	Lower Confidence Limit ROC	0.93689
	Upper Confidence Limit ROC	1.00000
	K-S Stat	0.95674
	D for binary models	1.55907

Appendix T. Confusion Matrix for Testing data for Random Forest for Combination 2 Algorithms.

	Actual Class	Total Class	Percent Correct	Predicted Classes	
				0 N = 51	1 N = 42
	0	50	98.00%	49	1
	1	43	95.35%	2	41
	Total:	93			
	Average:		96.67%		
	Overall % Correct:		96.77%		
	Specificity		98.00%		
	Sensitivity/ Recall		95.35%		
	Precision		97.62%		
	F1 statistic		96.47%		

Appendix U. Model Error Measures for TreeNet for Combination 2 Algorithms.

	Name	Learn	Test	Learn Sampled
	Average Log Likelihood (Negative)	0.20751	0.16890	0.20606
	ROC (Area Under Curve)	0.97385	0.98788	0.97527
	Variance of ROC (Area Under Curve)	0.00009	0.00015	n/a
	Lower Confidence Limit ROC	0.95526	0.96412	n/a
	Upper Confidence Limit ROC	0.99245	1.00000	n/a
	Lift	2.00752	1.60606	2.03030
	K-S Stat	0.90242	0.96970	0.90954
	Misclass Rate Overall (Raw)	0.04869	0.03774	0.04478
	Balanced Error Rate (Simple Average over classes)	0.04884	0.04545	n/a
	Class. Accuracy (Baseline threshold)	0.95131	0.94340	n/a
	Fraction Data Used after influence trimming	0.41199	n/a	n/a

Appendix V. Confusion Matrix for TreeNet for Combination 2 Algorithms.

	Actual Class	Total Class	Percent Correct	Predicted Classes	
				0 N = 23	1 N = 30
	0	20	100.00%	20	0
	1	33	90.91%	3	30
	Total:	53			
	Average:		95.45%		
	Overall % Correct:		94.34%		
	Specificity		100.00%		
	Sensitivity/ Recall		90.91%		

	Precision		100.00%		
	F1 statistic		95.24%		

Appendix W. Prediction Statistics for TreeNet for Combination 2 Algorithms

	Name	Score Result
	Mean Score	0.86926
	Log Likelihood	-31.84377
	Average Log Likelihood (Negative)	0.17120
	ROC (Area Under Curve)	0.98140
	Variance of ROC (Area Under Curve)	0.00018
	Lower Confidence Limit ROC	0.95545
	Upper Confidence Limit ROC	1.00000
	Lift	2.16279
	K-S Stat	0.95674
	D for binary models	2.99265

Appendix X. Confusion Matrix for Testing data for TreeNet for Combination 2 Algorithms.

	Actual Class	Total Class	Percent Correct	Predicted Classes	
				0 N = 50	1 N = 43
	0	50	98.00%	49	1
	1	43	97.67%	1	42
	Total:	93			
	Average:		97.84%		
	Overall % Correct:		97.85%		
	Specificity		98.00%		
	Sensitivity/ Recall		97.67%		

	Precision		97.67%		
	F1 statistic		97.67%		

Appendix Y. Model Error Measures for Decision Tree for Combination 3 Algorithms.

	Name	Learn	Test
	Average Log Likelihood (Negative)	0.22839	0.51117
	ROC (Area Under Curve)	0.94402	0.92319
	Variance of ROC (Area Under Curve)	0.03521	0.00030
	Lower Confidence Limit ROC	0.57624	0.88924
	Upper Confidence Limit ROC	1.00000	0.95715
	Lift	1.89759	1.81583
	K-S Stat	0.86559	0.83962
	Misclass Rate Overall (Raw)	0.06875	0.08125
	Balanced Error Rate (Simple Average over classes)	0.06720	0.08019
	Class. Accuracy (Baseline threshold)	0.93125	0.91875
	Relative Cost	0.13441	0.16038

Appendix Z. Confusion Matrix for Decision Tree for Combination 3 Algorithms.

	Actual Class	Total Class	Percent Correct	Predicted Classes	
				0 N = 164	1 N = 156
	0	154	94.81%	146	8
	1	166	89.16%	18	148
	Total:	320			
	Average:		91.98%		
	Overall % Correct:		91.88%		
	Specificity		94.81%		

	Sensitivity/ Recall		89.16%		
	Precision		94.87%		
	F1 statistic		91.93%		

Appendix AA. Prediction Statistics for Decision Tree for Combination 3 Algorithms.

	Name	Score Result
	Mean Score	0.87371
	Log Likelihood	-44.88645
	Average Log Likelihood (Negative)	0.24133
	ROC (Area Under Curve)	0.94047
	Lift	1.71692
	D for binary models	1.21494

Appendix BB. Confusion Matrix for Testing data for Decision Tree for Combination 3 Algorithms.

	Actual Class	Total Class	Percent Correct	Predicted Classes	
				0 N = 51	1 N = 42
	0	154	98.70%	152	2
	1	166	90.36%	16	150
	Total:	320			
	Average:		94.53%		
	Overall % Correct:		94.38%		
	Specificity		98.70%		
	Sensitivity/ Recall		90.36%		

	Precision		98.68%		
	F1 statistic		94.34%		

Appendix CC. Confusion Matrix for Testing data for Random Forest for Combination 3 Algorithms.

	Actual Class	Total Class	Percent Correct	Predicted Classes	
				0 N = 55	1 N = 38
	0	50	98.00%	49	1
	1	43	86.05%	6	37
	Total:	93			
	Average:		92.02%		
	Overall % Correct:		92.47%		
	Specificity		98.00%		
	Sensitivity/ Recall		86.05%		
	Precision		97.37%		
	F1 statistic		91.36%		

Appendix DD. Model Error Measures for Random Forest for Combination 3 Algorithms.

	Name	OOB
	Average Log Likelihood (Negative)	0.17060
	ROC (Area Under Curve)	0.97302
	Variance of ROC (Area Under Curve)	0.00037
	Lower Confidence Limit ROC	0.93533
	Upper Confidence Limit ROC	1.00000

	Lift	2.09302
	K-S Stat	0.95674
	Misclass Rate Overall (Raw)	0.03226
	Balanced Error Rate (Simple Average over classes)	0.03326
	Class. Accuracy (Baseline threshold)	0.96774

Appendix EE. Confusion Matrix for Random Forest for Combination 3 Algorithms.

	Actual Class	Total Class	Percent Correct	Predicted Classes	
				0 N = 51	1 N = 42
	0	50	98.00%	49	1
	1	43	95.35%	2	41
	Total:	93			
	Average:		96.67%		
	Overall % Correct:		96.77%		
	Specificity		98.00%		
	Sensitivity/ Recall		95.35%		
	Precision		97.62%		
	F1 statistic		96.47%		

Appendix FF. Prediction Statistics for Random Forest for Combination 3 Algorithms.

	Name	Score Result
	Mean Score	0.93399
	Log Likelihood	-16.72494
	Average Log Likelihood (Negative)	0.08992
	ROC (Area Under Curve)	0.99442
	Variance of ROC (Area Under Curve)	0.00002

	Lower Confidence Limit ROC	0.98559
	Upper Confidence Limit ROC	1.00000
	K-S Stat	0.95674
	D for binary models	1.92460

Appendix GG. Confusion Matrix for Testing data for Random Forest for Combination 3 Algorithms.

	Actual Class	Total Class	Percent Correct	Predicted Classes	
				0 N = 50	1 N = 43
	0	50	98.00%	49	1
	1	43	97.67%	1	42
	Total:	93			
	Average:		97.84%		
	Overall % Correct:		97.85%		
	Specificity		98.00%		
	Sensitivity/ Recall		97.67%		
	Precision		97.67%		
	F1 statistic		97.67%		

Appendix HH. Model Error Measures for TreeNet for Combination 3 Algorithms.

	Name	Learn	Test	Learn Sampled
	Average Log Likelihood (Negative)	0.24428	0.19550	0.24128
	ROC (Area Under Curve)	0.96336	0.98030	0.96702
	Variance of ROC (Area Under Curve)	0.00014	0.00039	n/a
	Lower Confidence Limit ROC	0.93996	0.94170	n/a
	Upper Confidence Limit ROC	0.98676	1.00000	n/a

	Lift	2.00752	1.60606	2.03030
	K-S Stat	0.90237	0.96970	0.90998
	Misclass Rate Overall (Raw)	0.05243	0.05660	0.05224
	Balanced Error Rate (Simple Average over classes)	0.05255	0.04545	n/a
	Class. Accuracy (Baseline threshold)	0.94757	0.94340	n/a
	Fraction Data Used after influence trimming	0.41199	n/a	n/a

Appendix II. Confusion Matrix for TreeNet for Combination 3 Algorithms.

	Actual Class	Total Class	Percent Correct	Predicted Classes	
				0 N = 23	1 N = 30
	0	20	100.00%	20	0
	1	33	90.91%	3	30
	Total:	53			
	Average:		95.45%		
	Overall % Correct:		94.34%		
	Specificity		100.00%		
	Sensitivity/ Recall		90.91%		
	Precision		100.00%		
	F1 statistic		95.24%		

Appendix JJ. Prediction Statistics for TreeNet for Combination 3 Algorithms.

	Name	Score Result
	Mean Score	0.83424
	Log Likelihood	-42.67600
	Average Log Likelihood (Negative)	0.22944

	ROC (Area Under Curve)	0.97977
	Variance of ROC (Area Under Curve)	0.00022
	Lower Confidence Limit ROC	0.95100
	Upper Confidence Limit ROC	1.00000
	Lift	2.16279
	K-S Stat	0.93674
	D for binary models	1.50048

Appendix KK. Confusion Matrix for Testing data for TreeNet for Combination 3 Algorithms.

	Actual Class	Total Class	Percent Correct	Predicted Classes	
				0 N = 53	1 N = 40
	0	50	98.00%	49	1
	1	43	90.70%	4	39
	Total:	93			
	Average:		94.35%		
	Overall % Correct:		94.62%		
	Specificity		98.00%		
	Sensitivity/ Recall		90.70%		
	Precision		97.50%		
	F1 statistic		93.98%		

Appendix LL. Model Error Measures for Decision Tree for Combination 4 Algorithms.

	Name	Learn	Test
	Average Log Likelihood (Negative)	0.20732	1.04313
	ROC (Area Under Curve)	0.95140	0.90915

	Variance of ROC (Area Under Curve)	0.03038	0.00039
	Lower Confidence Limit ROC	0.60974	0.87056
	Upper Confidence Limit ROC	1.00000	0.94774
	Lift	1.90136	1.70826
	K-S Stat	0.88366	0.79369
	Misclass Rate Overall (Raw)	0.05938	0.10938
	Balanced Error Rate (Simple Average over classes)	0.05817	0.10824
	Class. Accuracy (Baseline threshold)	0.94063	0.89063
	Relative Cost	0.11634	0.21648

Appendix MM. Confusion Matrix for Decision Tree for Combination 4 Algorithms.

	Actual Class	Total Class	Percent Correct	Predicted Classes	
				0 N = 165	1 N = 155
	0	154	92.21%	142	12
	1	166	86.14%	23	143
	Total:	320			
	Average:		89.18%		
	Overall % Correct:		89.06%		
	Specificity		92.21%		
	Sensitivity/ Recall		86.14%		
	Precision		92.26%		
	F1 statistic		89.10%		

Appendix NN. Prediction Statistics for Testing Data for Decision Tree for Combination 4 Algorithms.

	Name	Score Result
	Mean Score	0.84489

	Log Likelihood	-217.25935
	Average Log Likelihood (Negative)	1.16806
	ROC (Area Under Curve)	0.92116
	Lift	1.71412
	D for binary models	2.78412

Appendix OO. Confusion Matrix for Testing Data for Decision Tree for Combination 4 Algorithms.

	Actual Class	Total Class	Percent Correct	Predicted Classes	
				0 N = 57	1 N = 36
	0	50	96.00%	48	2
	1	43	79.07%	9	34
	Total:	93			
	Average:		87.53%		
	Overall % Correct:		88.17%		
	Specificity		96.00%		
	Sensitivity/ Recall		79.07%		
	Precision		94.44%		
	F1 statistic		86.08%		

Appendix PP. Model Error Measures for Random Forest for Combination 4 Algorithms.

	Name	OOB
	Average Log Likelihood (Negative)	2.18640
	ROC (Area Under Curve)	0.94729
	Variance of ROC (Area Under Curve)	0.00018
	Lower Confidence Limit ROC	0.92109

	Upper Confidence Limit ROC	0.97349
	Lift	1.86747
	K-S Stat	0.81599
	Misclass Rate Overall (Raw)	0.10937
	Balanced Error Rate (Simple Average over classes)	0.10824
	Class. Accuracy (Baseline threshold)	0.89063

Appendix QQ. Confusion Matrix for Random Forest for Combination 4 Algorithms.

	Actual Class	Total Class	Percent Correct	Predicted Classes	
				0 N = 165	1 N = 155
	0	154	92.21%	142	12
	1	166	86.14%	23	143
	Total:	320			
	Average:		89.18%		
	Overall % Correct:		89.06%		
	Specificity		92.21%		
	Sensitivity/ Recall		86.14%		
	Precision		92.26%		
	F1 statistic		89.10%		

Appendix RR. Prediction Statistics for Testing Data for Random Forest for Combination 4 Algorithms.

	Name	Score Result
	Mean Score	0.82266
	Log Likelihood	-515.83608

	Average Log Likelihood (Negative)	2.77331
	ROC (Area Under Curve)	0.93558
	Variance of ROC (Area Under Curve)	0.00086
	Lower Confidence Limit ROC	0.87815
	Upper Confidence Limit ROC	0.99302
	K-S Stat	0.84698
	D for binary models	9.07266

Appendix SS. Confusion Matrix for Testing Data for Random Forest for Combination 4 Algorithms.

	Actual Class	Total Class	Percent Correct	Predicted Classes	
				0 N = 56	1 N = 37
	0	50	98.00%	49	1
	1	43	83.72%	7	36
	Total:	93			
	Average:		90.86%		
	Overall % Correct:		91.40%		
	Specificity		98.00%		
	Sensitivity/ Recall		83.72%		
	Precision		97.30%		
	F1 statistic		90.00%		

Appendix TT. Model Error Measures for TreeNet for Combination 4 Algorithms.

	Name	Learn	Test	Learn Sampled
	Average Log Likelihood (Negative)	0.26533	0.19980	0.26784
	ROC (Area Under Curve)	0.96712	0.97500	0.96602
	Variance of ROC (Area Under Curve)	0.00010	0.00063	n/a

	Lower Confidence Limit ROC	0.94790	0.92600	n/a
	Upper Confidence Limit ROC	0.98634	1.00000	n/a
	Lift	2.00752	1.60606	2.03030
	K-S Stat	0.84996	0.96970	0.83512
	Misclass Rate Overall (Raw)	0.07865	0.05660	0.08955
	Balanced Error Rate (Simple Average over classes)	0.07875	0.04545	n/a
	Class. Accuracy (Baseline threshold)	0.92135	0.94340	n/a
	Fraction Data Used after influence trimming	0.41948	n/a	n/a

Appendix UU. Confusion Matrix for TreeNet for Combination 4 Algorithms.

	Actual Class	Total Class	Percent Correct	Predicted Classes	
				0 N = 23	1 N = 30
	0	20	100.00%	20	0
	1	33	90.91%	3	30
	Total:	53			
	Average:		95.45%		
	Overall % Correct:		94.34%		
	Specificity		100.00%		
	Sensitivity/ Recall		90.91%		
	Precision		100.00%		
	F1 statistic		95.24%		

Appendix VV. Prediction Statistics for Testing Data for TreeNet for Combination 4 Algorithms.

	Name	Score Result
	Mean Score	0.79017

	LogLikelihood	-53.56109
	Average LogLikelihood (Negative)	0.28796
	ROC (Area Under Curve)	0.95140
	Variance of ROC (Area Under Curve)	0.00056
	Lower Confidence Limit ROC	0.90496
	Upper Confidence Limit ROC	0.99783
	Lift	2.16279
	K-S Stat	0.88698
	D for binary models	4.95548

Appendix WW. Confusion Matrix for Testing Data for TreeNet for Combination 4 Algorithms.

	Actual Class	Total Class	Percent Correct	Predicted Classes	
				0 N = 53	1 N = 40
	0	50	98.00%	49	1
	1	43	90.70%	4	39
	Total:	93			
	Average:		94.35%		
	Overall % Correct:		94.62%		
	Specificity		98.00%		
	Sensitivity/ Recall		90.70%		
	Precision		97.50%		
	F1 statistic		93.98%		

Appendix XX. Model Error Measures for Decision Tree for Combination 5 Algorithms.

	Name	Learn	Test
	Average LogLikelihood (Negative)	0.22916	0.26805
	ROC (Area Under Curve)	0.94881	0.91650
	Variance of ROC (Area Under Curve)	0.02656	0.00033
	Lower Confidence Limit ROC	0.62937	0.88069
	Upper Confidence Limit ROC	1.00000	0.95232
	Lift	1.89759	1.80723
	K-S Stat	0.85675	0.83821
	Misclass Rate Overall (Raw)	0.07188	0.08438
	Balanced Error Rate (Simple Average over classes)	0.07162	0.08391
	Class. Accuracy (Baseline threshold)	0.92813	0.91563
	Relative Cost	0.14325	0.16781

Appendix YY. Confusion Matrix for Decision Tree for Combination 5 Algorithms.

	Actual Class	Total Class	Percent Correct	Predicted Classes	
				0 N = 159	1 N = 161
	0	154	92.86%	143	11
	1	166	90.36%	16	150
	Total:	320			
	Average:		91.61%		
	Overall % Correct:		91.56%		
	Specificity		92.86%		
	Sensitivity/ Recall		90.36%		
	Precision		93.17%		
	F1 statistic		91.74%		

Appendix ZZ. Prediction Statistics for Testing Data for Decision Tree for Combination 5 Algorithms.

	Name	Score Result
	Mean Score	0.87682
	Log Likelihood	-43.69141
	Average Log Likelihood (Negative)	0.23490
	ROC (Area Under Curve)	0.93977
	Lift	1.71692
	D for binary models	0.47432

Appendix AAA. Confusion Matrix for Testing Data for Decision Tree for Combination 5 Algorithms.

	Actual Class	Total Class	Percent Correct	Predicted Classes	
				0 N = 52	1 N = 41
	0	50	96.00%	48	2
	1	43	90.70%	4	39
	Total:	93			
	Average:		93.35%		
	Overall % Correct:		93.55%		
	Specificity		96.00%		
	Sensitivity/ Recall		90.70%		
	Precision		95.12%		
	F1 statistic		92.86%		

Appendix BBB. Model Error Measures for Random Forest for Combination 5 Algorithms.

	Name	OOB
	Average LogLikelihood (Negative)	2.63258
	ROC (Area Under Curve)	0.94692
	Variance of ROC (Area Under Curve)	0.00017
	Lower Confidence Limit ROC	0.92101
	Upper Confidence Limit ROC	0.97283
	Lift	1.90166
	K-S Stat	0.85026
	Misclass Rate Overall (Raw)	0.08438
	Balanced Error Rate (Simple Average over classes)	0.08391
	Class. Accuracy (Baseline threshold)	0.91563

Appendix CCC. Confusion Matrix for Random Forest for Combination 5 Algorithms.

	Actual Class	Total Class	Percent Correct	Predicted Classes	
				0 N = 159	1 N = 161
	0	154	92.86%	143	11
	1	166	90.36%	16	150
	Total:	320			
	Average:		91.61%		
	Overall % Correct:		91.56%		
	Specificity		92.86%		
	Sensitivity/ Recall		90.36%		
	Precision		93.17%		
	F1 statistic		91.74%		

Appendix DDD. Prediction Statistics for Testing Data for Random Forest for Combination 5 Algorithms.

	Name	Score Result
	Mean Score	0.88119
	Log Likelihood	-53.10882
	Average Log Likelihood (Negative)	0.28553
	ROC (Area Under Curve)	0.96721
	Variance of ROC (Area Under Curve)	0.00024
	Lower Confidence Limit ROC	0.93702
	Upper Confidence Limit ROC	0.99740
	K-S Stat	0.86698
	D for binary models	6.36171

Appendix EEE. Confusion Matrix for Testing Data for Random Forest for Combination 5 Algorithms.

	Actual Class	Total Class	Percent Correct	Predicted Classes	
				0 N = 52	1 N = 41
	0	50	96.00%	48	2
	1	43	90.70%	4	39
	Total:	93			
	Average:		93.35%		
	Overall % Correct:		93.55%		
	Specificity		96.00%		
	Sensitivity/ Recall		90.70%		
	Precision		95.12%		
	F1 statistic		92.86%		

Appendix FFF. Model Error Measures for TreeNet for Combination 5 Algorithms.

	Name	Learn	Test	Learn Sampled
	Average LogLikelihood (Negative)	0.26983	0.19878	0.27038
	ROC (Area Under Curve)	0.96364	0.97727	0.96546
	Variance of ROC (Area Under Curve)	0.00013	0.00052	n/a
	Lower Confidence Limit ROC	0.94124	0.93273	n/a
	Upper Confidence Limit ROC	0.98604	1.00000	n/a
	Lift	2.00752	1.60606	2.03030
	K-S Stat	0.86483	0.96970	0.86497
	Misclass Rate Overall (Raw)	0.08989	0.03774	0.09701
	Balanced Error Rate (Simple Average over classes)	0.08995	0.04545	n/a
	Class. Accuracy (Baseline threshold)	0.91011	0.94340	n/a
	Fraction Data Used after influence trimming	0.42697	n/a	n/a

Appendix GGG. Confusion Matrix for TreeNet for Combination 5 Algorithms.

	Actual Class	Total Class	Percent Correct	Predicted Classes	
				0 N = 23	1 N = 30
	0	20	100.00%	20	0
	1	33	90.91%	3	30
	Total:	53			
	Average:		95.45%		
	Overall % Correct:		94.34%		
	Specificity		100.00%		
	Sensitivity/ Recall		90.91%		

	Precision		100.00%		
	F1 statistic		95.24%		

Appendix HHH. Prediction Statistics for Testing Data for TreeNet for Combination 5 Algorithms.

	Name	Score Result
	Mean Score	0.81657
	Log Likelihood	-46.62625
	Average Log Likelihood (Negative)	0.25068
	ROC (Area Under Curve)	0.96442
	Variance of ROC (Area Under Curve)	0.00033
	Lower Confidence Limit ROC	0.92867
	Upper Confidence Limit ROC	1.00000
	Lift	2.16279
	K-S Stat	0.88698
	D for binary models	1.51198

Appendix III. Confusion Matrix for Testing Data for TreeNet for Combination 5 Algorithms.

	Actual Class	Total Class	Percent Correct	Predicted Classes	
				0 N = 52	1 N = 41
	0	50	96.00%	48	2
	1	43	90.70%	4	39
	Total:	93			
	Average:		93.35%		
	Overall % Correct:		93.55%		

	Specificity		96.00%		
	Sensitivity/ Recall		90.70%		
	Precision		95.12%		
	F1 statistic		92.86%		