MASTERS BY RESEARCH

# Regulation of fintech development: a critical analysis with a case study of crypto assets in the UK and EU

Huang, Sherena

*Award date:*
2020

*Awarding institution:*
Bangor University

# REGULATION OF FINTECH DEVELOPMENT:

# A CRITICAL ANALYSIS WITH A CASE STUDY OF CRYPTO ASSETS IN THE UK AND EU


Sherena Sheng Huang

Department of Law

A thesis submitted for the degree of

LLM by Research

2019 – 2020

# Declaration and Consent

Yr wyf drwy hyn yn datgan mai canlyniad fy ymchwil fy hun yw'r thesis hwn, ac eithrio lle nodir yn wahanol. Caiff ffynonellau eraill eu cydnabod gan droednodiadau yn rhoi cyfeiriadau eglur. Nid yw sylwedd y gwaith hwn wedi cael ei dderbyn o'r blaen ar gyfer unrhyw radd, ac nid yw'n cael ei gyflwyno ar yr un pryd mewn ymgeisiaeth am unrhyw radd oni bai ei fod, fel y cytunwyd gan y Brifysgol, am gymwysterau deuol cymeradwy.

I hereby declare that this thesis is the results of my own investigations, except where otherwise stated. All other sources are acknowledged by bibliographic references. This work has not previously been accepted in substance for any degree and is not being concurrently submitted in candidature for any degree unless, as agreed by the University, for approved dual awards.

# Abstract

The financial market is more complicated than it has been for a long time. The anonymous peer-to-peer transaction networks of crypto assets are challenging the existing regulatory regimes and call out a decentralised financial system. Are the current regulatory perimeters of the Financial Conduct Authority sufficient and effective to guide the crypto markets? What actions are needed for a harmonised EU-wide regulatory crypto asset policy? What are the Laws and Acts applicable to crypto assets crimes? The three research questions address the potential issues in the current regulatory schemes: effectiveness, consistency and applicability.

Chapter 1 outlines the research questions, objectives, scope and outcomes as well as the research methods employed by this thesis. Chapter 2 reviews the background of crypto asset development and the technology underpins it, as well as the role of crypto assets in financial crimes. Chapter 3 provides an overview of the development of anti-money laundering regulations in the UK and EU and discusses the use of crypto assets in international money-laundering. Chapter 4 uncovers the pros and cons of the Distributed Ledger Technology to central banks and searches out the opinions of the central bank on issuing national cryptocurrencies. The three chapters establish the theoretical framework of this thesis and examine the issues that crypto asset may bring to the financial systems and the official responses, accordingly.

Chapter 5 and Chapter 6 employs comparative methods to evaluate the effectiveness, consistency and applicability of existing regulations on crypto assets in the UK and EU. Chapter 5 analyses the effectiveness of the regulatory framework of crypto assets in the UK, effective of July 2019. The existing regulatory perimeters of the FCA on commercial activities of crypto assets are complicated in structure and have put additional economic and operational pressures to FinTech firms. Three loopholes discovered in the secondary legislation of the UK could lead to difficulties in prosecution and court judgement for crypto asset cases in the future. Non-commercial crimes of crypto assets can be prosecuted under different Acts in the UK subject to the motives, actions and consequences taking place in a criminal process. Chapter 6 examines the consistency of crypto asset regulations within the EU using six EU countries that represent the three regulatory stages of crypto assets as examples. Despite the unified anti-money regulation within the EU under the Fifth AML Directive, the national regulatory regimes on commercial activities of crypto assets in EU countries are disparate. The unharmonised regulatory framework across the EU raises the questions of prosecution and jurisdiction for transnational activities of crypto assets. Chapter 7 recaps the research outcomes responding to the three research questions and identifies research implications as well as research limitations and the potential for further development.

# Acknowledgement

I would like to thank my sister, Ms Anqin Huang and her family, for their unlimited care and support.

I would also like to thank my LLM supervisor, Dr Wei Shi for his patience and valuable guidance and Dr Mark Hyland for supporting me working on this topic.

Additional thanks to my former PhD supervisor, Professor Jonathan Williams, and my former colleagues at the FCA, especially to Mrs Julia Hoggett, Director of Market Oversight Division, and Mr Vincent Coughlin QC, Chief Criminal Counsel, for their trust and encouragement.

My appreciation also goes to Bangor University for the scholarship and to all Bangor staff whom have been supporting my study.

This research bridges my knowledge and experiences in Economics and Finance, Computer Science and Business Management and fulfils my curiosity in FinTech regulations and legal research.

# Contents

List of Abbreviations ..... i
1 Introduction and Overview ..... 1
1.1 Research Questions ..... 1
1.2 Research Objectives ..... 6
1.3 Research Methods ..... 8
1.4 Research Scope ..... 12
1.5 Research Outcomes ..... 15
2 Background and Theoretical Analysis ..... 19
2.1 Background of Fintech and Crypto Assets ..... 19
2.2 Definitions of Crypto Assets around the World ..... 21
2.3 The Properties of Crypto Assets ..... 29
2.4 The Role of Crypto Assets in Financial Crime ..... 34
3 The Development of Anti-Money Laundering Regulations ..... 39
3.1 Initiatives of Anti-Money Laundering in the UK and EU ..... 39
3.1.1 Money Laundering Regulation in the UK ..... 39
3.1.2 Money Laundering Regulation in the EU ..... 45
3.2 The Role of Crypto Assets in Money Laundering ..... 48
4 Central Bank Cryptocurrency ..... 54
4.1 The Concept and Underlying Rationale ..... 54
4.2 Current Plans of Central Banks ..... 55
5 An Insight into the Regulation of Crypto Assets in the UK ..... 60
5.1 The Legal Basis of Crypto Assets Regulation in the UK ..... 60
5.2 Regulated Crypto Tokens ..... 66
5.2.1 Security Tokens ..... 67
5.2.2 Analysis of the Effectiveness of the Security Token Regulation ..... 70
5.2.3 E-money Tokens ..... 73
5.2.4 Analysis of the Effectiveness of the E-Money Token Regulation ..... 75
5.3 Unregulated Crypto Tokens ..... 77
5.3.1 Exchange Tokens and Relevant Regulations ..... 77
5.3.2 Utility Tokens and Relevant Regulation ..... 78
5.3.3 Analysis of Unregulated Tokens and Potential Issues ..... 78
5.4 Illicit Activities of Crypto Assets in the UK ..... 80

5.4.1 Direct Unlawful Activities ..... 82
5.4.2 Indirect Unlawful Activities ..... 83
5.4.3 Anti-Money Laundering in the UK ..... 86
6 Regulation of Crypto Assets in the EU ..... 90
6.1 Analysis of General Regulations ..... 90
6.2 Analysis of Crypto Assets Regulations in EU Countries ..... 93
6.2.1 Germany ..... 93
6.2.2 Malta ..... 97
6.2.3 France ..... 99
6.2.4 Italy ..... 101
6.2.5 Spain ..... 102
6.2.6 Ireland ..... 103
6.2.7 Summary ..... 104
6.3 Illicit Activities of Crypto Assets in the EU ..... 105
6.3.1 Transnational activities ..... 105
6.3.2 Anti-Money Laundering in the EU ..... 106
7 Thesis Conclusions, Implications and Limitations ..... 110
7.1 Thesis Conclusions ..... 110
7.2 Research Implications ..... 113
7.3 Limitations and Further Development ..... 115
Bibliography ..... 118
Acts ..... 118
Regulations ..... 119
Cases ..... 122
Books ..... 122
Journal Articles ..... 123
Working Papers ..... 125
Conferences and Seminars ..... 128
Websites ..... 128

# List of Abbreviations

| Abbreviations | Terms/ organisations |
|---|---|
| AI | Artificial Intelligence |
| AMF | Financial Markets Authority of France |
| AML | Anti-Money Laundering |
| API | Application Programming Interface |
| ATM | Automatic Telling Machine |
| BaFin | Federal Financial Supervisory Authority |
| BCOBS | Banking: Conduct of Business sourcebook |
| BIS | Bank for International Settlements |
| BoE | Bank of England |
| CBCC | Central Bank Crypto-Currency |
| CBI | Central Bank of Ireland |
| CCAs | Convertible crypto assets |
| CONSOB | Companies and Stock Exchange Commission of Italy |
| DCMs | Designated Contract Markets |
| DLT | Distributed Ledger Technology |
| DRSR | Data Reporting Services Regulations |
| EBA | European Banking Authority |
| EC Directive | Privacy and Electronic Communications Directive |
| EC* | European Commission |
| EEA | European Economic Area |
| EMD | Electronic Money Directive |
| E-Money | Electronic Money |
| EMR | Electronic Money Regulation |
| ENISA | European Union Agency for Network and Information Security |
| ESA | European Supervisory Authorities |
| ESMA | European Securities and Markets Authority |
| EU | European Union |
| Europol | European Union Agency for Law Enforcement Cooperation |

| | |
|---|---|
| FATF | Financial Action Task Force |
| FCA | Financial Conduct Authority |
| FinCEN | Financial Crimes Enforcement Network |
| Fintech | Financial Technology |
| FIUs | Financial Intelligence Units |
| FSMA | Financial Service and Markets Act |
| GFIN | Global Financial Innovation Network |
| HMT | Her Majesty's Treasury |
| ICAEW | Institute of Chartered Accountants in England and Wales |
| ICO | Initial Coin Offering |
| IMF | International Monetary Fund |
| IOSCO | International Organization of Securities Commissions |
| ITAS | Innovative Technology Arrangements and Services Act |
| JMLSG | Joint Money Laundering Steering Group |
| MAR | Market Abuse Regulation |
| MDIA | Malta Digital Innovation Authority |
| MiFID | Markets in Financial Instruments Directive |
| MLR | Money Laundering, Terrorist Financing and Transfer of Funds Regulations |
| NCA | National Crime Agency |
| NIS | Network and Information Systems |
| OECD | Organisation for Economic Co-operation and Development |
| PERG | Perimeter Guidance manual |
| POC | Proceeds of Crime Act |
| PRIIPs | Packaged Retail and Insurance-based Investment Products |
| PRIN | Principles for Business |
| PSD | Payment Services Directive |
| PSR | Payment Services Regulation |
| RAO | Regulated Activities Order |
| RBA | Risk-Based Approach |
| REC | Recognised Investment Exchanges |

| | |
|---|---|
| RegTech | Regulatory Technology |
| SEROCU | South East Regional Organised Crime Unit |
| SMCR | Senior Managers and Certification Regime |
| UK | United Kingdom |
| UN | United Nations |
| US | United States of America |
| VFA | Virtual Financial Assets Act |

# 1 Introduction and Overview

## 1.1 Research Questions

Information technology[1] has developed rapidly over the past a few decades alongside the popularity of the internet. Information technology allows a fast distribution of digital products and services through the internet while reducing the cost of geographical business expansion for firms. The possibility of wider business expansion and higher expectations of profitability have made the information technology becoming a popular investment objective. Many industries see the use of information technology and big data as the next step in maintaining their market power and strengthening competitiveness, and this is particularly true for the banking and financial sector. Some financial institutions have adopted information technologies in their managerial systems, product lines and customer services and other financial institutions are following close behind. The application of information technology in the financial industry is commonly referred to as Financial Technology or FinTech.[2]

The development of Fintech has yielded positive impacts on many aspects within and beyond the financial industry. For instance, crypto payments and crowdfunding methods that are

[1] Information technology refers to 'highly refined processes are introduced with little attendant use of advanced technology or radical approaches to human resource management. They simply are logical, balanced, and streamlined. The goal of information engineering is to describe an already conceptualised process in information (or, more accurately, data-oriented) terms so that a system can be rapidly and rigorously constructed to support the new process design'. Thomas H Davenport, *Process Innovation: Reengineering Work Through Information Technology* (Harvard Business School Press 1993). at pp. 3 and 49.

[2] Information technology provides a comprehensive application in the financial sector and brings improvement to optimising process efficiency with data driven. Financial institutions include capital markets, insurance companies and large banks, tend to implement information technology to their managerial and operational systems. The value proposition of information technology in the financial sector are 'Application Integration; complexity reduction; reuse; cost; and economic flexibility/differentiation'. Detlef Seese, Christof Weinhardt and Frank Schlottmann (eds), *Handbook on Information Technology in Finance.* (Springer-Verlag 2008). at pp. 17 - 18.

underpinned by the Blockchain[3] and the Distributed Ledger Technology (DLT),[4] which makes transactions more efficient, economical, secure and transparent.[5] Authorities also benefit from the development of information technology; examples include Regulatory Technology (RegTech)[6] that aims to enhance the process efficiency of market oversight, reporting and compliance.

The authorities in the UK and the EU have established regulatory frameworks pertaining to the regulations of crypto assets, which is a notable product of Blockchain. This new-born product carries combined characteristics consisting of virtual property and financial products. It can be adopted in payment transactions, financial instruments, investments and corporate coupons. Other than the sophisticated features of crypto assets, more concerns are laid on the anonymity

[3] 'A blockchain is a distributed system for recording and storing transaction records. More specifically, blockchain is a shared, immutable record of peer-to-peer transactions built from linked transaction blocks and stored in a digital ledger. Blockchain relies on established cryptographic techniques to allow each participant in a network to interact (e.g. store, exchange, and view information), without pre-existing trust between the parties. In a blockchain system, there is no central authority; instead, transaction records are stored and distributed across all network participants. The three design principles of blockchain and distributed ledger technology listed below make the technology a perfect fit for public services'. Blockchain is alleged to be: (1) Transparency and Privacy; (2) Security and Reliability; (3) Trust and Integrity'. Craig Holloway, 'State of Illinois: Request for Information (RFI) Distributed Ledger and Blockchain Applications in the Public Sector' (2017) < https://www2.illinois.gov/sites/doit/Documents/BlockchainInitiative/RFI+Blockchain+and+Distributed+Ledger+Applications+in+the+Public+Sector.pdf > accessed 5 January 2020. at pp. 3 - 4. I provide an overview of the properties of the DLT, Blockchain and crypto assets in Chapter 2 of this thesis.

[4] The term distributed ledger technology or DLT refers broadly to distributed network technology that '(1) enables users to upload programs and to leave the programs to self-execute; (2) maintains a permanent and public record (ledger) of the current and past states of every program; (3) is distributed; (4) uses public key cryptography for authentication; and (5) uses a consensus mechanism to ensure that the network maintains the technology'. Carla Reyes, 'Conceptualizing Cryptolaw' (2017) 96 Nebraska Law Review. at p. 8.

[5] "Transparent" is used to define the nature of the distributed ledger to cover both permission-less and permissioned ledgers. Permission-less refers to the open source DLT or public ledgers, open for anyone to inspect. 'Many states that open-source software is less vulnerable and more resilient than proprietary software, because the development of the software is transparent, and since more eyes are looking for bugs, more bugs will be noticed and fixed'. Angela Walch, 'The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk' (2015) 18 New York University Journal of Legislation & Public Policy. at pp. 40 - 41.

[6] For example, the FCA has established a department of RegTech in 2017 intending to introduce information technology with data driven in market oversight and consumer protection. See 'RegTech | FCA' (2017) <https://www.fca.org.uk/firms/innovation/regtech> accessed 26 March 2020.

of user information on peer-to-peer networks that the technology offers. Given the fact that regulatory attention has followed roughly a decade later than the technological development,[7] the sufficiency and effectiveness of current regulatory regimes require a thorough examination, which this thesis intends to do.

This thesis analyses the regulatory status of crypto assets in the UK and the EU. It does so by particularly focusing on three research questions. The first research question considers whether the current regulatory perimeters of the FCA (Financial Conduct Authority) are sufficient to clarify and classify the crypto asset markets in the UK in line with the missions of consumer protection and market integrity. In addressing this question, this thesis will examine the effectiveness of the current regulatory perimeters in the UK. As one of the biggest financial markets in the world,[8] UK financial regulations can be a weathervane for other financial markets. Clearly elaborated regulatory policies assist firms to set up an appropriate process for compliance and to establish their business models. Also, clear regulatory policies guide consumers on their decision making. In addition, the classification of crypto assets manifests the opinions of the UK regulators, and this can be a signal to direct the future innovation and development of technology in the financial sector.

The second research question examines what actions are needed to develop an effective and properly functioning EU-wide regulatory crypto asset policy. This question is vital due to the universal use of crypto assets on the internet. Divergent regulations or regulatory opinions on

[7] For example, the regulatory framework in the UK was finalised in July 2019 whereas Bitcoins were conceptualised in 2008. The regulatory framework came into being 11 years later than the technology initialisation.

[8] The Global Financial Centres Index is a ranking of the competitiveness index among 120 financial centres. The index is produced by Y/Zen (a City of London's leading commercial think-tank) and CDI (China Development Institute) since 2007. The ranking is an aggregate of indices from five key areas: "business environment", "financial sector development", "infrastructure factors", "human capital", "reputation and general factors". As of March 2020, London was ranked the second largest and competitive financial market in the world after New York. Financial Centre Futures, 'The Global Financial Centres Index 27' (2020) < https://www.longfinance.net/media/documents/GFCI_27_Full_Report_2020.03.26_v1.1_.pdf> accessed 30 March 2020.

crypto assets among EU member states[9] leads to inconsistency in national laws which works against the implementation of EU regulations under the single market system.[10] The economic situation across EU member states is variable and the diversified economic environment leads to gaps in responding to the EU regulations. Such gaps may take place in the implementation schedules or common understanding of initiatives.[11] In the situation of crypto assets, some EU members regard this as an opportunity to attract new investment and economic growth; for instance, Germany, Malta and France whereas other EU countries, such as Ireland, see this harmful to the financial markets on the ground of consumer protection. There are also some countries holding a neutral viewpoint in respect to crypto assets and may only work on regulatory policies in the future when markets become more mature. Moreover, the unbalanced economic and financial status within the EU,[12] together with the different structures of the historically established regulatory databases among EU countries incur difficulties and obstacles in creating unified recordkeeping and reporting regulatory system in the EU. Therefore, it is a major challenge to establish a harmonised legal system in the EU in relation to crypto assets.

[9] The financial regulatory agencies in EU countries hold different opinions on the crypto asset businesses and products. For example, Malta has permitted payment types of crypto assets, Germany hasn't allowed e-money type of crypto assets, the UK includes e-money type of crypto assets in the regulatory perimeters, Ireland is cautious about crypto assets businesses and produces, etc. This thesis provides a detailed discussion in Chapter five and Chapter six.

[10] The single market system allows free movement of goods and services within the EEA member states and financial services and e-commerce are included in the system. European Commission, 'The European Single Market | Internal Market, Industry, Entrepreneurship and SMEs' <https://ec.europa.eu/growth/single-market_en> accessed 5 November 2019.

[11] Countries in different level of technology and economy may understand crypto assets differently.

[12] 'Economic Performance by Country | European Commission' <https://ec.europa.eu/info/business-economy-euro/economic-performance-and-forecasts/economic-performance-country_en> accessed 25 March 2020.

The third research question investigates how the Laws and Acts could possibly apply to crypto assets when it comes to financial crime.[13] Crypto assets create a channel allowing technological firms to participant in the financial markets. Those technological firms are regulated by general laws and regulations in terms of business practices and commercial activities. However, they do not fully follow the financial regulation requirements of financial firms and financial institutions. For example, the requirement of recordkeeping and suspicious transaction reporting. In addition, online financial crimes may occur to individual crypto asset accounts without an involvement of third parties, such as banks. This situation makes consumers more vulnerable to cyberattack. Furthermore, although crypto assets activities are mainly the internet-based, there are offline illicit activities taking place using crypto asset as a means of value transactions. The multi-faceted properties and market positions of crypto assets indicate that those related illicit activities may have to be examined under different laws, which include but not limited to criminal laws, information technology laws and anti-money laundering regulations.

Through a careful and critical examination of the abovementioned questions, the thesis provides first a thorough discussion of the regulatory frameworks of crypto assets in the UK and other EU member states, respectively; second, a critical analysis of the ambiguity in the current regulatory regimes in the UK; third, an assessment of the regulatory inconsistencies between the EU laws and national laws among EU member states; and finally, this thesis will give examples of the application of laws and regulations in terms of financial crimes.

[13] '"Financial crime" includes any offence involving— (a) fraud or dishonesty; (b) misconduct in, or misuse of information relating to, a financial market; or (c) handling the proceeds of crime'. The Financial Services and Markets Act 2000 c. 8. s.6 (3); Financial crime is a broad concept that includes money laundering, terrorist financing, fraud, tax evasion and corruption or in the broadest context, 'any type of illegal activity that results in a pecuniary loss'. Financial crime 'has the power to corrupt and destabilise communities or whole national economies'; it threats financial systems and national security and erodes the integrity of national financial institutions. Nicholas Ryder, *Financial Crime in the 21st Century : Law and Policy* (6th edn, Edward Elgar 2011). notes 6, 14 - 17. at pp. 2 - 3.

## 1.2 Research Objectives

Crypto assets have become a controversial topic in the financial sector and academia.[14] Crypto assets have attracted substantial attention because of the debatable techniques that provide anonymous value transactions and have created a channel allowing technology firms to enter financial markets. While crypto assets are new to the financial sector, the underpinning technology (DLT) has existed for around two decades since the 2007 financial crisis and within the technology field. Although the technology was banned previously due to protection of copyright in the music industry,[15] the ideas of sharing information freely and anonymously have been well received by large numbers of online users. Eventually, this technology has made a comeback and become popular under the developments of information technology and the internet. However, the cross-cutting fields of crypto assets that consist of information technology and finance bring fundamental changes and challenges to financial markets, which urges regulatory agencies to adopt prudent policies and catch up with the new technology developments. On the one hand, strict regulatory policies may impede technological innovation and churn investors and innovators to other countries, while on the other hand, loose regulations may place investors and consumers in a vulnerable position.

This thesis aims to analyse the effectiveness of current regulations in the UK and the EU on the use of crypto assets. It considers also the legal Acts relating to the use of crypto assets in financial crimes. Additionally, the analysis of the regulatory status in the UK is set out separately because of its leading position on global financial markets and the situation of the EU Withdrawal in January 2020.

The existing Regulations and Directives on crypto assets in the UK and the EU are supposed to enable consumer protection and market integrity in terms of commercial activities, such as

[14] As explained in Section 1.1 of this thesis, the DLT is alleged to improve process efficiency and transparency of financial transactions, however, it leads to decentralised networks challenging the role of intermediation of banks and financial institutions. The technology and the usage of crypto assets and DLT makes them an interdisciplinary topic that cover Information Technology, Business, Finance and Law as well as Data protection. Some fields may find DLT very beneficial, such as Information Technology, Business, as it improves efficiency and transparency; Some fields may find it challenging when prudent regulations are yet present.

[15] Peer to peer networks have become popular in the financial sector. The technology was originally developed in the music industry and banned because it allowed permission-less and free downloading and sharing of music through a peer-to-peer network on the internet. This permission-less downloading and sharing did not verify the copyrights of the music. Steven David Brown, 'Cryptocurrency and Criminality' (2016) 89 The Police Journal: Theory, Practice and Principles, 327 - 339. See further discussions in Chapter 2 of this thesis.

investment and trading. There are also individual/non-business groups carrying out wrongdoings using crypto assets as a means of intermediation. For instance, online stealing and financial fraud. Given the multi-faceted characteristics of crypto assets, such wrongdoings cannot be simply identified under the laws applied to financial markets alone. Laws that apply to other illicit activities may apply to crypto assets wrongdoings, such as the Computer Misuse Act 1990[16] and the Serious Crime Act 2007[17] of the UK (see detailed discussion of this thesis, Section 5.4 Illicit activities of crypto assets in the UK).

Therefore, this thesis intends to highlight the importance of monitoring the non-commercial wrongdoings associated with crypto assets beyond the supervision of commercial activities. The clarified applicable Laws and Acts may assist in financial crime prevention. The thesis discusses some arrests and cases of crypto assets wrongdoings and court judgements taking place the UK and EU[18] to analyse the possible Laws and Acts that may be applied against those violations. In the context of the complicated roles of crypto assets in financial markets, the main purpose of this analysis focuses on identifying the roles of crypto assets in financial crimes and analysing the rationale behind the adaptation of those Acts. In the meantime, clearly classified illegal activities in relation to crypto assets may help to raise the awareness of potential financial crimes. The analytical outcomes may assist in updating the relevant legal provisions in the future.

In addition, the thesis covers the background of the development and evolution of crypto assets markets and the impact of information technology on financial markets. This helps to understand the incentives behind using crypto assets products and services and identifying weaknesses in the current regulatory frameworks. The progressive developments of information technology and the internet are the foundations of the crypto assets establishment and bring out its popularity in financial markets. Thoroughly analysing and interpreting the regulatory structures of crypto assets and related Laws and Acts adopted by the authorities in the UK shall shed some light on the clarity of the current regulatory framework. This is expected to assist authorities to identify the strengths and weaknesses in the regulatory regime.

In the meantime, an in-depth discussion on crypto asset regulations among EU member states may give an impression on the effects of the diverse regulatory opinions on crypto assets

[16] Computer Misuse Act 1990 c. 18.

[17] Serious Crime Act 2007 c. 27.

[18] See Section 5.4 and 6.2.1 of this thesis.

regulation (see Chapter Six, Regulation of crypto assets in the EU) and the single market system within the EU. The discussion also intends to identify the regulatory obstacles and challenges in the existing regulatory regimes among the EU countries, for example, information sharing.

Another research objective of this thesis is to clarify the official opinions of central banks on issuing Central Bank Crypto-Currencies (CBCCs). Crypto assets are considered an alternative to paper-based banknotes in industries with the ability to create a decentralised financial system that is more efficient and secure.[19] Such assumptions challenge the power of national central banks and even threaten financial stability. Some countries have not yet accepted crypto assets products and services like Spain whereas some authorities like Malta are encouraging financial inclusion (see Section 6.2.2 and 6.2.5 of this thesis). It is understandable that countries may decide whether to adopt crypto assets into their financial system based on national economic situations and market structure. However, the diverse opinions of crypto assets regulation among global financial markets may incur information asymmetry and further lead to uncertainty in the financial markets. People with speculative intentions may take advantages from others by using asymmetric information and gaming with the regulatory system. For example, distributing rumours to manipulate stock prices or falsify CBCC issuance to deceive investors and consumers for their own benefit.[20] Therefore, clarifying current plans and opinions of central banks on CBCCs is a main priority to ensure market stability. Additionally, identified benefits and potential harms of issuing CBCCs may contribute to enhancing the soundness of the financial system.

## 1.3 Research Methods

For the purpose of analysing the effectiveness of the Fintech regulations, particularly on crypto assets, in the UK and the EU, this thesis will employ both the theoretical and comparative methods are essential to carry out the research. Crypto assets are chosen as a representative of Fintech products due to their rapid growth and global influences and the diverse regulatory schemes on them across EU member states.

The theoretical analysis in this thesis focuses on two main aspects: the regulation of crypto assets and illegal activities relating to crypto assets. The regulation of crypto assets is relevantly

[19] Decentralisation refers to a system that has no central authority to control it. Walch (n 5). at p. 7.

[20] News about China's central bank issuing CBCCs in 2019 was found false. See detailed discussion in 4.2 of this thesis.

new given the fact that crypto assets started to draw the attention of national authorities only in recent years. For instance, the UK only finalised its first regulatory guidance in July 2019. In addition, financial crimes in relation to crypto assets are normally connected to other illegal activities and present a complicated pattern on global networks. Besides, since most of the accessible case judgements are in the US, case judgements involving crypto assets in the UK and the EU are sparse, which serves as further motivation for this thesis to consider such cases.

Therefore, this thesis tries to classify the roles that crypto assets play in the financial sector and their effect on both the commercial and non-commercial activities in relation to financial wrongdoings. By doing so, the thesis first, provides an overview of the evolution of crypto assets, including the technological background, the official definitions in different countries, academic discussions and the illicit activities relating to crypto assets. Second, the thesis reviews the developments of the money laundering regulations in the UK and EU as well as the international standards and recommendations of the Financial Action Task Force (FATF). This covers the establishment of money laundering in the UK and the EU, as well as the roles of crypto assets in global money laundering activities. Third, the thesis analyses the structure of the current regulatory frameworks in the UK and some EU countries and identifies the relevant Laws and Acts that apply to the regulations. Under a thorough theoretical analysis, this thesis is then able to establish the foundation for further comparative analysis.

Comparative legal research is classified as the functional method, the structural method, analytical method, the law-in-context method, the historical method and the common-core method. Of which the common-core method is often a combination of the functional method and analytical method. The functional method focuses on the similarity or differences of legal/social results rather than legal approaches between legal systems. The analytical method identifies if 'the subdivisions of a legal concept or field is in a logic, systematic, succinct, and complete way'.[21]

The functional method deems that some laws are structured under similar legal concepts no matter what the legal systems and legal cultures are.[22] For instance, identifying rights, resolving conflicts and preventing crimes. These types of legal concepts are similar across countries and legislative systems meant to secure rights and justices and punish wrongdoings. Therefore, the

[21] Mark Van Hoecke, 'Methodology of Comparative Legal Research' [2016] Law and Method 279.

[22] Oliver Brand, 'Conceptual Comparisons: Towards a Coherent Methodology of Comparative Legal Studies' [2007] Brook J Int'l L 405.

functional method compares the effectiveness of laws rather than the legal systems between countries.[23]

The functional method allows researchers to examine similarities and differences of the laws among EU member states in terms of their effectiveness without consulting the entire legal systems of those countries. On the one side, the legislation system of the EU is structured under a mutual agreement of member states, thus, each member country is required to implement EU laws into national laws. Under this structure, the legal system of each EU member state is a combination of national law and EU law. On the other side, divergence occurs as the implementation time frames and approaches of EU laws rely on the existing legal systems of each EU member state, which differ from one state to another.[24] Thus, EU law implementation is more result-driven rather than process-driven. In addition, the results of EU law implementation may also be affected by the capabilities and the financial constraints of national authorities.

The functional method makes the comparative law applicable to examine the effectiveness of the laws in different financial systems and legal cultures. Siems and Deakin[25] adopt the functional method to analyse the impact of laws on the financial sector in countries that have different economic scales and legal systems, including the EU countries, the US and some emerging countries. Given the fact that Fintech, particularly crypto assets, has spread rapidly worldwide within a short period, the relevant laws and regulations in most of countries are still at their initial phases. Besides, the laws and regulations of the financial sector mainly focus on commercial activities, while the legal concepts and purposes of commercial activities are fairly similar from one country to another. For example, protecting property rights and facilitating market integrity. Thus, the common-core method that contains both the functional method and the analytical method is more appropriate for evaluating the effectiveness of crypto assets regulation in the UK and the EU.

[23] David Nelken, 'Comparative Legal Research and Legal Culture: Facts, Approaches, and Values' [2016] Annual Review of Law and Social Science 45.

[24] 'Applying EU Law | European Commission' <https://ec.europa.eu/info/law/law-making-process/applying-eu-law_en> accessed 25 March 2020.

[25] Mathias Siems and Simon Deakin, 'Comparative Law and Finance: Past, Present, and Future Research' [2010] Journal of Institutional and Theoretical Economics 120.

Therefore, the thesis first, applies the functional method to examine the effectiveness of the crypto asset regulations in the UK and some EU countries that have and have not established the regulations on crypto assets. The comparison of laws focuses on regulations of commercial activities and possible wrongdoings of individuals or groups of criminals, particularly money laundering activities. Such a comparison provides insight into the feasibility and practicability of current regulations and applicable Acts in EU countries. This thesis carries out the evaluation of the effectiveness of crypto assets regulation in the UK, separately, due to its important position as a global financial hub and the situation of EU Withdrawal.

Second, this thesis applies the analytical method to examine the consistency of the current regulations of crypto assets in terms of commercial activities. The rapid developments of Fintech have added complexity to current regulatory schemes in many countries. On the one hand, authorities are the main bodies responsible to ensure financial stability, market integrity and consumer protection. Thus, strict regulations may be a straightforward solution. On the other hand, authorities are obliged to facilitate financial innovation and market competition and to attract investments and start-ups. Therefore, financial inclusion and market deregulation may be used as a vehicle to achieve these regulatory objectives. Under this situation, inconsistency may occur in regulatory schemes when the authorities are trying to balance the market regulation and financial inclusion. By applying the analytical method, this thesis carries out extensive discussion to identify the potential inconsistencies in existing regulatory schemes and to determine if there are loopholes in the existing regulatory frameworks.

In summary, the thesis applies for theoretical methods and comparative analysis to evaluate the effectiveness and consistency of the laws and regulations in the UK and the EU with respect to both commercial activities and non-commercial crimes in relation to crypto assets. Of which, the theoretical analysis provides a comprehensive review of the background and the impact of crypto assets in the financial sector and the regulatory regimes of both commercial and non-commercial, as well as the Acts that may be applicable to financial crimes. Additionally, the common-core method (one of the comparative methods) that embodies the functional method and the analytical method allows a coherent examination of the effectiveness and consistency of the current regulations under the different legal structures of the EU member states. Both the theoretical method and comparative method are indispensable to one another to establish the analytical framework of the thesis. The theoretical analysis builds the foundation of the comparative research of the thesis and the comparative method carries out the critical analysis.

Meanwhile, both the methods work collectively to generate research impact and bring out the research implications.

## 1.4 Research Scope

This thesis analyses the effectiveness and consistency of the current regulations and laws in the UK and the EU in terms of financial innovation, particularly, crypto assets and related activities. The EU is the second-largest market of crypto assets businesses in the world after the US with EU countries demonstrating a complicated legal structure combining national laws and EU laws. The UK and six EU countries are chosen to be representative countries for a comparative evaluation. The UK possesses a unique position as the central hub of the global financial markets and the EU embodies diverse regulatory schemes and different legal systems amongst the EU member states.

In order to compare the different regulatory schemes of crypto assets in the EU and carry out critical analysis, I select six economies that represent three stages of the regulatory scheme, cognitive stage, preparatory stage and development stage. The cognitive stage refers to countries that recognise the new financial product whereas are not ready to react to it; the preparatory stage consists of countries that are in progress of consulting the regulatory schemes; and the development stage includes countries that have established a well-developed regulatory framework. The six EU economies are Germany, Malta, France, Italy, Spain, and Ireland. Of which, Germany and Malta have adopted Acts and Laws to regulate crypto asset businesses; France and Italy are in the stage of establishing the regulatory schemes of crypto assets businesses; Spain and Ireland have acknowledged the new financial products and the potential effect, whilst have not yet shown incentives to establish relevant regulatory schemes.

The thesis utilises two analytical categories to carry out a comprehensive assessment. The first category is the legislative basis of crypto asset business regulations, including relevant primary and secondary legislation. The second category is the Laws and Acts applicable to financial violations in terms of crypto assets. Of which, the primary and secondary legislation that establishes the regulatory schemes of crypto assets focus on commercial activities, such as product classifications, business registrations and due diligence measures for anti-money laundering regulations. The Acts applicable to financial violations refer to non-commercial activities in relation to crypto assets, for example selling prohibit goods or online stealing.

Based on the first research category, the thesis will provide a detailed discussion about the current regulatory structures of crypto assets in the UK and selected EU countries. The thesis

firstly interprets the Primary and Secondary legislation adopted by authorities for crypto asset regulation, such as Acts and Regulations in the UK and some EU countries, as well as Directives in the EU. Crypto assets regulations in the UK are directly adopted from applicable Acts and Regulations, for example, the primary legislation, the Financial Services and Markets Act 2000[26] and the secondary legislation, the Regulated Activities Order (RAO) 2001.[27] Crypto assets regulations in the selected EU countries demonstrate different approaches. For instance, the crypto assets regulations in Germany are adopted directly from updated Laws, like the Banking Act 2014;[28] Malta has established Acts to regulate crypto assets products and services including the Innovative Technology Arrangements and Services Act 2018.[29] Through detailed discussion, the thesis assesses if the applicable Laws and Acts are sufficient to regulate crypto asset activities in the UK and the EU countries and if the established regulations are effective and consistent. In the meantime, the thesis evaluates the possible causes of the inconsistency and ineffectiveness in terms of crypto asset regulations.

In the second research category, the thesis identifies possible wrongdoings relating to crypto assets activities. These include individuals or grouped criminals of non-commercial activities. The analysis gives insight into the types of illicit activities that crypto assets could be used and how crypto assets may assist with. The analysis mainly focuses on the anti-money laundering in the UK and EU, respectively, and assesses the related financial crimes using the UK as an example, such as online stealing and selling prohibited goods. The analysis breaks down the processes of unlawful activities that may involve crypto assets, particularly money laundering activities, and provides comprehensive discussions on applicable Acts in the UK, such as the Computer Misuse Act 1990,[30] the Forgery and the Counterfeiting Act 1981.[31] In addition, the thesis employs several crypto asset related case studies to discuss the use of relevant legal provisions, although both the reported crypto asset crimes and published official judgements in the UK and the EU are sparse. Even though there have been two reported arrests in the UK and EU in relation to non-commercial crypto asset crimes, including online stealing, fraud and money laundering, official judgements have not yet been made public at the time of writing.

[26] The Financial Services and Markets Act 2000 c. 8.

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

[28] 'Banking Act (KWG)' [2014] Bundesgesetzblatt.

[29] The Innovative Technology Arrangements and Services Act 2018.

[30] Computer Misuse Act 1990 c. 18.

[31] Forgery and Counterfeiting Act 1981 c. 45.

So far, only one case judgement relating to commercial activities of crypto assets has been made public in Germany.[32] Due to limited sources of analytical material, I provide discussion about the relevant UK Laws and Acts that possibly apply to crypto asset crimes based on their use in traditional financial crimes. The official webpage of the Crown Prosecution Service on cybercrimes is used as a reference.[33]

One must be aware that although each country can freely set up its own regulatory framework, the unlawful activities in relation to crypto assets are an international matter. Information technology and the internet together with the anonymous transaction networks of crypto assets create a convenient conduit allowing illicit earnings to move around the globe. By virtue of the fact that crypto asset related financial crimes are likely an internet-based and transnational matter, the discussions of the activities in violation of Laws and Acts relating to crypto assets have to involve other countries for the purposes of comparison. For instance, the United States of America, which is the origin and the seedbed of crypto assets products and services, as well as the technology that underpins it. The discussion also considers those countries that are involved in grouped multinational financial crimes. For instance, the Japanese crypto assets markets have been used as a platform of money laundering by international criminals since 2017.

Moreover, the thesis talks over the benefits and potential risks of Central Bank Crypto Currencies (CBCCs) and the current plans of the central banks to issue CBCCs. The potential to develop an alternative to paper-based banknotes internationally and to decentralise the current financial and banking system is the main reason that crypto assets have been attracting the attention of the authorities. Although almost all countries have declared that crypto assets are not legal tender and they have no plans to issue CBCCs, the popular use of crypto assets in the industry and financial markets may force traditional banks to take part. Meanwhile, some visible advantages of crypto assets may benefit banking regulation in the future. Therefore, central banks have not yet ruled out the possibilities of issuing CBCCs. Actually, some central banks have started to carry out relevant research and discussion. For example, the Bank of

[32]'Citizen Service Berlin - Brandenburg - Criminality of Trade in Bitcoins' (2019) <http://www.gerichtsentscheidungen.berlinbrandenburg.de/jportal/portal/t/279b/bs/10/page/sammlung.psml?pid=Dokumentanzeige&showdoccase=1&js_peid=Trefferliste&documentnumber=1&numberofresults=1&fromdoctodoc=yes&doc.id=KORE223872018&doc.part=L&doc.price=0.0> accessed 8 December 2019.

[33] The Crown Prosecution Service (n/d), 'Cybercrime - Prosecution Guidance' <https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance> accessed 23 April 2019.

England published a discussion paper in March 2020 inquiring the public opinions on central bank cryptocurrency; while one country, Venezuela, has published a whitepaper regarding its own government cryptocurrency against crude oil in 2018 to eliminate the pressure of its currency depreciation under the economic sanctions by the US.[34]

The thesis is structured as follows: chapter two provides an overview of the background and the market status of the DLT and crypto – assets, including related illicit activities and the evolution of the anti-money laundering regulations from a global point view; chapter three provides an overview of the anti-money laundering regulation in the UK and the EU and analyses the role of crypto-assets in global money laundering; Chapter four expounds the so-called decentralisation of the financial markets caused by crypto assets and discusses the benefits and potential risks that cryptocurrency may bring to the central banks; chapter five analyses the regulatory frameworks and the legal systems in relation to both commercial and non-commercial crypto asset activities in the UK; chapter six extends the analysis to the overall EU regulations and national regulations of six representative EU countries; and chapter seven presents the thesis conclusions, implications and limitations.

## 1.5 Research Outcomes

This thesis provides an in-depth analysis of existing regulations of crypto assets in the UK and the EU. The thesis is one of the first research that examines literature and working papers in an interdisciplinary way encompassing studies in Computer Science, Business, Finance and Law. The thesis is one of the earliest investigations that examine the effectiveness and consistency of the existing regulation on crypto assets in the UK and it is among the first moves to identify the harmonisation and consistencies of the regulatory frameworks of crypto assets in the EU. It looks into the legal provisions applied by existing regulatory perimeters and analyses the possible effects on consumers and commerce as well as on financial markets. The thesis also

[34] 'Due to the imposition of the US dollar as the international backing currency and the subsequent replacement of the gold standard with the fiduciary model, the world economy has suffered from uncertainty and instability caused by the foundation in a currency without a gold backing, which has been particularly harmful to emerging economies … Petro (PTR) will be a sovereign crypto asset backed by oil assets and issued by the Bolivarian Republic of Venezuela on a blockchain platform. Its launch will spearhead the promotion of an independent, transparent digital economy, open to direct citizen participation, which will serve as a platform for the development of crypto assets and innovation in Venezuela and other emerging countries with great potential'. 'Venezuela Petro Cryptocurrency (PTR)--English White Paper' [2018] Gobierno Bolivariano de Venezuela. at pp. 1 and 4.

provides original analysis to pinpoint specific Laws and Acts that are applicable to crypto assets crimes with up-to-date case studies, including anti-money laundering. In the meantime, the thesis clarifies the current plans and potential risks of central banks on issuing Central Bank Crypto Currencies.

The cutting-edge technology – the Distributed Ledger Technology (DLT) is taking the financial industry into a new digital era. The DLT offers crypto assets a unique feature combining the technology and financial sectors and opens a door for technology firms stepping into the financial industry.

Looking into the regulation of crypto assets in the UK, the thesis traces the regulatory roadmap of the UK regulatory regime of the Bank of England (BoE), Her Majesty's Treasury (HMT) and the Financial Conduct Authority (FCA). The FCA has taken the responsibility of regulating commercial activities of crypto assets in the UK[35] and anti-money laundering measures in accordance with the EU Fifth Anti-Money Laundering Directive[36] effective until December 2020[37] and with the MLR 2019 (EU Exit)[38] afterwards. Meanwhile, non-commercial illicit activities in relation to crypto assets are regulated accordingly under relevant Regulations and Acts.[39]

The thesis discovers that the UK regulation on commercial activities in relation to crypto assets is less effective in some ways and it is more complicated than some European economies that studied by this thesis. The UK regulatory framework of crypto assets focuses on product types applications rather than business entities. This regulatory framework is rather complicated and inflexible under the rapid technology development of financial innovation. This regulatory complexity may lead to UK firms mistakenly identify the regulatory status of their token businesses and face increasing managerial costs, such as implementing new compliance measures and relevant staff training. The misidentified information may be further passed on consumers and affect their decisions.

[35] FCA, 'Guidance on Cryptoassets Feedback and Final Guidance to CP 19/3' (2019) PS19/22.

[36] The Money Laundering and Terrorist Financing (Amendment) Regulations 2019, SI 2019/1511.

[37] The Money Laundering and Transfer of Funds (Information) (Amendment) (EU Exit) Regulations 2019, SI 2019/253.

[38] ibid.

[39] The Crown Prosecution Service (n 33).

Additionally, the thesis discovers three loopholes in the existing regulations in the UK in terms of crypto asset. The first loophole is found in Regulation 76 of the Regulated Activities Order (RAO) 2001.[40] Regulation 76 is the main provision applied by the Final Guidance paper of the FCA to identify if crypto assets fall within the regulatory perimeters of security tokens.[41] However, the Regulation gives an equivocal definition of specified investments. The equivocal definition of specified investment can lead to some crypto asset products categorised into both regulated and unregulated tokens at the same time. This inconsistency is anticipated to place difficulties in the processes of prosecution and judgement when dealing with security token cases in the UK.

The other two loopholes are caused by the conflict between the UK regulatory frameworks and the EU Single market system. There are exemptions for firms registered in the EU to comply with certain regulatory requirements under the Carrying on Regulated Activities by Way of Business in the UK.[42] One loophole allows EU firms to provide products and services of unregulated tokens in the UK with licences issued in another EU member state. Another loophole is the relaxed regulatory requirements for EU firms operating in the UK through the internet.[43] All overseas entities providing goods and services to UK residents are required to comply with the Carrying on Regulated Activities by Way of Business in the UK regardless of their registration and operation venues.[44] This in principle shall cover internet-based crypto assets businesses, such as online trading platforms, exchanges and digital custody wallets. However, these regulatory requirements are lifted for EU firms under the single market system according to the PERG[45] of the FCA.

The three loopholes in the existing crypto assets regulation are assumed to puzzle firms, developers and investors to identify their market positions and carry out business compliance. And these loopholes may be used by speculators to game with the financial system and further jeopardise market integrity and weaken consumers protection.

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

[41] FCA, 'Guidance on Cryptoassets Feedback and Final Guidance to CP 19/3' (n 35).

[42] FCA, 'The Perimeter Guidance Manual' (2019).

[43] See detailed discussion in Section 5.2 of this thesis.

[44] FCA, 'The Perimeter Guidance Manual' (n 42). See detailed discussion in Chapter 5 of this thesis.

[45] ibid. See detailed discussion in Chapter 5 of this thesis.

The regulations of crypto assets within the EU are somewhat less harmonised. The only unified understanding within EU member states is that crypto assets are neither legal tender nor units of accounts. Other than that, the EU regulatory frameworks on crypto assets exhibit differences across member countries. For example, crypto assets are recognised as financial instruments for investment, trading and exchange (except e-money and payment instruments) in Germany[46] whereas are e-money type of tokens for making payments in Malta.[47] There are other EU countries are in the process of introducing regulatory regimes of crypto assets (like France and Italy) whereas some are not (for instance, Ireland and Spain). The diverse regulatory schemes across EU member states can be more complicated when it comes to regulatory exceptions under the single market system. For instance, regulatory perimeters applied to domestic Fintech firms may not be applicable to overseas entities, particularly firms registered in the EU. A foreseeable example is that a firm registered in Malta providing e-money-like products and services intends to operate in Germany and other EU countries through the internet. A commercial case of crypto assets taking place in Germany in 2018 uncovers a controversial understanding of financial instruments between the court and legal professionals.[48] Although crypto assets are not yet major financial products in the EU, the less harmonised regulatory regimes could be problematic in the future.

In addition, the unified Anti-Money Laundering regulation in the EU is expected to prevent illicit activities in relation to crypto assets. These illicit activities include misuse of computers, distribution of prohibited goods, counterfeit and fraudulence, as well as misconduct of officials. It is believed that all EU countries have adopted relevant Laws and Directives to combat financial crimes and to assist in preventing illicit earnings circulating into the financial system.

Despite the ineffectiveness and inconsistencies in the existing regulatory frameworks of crypto assets, authorities of the UK and EU have undertaken a series of progress to improve Regulatory Technology and introduce more prudent measures. Business entities that provide crypto assets products and services are requested to comply with business registration and reporting and recordkeeping requirements under either domestic Laws or EU Directives.

[46] 'BaFin - Virtual Currency' (n/d) <https://www.bafin.de/EN/Aufsicht/FinTech/VirtualCurrency/virtual_currency_node_en.html> accessed 16 July 2019. See detailed discussion in Section 6.2.1 of this thesis.

[47] 'Distributed Ledger Technology and Virtual Currencies - Central Bank of Malta' (n/d) <https://www.centralbankmalta.org/en/qqa-dlt-vcs> accessed 30 October 2019. See detailed discussion in Section 6.2.2 of this thesis.

[48] 'Citizen Service Berlin - Brandenburg - Criminality of Trade in Bitcoins' (n 32).

Transnational coordination and cooperation, as well as a standardised accounting system are essential to prevent, detect and investigate global money laundering and related illicit activities.

# 2 Background and Theoretical Analysis

## 2.1 Background of Fintech and Crypto Assets

Information technology has been applied in many industries to help decision-making and data analysis. For instance, establishing analytical methods and algorithms to improve managerial efficiency and to analyse consumer behaviour for marketing plans.[49] Information technology has also assisted banks and financial institutions to improve their efficiency and productivity. For instance, smart contracts and online banking.[50] Information technology affects the financial sector in several ways. First, the development of Fintech lowers the cooperative obstacles between financial and technology firms. A worth mention example is the use of the Application Programming Interface (API),[51] which offers solutions to the concerns over security and confidentiality of user information of banks and businesses. The API permits financial firms to access commercial databases without requesting user information. Thus, financial firms can analyse consumer preferences and credibility in order to tailor financial products and services and prevent financial fraud, meanwhile, enhance their competitiveness.

Second, information technology creates a channel allowing non-financial firms to participate in the financial sector that previously dominated by banks and financial institutions.[52] These new market entrants bring innovation to the industry and extend the scope of financial products and services. However, the increasing number of market participants that hold advanced technology heightens the competitive pressure of traditional financial firms and drives the overall financial industry evolving towards a digital era. In the meantime, new market participants with cutting edge technology complicate the market structure of the financial

[49] Davenport (n 1). at chs. 10 and 12.

[50] Seese, Weinhardt and Schlottmann (n 2). at chs. 10 and 13.

[51] 'A server system having one or more processors and memory receives, from a client, a generic request to access remotely hosted services'. David Tribbett, 'Method and System for Providing Access to Remotely Hosted Services through a Normalized Application Programming Interface' [2012] United States Patent. at p. 1.

[52] For instance, the payment technology firms, PayPal and Alipay, are providing transaction services to their users through registered and verified email addresses or phone numbers. 'PayPal User Agreement' (2019) <https://www.paypal.com/uk/webapps/mpp/ua/useragreement-full> accessed 9 April 2020.; 'Alipay Account Service Agreement' (2016) <https://render.alipay.com/p/f/agreementpages/alipayaccountserviceagreement.html > accessed 9 April 2020.

sector and further challenge the capacity of the financial regulatory agencies. In addition, the rapid growth of Fintech firms may create gaps between regulation improvement and technological advancement.[53] Such gaps may cause asymmetric information between businesses and consumers/investors or be used for gaming with regulatory systems. For instance, misleading product marketing and service promotion, as well as imprecise prospectuses.

Moreover, the presence of information technology in the financial industry has made the existing regulatory frameworks more complicated and urged the development of regulatory technology. The assemblage of 'big data' and 'machine learning', along with the extensive expansion of the 'social media network' is blurring the boundary between the financial industry and others, while challenging the regulatory abilities.[54] The possibility of misusing new technologies is higher when regulations are loose, especially to uninformed consumers. In the meantime, anonymity or semi-anonymity of Fintech products and services increases the complexity of identifying property rights of the product owners. The ownership rights may become untraceable and unidentifiable under the fast distribution of Fintech products and the variation of information technology.[55] For example, one technology, the Distributed Ledger Technology (DLT), is not only improving the efficiency and security[56] of financial institutions but also challenging the existing centralised financial system through its main product, crypto assets its decentralised networks. Thus, crypto assets are commonly used as an example of

[53] For example, the BaFin recorded an increase in queries of fintech companies, ICOs and new payment services, from 1, 208 in 2017 to 1, 397 in 2018. BaFin, '2018 Annual Report' (2018) <https://www.bafin.de/SharedDocs/Downloads/EN/Jahresbericht/dl_jb_2018_en.pdf?__blob=publicationFile&v=3> accessed 20 November 2019. at p. 46.

[54] The current regulatory pressures faced by the financial services industry focuses on three actions: 'a) an open-source platform for FinTech regulation, b) a regulatory XML to help standardize reporting and c) an overarching international standards body'. Philip Treleaven, 'Financial Regulation of Fintech' [2015] Journal of Financial Perspectives. at p. 1.

[55] Andrew Murray, *Information Technology Law : The Law and Society* (4th edn, Oxford University Press 2019). at Part III: Digital Content and Intellectual Property Rights and Part IV: E-Commerce.

[56] The technical rationale behind the DLT is that 'the key design element of blockchains –embedded security – makes them different from ordinary horizontally scalable distributed databases such as MySQL Cluster, MongoDB and Apache HBase. Blockchain security makes it practically impossible to modify or delete entries from the database'. BitFury Group and Jeff Garzik, 'Public versus Private Blockchains Part 1: Permissioned Blockchains White Paper' (2015) < https://bitfury.com/content/downloa ds/public-vs-private-pt1-1.pdf > accessed 5 January 2020. at p. 6.

financial technology development urging improvements of the regulatory regimes. Crypto assets inherit the main function of the DLT and Blockchain and provide permission-less open source to developers and users.[57]

## 2.2 Definitions of Crypto Assets around the World

Information technology started to draw the attention of the authorities and publics alongside the popularity of the internet. On the one hand, it allows data being transferred and stored in various formats without geographical restrictions, such as peer-to-peer data transfer and cloud servers. On the other hand, it leads to no user privacy on the internet and drives out central administrations. All information can be traceable or decodable since every activity on a single computer is synchronised with could servers or stored on hard drives. This exposes user information to internet hackers and threatens the confidentiality of individuals and enterprises. Therefore, both individual and organisational users seek solutions that provide decentralised networks and are more secure and see the Distributed Ledger Technology (DLT) as one of the solutions.

The Distributed Ledger Technology (DLT) is one of the notable outcomes of Fintech developments. It offers a new transaction method with enhanced privacy and efficiency that challenges the intermediary role of banks and financial institutions.[58] One of the DLT application is crypto assets and the blockchain technology that underpins it.[59] Crypto assets transactions are anonymous or semi-anonymous and processed in peer-to-peer networks using encrypted keys that are generated randomly and held by transaction parties only.[60] This aims to improve transaction efficiency and to strengthen user confidentiality. However, the

[57] 'Permission-less blockchains are systems with an open membership allowing every node to create blocks, utilize more complex algorithms out of necessity' ibid. at p. 9.; 'Crucially, the network of computers running the Bitcoin software and maintaining the blockchain is decentralized, with no central authority that controls it. Because there are no permissions required to join the network of computers that run the Bitcoin software and help to maintain the blockchain, the Bitcoin blockchain is said to be public, or "permissionless," distinguishing it from private, or "permissioned," blockchains that are being developed by financial and technology companies'. Walch (n 5). at p. 7.

[58] The World Bank, 'Distributed Ledger Technology (DLT) and Blockchain: FinTech Note No.1' (2017) < https://openknowledge.worldbank.org/bitstream/handle/10986/29053/WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.p df?sequence=1&isAllowed=y> accessed 23 April 2019. at pp. VII-X.

[59] Steven Dryall, 'Cryptocurrencies and Blockchain' in S. Chishti (ed.). *The WealthTech Book* (2020). at pp. 158 - 161.

[60] Murray (n 55). at pp. 438 - 452.

anonymity of crypto assets opens a window for financial crime making financial misconduct harder to monitor, especially when it involves multiple countries or jurisdictions.

Crypto assets are known as digital or virtual currency representatives (unofficially) or digital assets/tokens (officially in the UK)[61] that are able to operate as a medium of exchange at a person-to-person level enabling direct payments between individuals. Crypto assets are based on cryptography and process transactions anonymously or semi-anonymously without third parties. This transaction method demonstrates advantages in assisting in securing transactions and mapping the creating of additional units. Such encryption technology is known as Blockchain, one type of DLT.[62] As of July 2019, there are over 2,300 crypto assets[63] and 250 crypto assets exchanges[64] available online. Bitcoins, the original and by far the most well-known crypto assets launched in January 2008,[65] hold the majority of the market shares and it is commonly used as a representative of crypto assets.

Bitcoins were conceptualised by Nakamoto in 2008[66] and were acknowledged as the first crypto assets that apply Block Chain technology. Bitcoins inherit the idea and the technology of peer-to-peer sharing used by the music industry in the late 1990s. The peer-to-peer technology was applied by software "Napster". Napster provides a music-swapping service on

[61] FCA, 'Guidance on Cryptoassets Feedback and Final Guidance to CP 19/3' (n 35).

[62] The World Bank (n 58), p. IV; Dryall (n 59), at p. 15.; Robby Houben and Alexander Snyers, 'Cryptocurrencies and Blockchain Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion' (2018) at p. 15.; Anton Badev and Matthew Chen, 'Bitcoin: Technical Background and Data Analysis' (2014) Finance and Economics Discussion Series NO. 2014-104. at p. 5; Walch (n 5). at p. 6.

[63] According to CoinMarketCap < https://coinmarketcap.com> accessed 02 July 2019.

[64] According to Coin.market < https://coin.market/exchanges> accessed 02 July 2019.

[65] Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2008).

[66] The creator of Bitcoins notes that 'purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers'. ibid. at p. 1.

its peer-to-peer network for users to exchange MP3[67] music files.[68] Although Napster did not directly breach copyright since the peer-to-peer network did not hold or store the music, Napster was charged infringement of copyright for indirectly contributing music files without the authorisation and was ordered shut down in 2001.[69] This case brought the copyright of digital properties into a discussion. Shih and Ku[70] and Landes and Lichtman[71] denote that Napster created a new approach to encourage private/individual musicians to publish their work online and facilitate creation. A few years after the shutdown of Napster, the ideas of free sharing without central controls on peer-to-peer networks have come back and made a resurgence in the financial sector since 2008.[72]

However, so far only few countries embrace this new technology and utilise it to facilitate financial services. By the end of 2019, only Japan and Venezuela have introduced crypto assets

[67] A format of compressed digital representations of musical recordings.

[68] Napster doesn't maintain copies of the music recordings on its computer or servers neither permanently nor temporarily. Napster maintains an index facility and provides access to software, accessible to Napster users via the Internet. The index and software permit one user to access another user's HDD directly to request music file swapping. Richard Stern, 'Napster: A Walking Copyright Infringement?' (2000) 95 Micro Law 3 - 5. at p. 4.

[69] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 [9th Cir. 2001]

[70] 'argues against copyright protection for digital works because the economics of digital technology undercuts prior assumptions about the efficacy of a private property regime for information, a public good. Questioning the conventional wisdom that the two interests served by copyright, creation and public dissemination, are aligned, the Article reveals that the argument for copyright is primarily an argument for protecting content distributors in a world in which middlemen are obsolete. Copyright is no longer needed to encourage distribution because consumers themselves build and fund the distribution channels for digital content. With respect to the creation of music, this Article argues that exclusive rights to reproduce and distribute copies provide little if any incentive for creation, and that digital technology makes it possible to compensate artists without control'. Raymond Shih and Ray Ku, 'The Creative Destruction of Copyright: Napster and the New Economics of Digital' (2002) 69 The University of Chicago Law Review 263. at p. 263.

[71] 'Napster facilitated the online exchange of music files in two ways: it provided software that allowed a user to identify any song the user was willing to share with others; and it provided a website where that information was made public so that an individual looking for a particular song would be able to find a willing donor. Several firms in the music industry sued Napster, alleging that these tools promoted the unauthorized distribution and duplication of copyrighted music'. William Landes and Douglas Lichtman, 'Indirect Liability for Copyright Infringement: Napster and Beyond' (2003) 17 Journal of Economic Perspectives 113. at p. 119.

[72] The creation of Bitcoins and the DLT.

into their payment systems and are regulating crypto assets businesses accordingly.[73] For instance, the Japanese authorities have allowed crypto assets to be a payment method effective from 1st April 2017, and all crypto assets exchangers shall comply with the Payment Service Act[74] of Japan; Venezuela issued its governmental cryptocurrency against crude oil in 2018[75] under the tough economic condition of currency depreciation against US Dollars.

Apart from the interpretation of the technology applied for payments and transactions, some authorities are trying to identify and clarify the roles of crypto assets in the financial sector. The Organisation for Economic Co-operation and Development (OECD) elaborated the status of crypto assets in the financial sector as early as in 2014 giving Bitcoins as an example.[76] This OECD's working paper sets forth that crypto assets can never become an alternative currency to fiat money because people have to pay taxes. The OECD working paper also accents the potential issues of crypto assets in consumer protection and financial crimes. The working paper suggests that the policies of consumer protection shall set against online stealing, value volatilities and business shutdown and the policies of financial crimes prevention shall focus on tax evasion and money laundering. A few years after, the OECD has recognised the increasing popularity of crypto assets and blockchain technology in industries and published a working paper in October 2018 to discuss the possibility of adopting crypto assets in the System of National Accounts. The paper states that crypto assets and the DLT may become the take-up in the future. For example, crypto assets may link to fiat currency and central banks may

[73] Apolline Blandin and others, 'Global Cryptoasset Regulatory Landscape Study' [2019] Cambridge Centre for Alternative Finance < https://www.jbs.cam.ac.uk/fileadmin/userupload/research/centres/alternative-finance/downloads/2019-04-ccaf-global-crypto a sset-regulatory-landscape-study.pdf > accessed 29 February 2020.

[74] Details of Screening for New Registration Application as Virtual Currency Exchange Service Provider [2017]. Appendix 2 of the Payment Services Act 2017 of Japan.

[75] 'Venezuela Petro Cryptocurrency (PTR)--English White Paper' (n 34).

[76] Adrian Blundell-Wignall, 'The Bitcoin Question: Currency versus Trust-Less Transfer Technology' (2014) OECD Working Papers on Finance, Insurance and Private Pensions, No. 37.< https://www.oecd.org/daf/fin/financial-markets/The-Bitcoin-Ques tion-2014.pdf > accessed 27 September 2019. at p. 7.

design central bank cryptocurrencies using the DLT.[77] Soon after in 2019, the OECD published a guidance paper for Initial Coin Offerings for small and medium business financing.[78]

Additionally, the International Monetary Fund (IMF) has discussed the risks of crypto asset applications at the Law and Financial Stability Seminar taking place in September 2018 in the US. The seminar emphasised the rising issues in anti-money laundering and market manipulation using crypto assets and urged authorities to put relevant regulations on their agenda to ensure market integrity.[79] For instance, the US authorities have allowed trading crypto assets on regulated derivative exchanges, such as Swaps on the Designated Contract Markets (DCMs) and consider delivering financed virtual currencies to retail customers.[80] The IMF considered that these measures will expose retail customers to risks, especially uninformed consumers.

In the case of European countries, most policymakers have refrained from defining the term of crypto assets altogether due to the divergent roles of crypto assets across the EU member countries.[81] A joint publication of the Her Majesty's Treasury (HMT), the Financial Conduct Authority (FCA) and the Bank of England (BoE) names crypto assets as 'crypto assets',[82] and this thesis follows this term. The FCA specifies the terms of crypto assets into four categories,

---

[77] OECD, 'How to Deal with Bitcoin and Other Cryptocurrencies in the System of National Accounts?' (2018) < http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=COM/SDD/DAF(2018)1&docLanguage =En > accessed 10 August 2019. at p. 8.

[78] OECD, 'Initial Coin Offerings (ICOs) for SME Financing' (2019) < https://www.oecd. org/finance/ICOs-for-SME-Financing.pdf > accessed 22 May 2019.

[79] IMF, 'Private Crypto Assets and Central Bank Digital Currencies' (2018) < https://www.imf.org/en/News/Seminars/Conferences/2018/07/24/2018-seminar-on-law-and-financial-stability > accessed 15 January 2020.

[80] U.S. Commodity Futures Trading Commission, 'Keynote Address of Commissioner Brian Quintenz before the DC Blockchain Summit' (2018) <https://www.cftc.gov/PressRoom/SpeechesTestimony/opaquintenz8> accessed 2 July 2019. and U.S. Commodity Futures Trading Commission, 'CFTC Designates TrueEX LLC as a Contract Market' (2012) <https://www.cftc.gov/PressRoom/PressReleases/pr6371-12> accessed 2 July 2019. Whilst the UK is considering to ban the sale to retail consumers of certain types of crypto-assets derivatives. FCA, 'Guidance on Cryptoassets Feedback and Final Guidance to CP 19/3' (n 35). para. 2.36 at p. 14.

[81] For example, the FCA (UK authority) and BaFin (German authority) refer to crypto asset as a token (not a payment instrument), the EU sees it as virtual currency and BoE (Bank of England) sees it as digital currency (having payment functions). See the following discussions of this section.

[82] HM Treasury, FCA and Bank of England, 'Cryptoassets Taskforce: Final Report' (2018) < https://assets. publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf> accessed 20 December 2019.

exchange tokens, e-money tokens, security tokens and utility tokens.[83] Interestingly, on the websites of the BoE and the FCA, the terms of 'cryptocurrency', 'crypto assets', 'digital currency' and 'exchange tokens' are used interchangeably. In addition, the EU refers to crypto assets as 'virtual currency' under the Directive (EU) 2018/843, known as the Fifth Anti-Money Laundering Directive. The EU is not alone in using these terms of crypto assets interchangeably. There are also various definitions of crypto assets across the member states in the US. For instance, the Federal Reserve of the US refers to crypto assets as 'digital currency'[84] and use the terms of 'digital assets', 'virtual currency' and 'crypto assets' interchangeably.[85]

Officially, the EU refers to crypto assets as 'virtual currency' under the Fifth AML Directive:

> 'virtual currency means a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically'. [86]

The Bank of England defines cryptocurrency as Digital Currency:

> 'A digital currency is an asset that only exists electronically. Digital currencies such as Bitcoin were designed to be used to make payments, but today many digital currencies are held as speculative assets by investors who hope their value will rise'. [87]

The FCA defines cryptocurrency as an Exchange Token:

---

[83] FCA, 'CP19/3: Guidance on Cryptoassets UK' (2019).

[84] Brainard L, 'Cryptocurrencies, Digital Currencies, and Distributed Ledger Technologies: What Are We Learning?', Decoding Digital Currency Conference Sponsored by the Federal Reserve Bank of San Francisco (2018). <https://www.federal reserve.gov/newsevents/speech/files/brainard20180515a.pdf> accessed 17 June 2019.

[85] U.S. Commodity Futures Trading Commission, 'Keynote Address of Commissioner Brian Quintenz before the DC Blockchain Summit' (n 80).

[86] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU [2018] (OJ L156/43). art. 1. para. (2) (d) (18), at p. 54.

[87] <https://www.bankofengland.co.uk/research/digital-currencies> accessed 13 May 2019.

> ‘Cryptoassets is a broad term and covers many different types of products. The most popular forms of cryptoassets include tokens like ‘Bitcoin’ and ‘Litecoin’. We call these ‘exchange tokens’ but they are sometimes referred to as ‘cryptocurrencies’, ‘cryptocoins’, or ‘payment tokens’. Exchange tokens use a distributed ledger technology (DLT) platform and are not issued or backed by a central bank or other central authority so are not considered to be a currency or money’. [88]

The three definitions above indicate different opinions on crypto assets from the three authorities. The EU authorities see ‘crypto currency’ as an unofficial intermediator accepted by individuals and legal persons and carrying out transactions among them without central authorisations. Thus, the EU names crypto assets as ‘virtual currency’. Crypto assets are neither issued nor guaranteed by any authorised bodies in the EU and is not fully attached to fiat money, therefore, crypto assets are not liable to official regulations of money businesses in the EU. Based on this definition, crypto assets are treated as transferable and tradable assets within the EU under the EU regulations. However, EU member states are permitted to have their own opinions to set up their own regulatory schemes in addition to the EU regulations.

The definition by the BoE focuses on other uses of crypto assets, such as payment methods and trading for value appreciation. The BoE refers to crypto assets as digital currencies or virtual assets similar to some traditional financial instruments. These traditional financial instruments are held for investment purposes and can be traded on markets. This definition completely ousts crypto assets from the intermediary roles of the financial system and categorises crypto assets into asset investments and financial instruments.

The FCA defines bitcoin-like crypto assets as exchange tokens. The FCA emphases that exchange tokens that employ DLT are sometimes used for making payments and these tokens may be referred to different financial terms similar to currency or money. However, these tokens are neither currency nor fiat money and are not regulated under traditional financial regulations. The FCA further classifies crypto assets into four groups and differentiates exchange tokens from other types of crypto assets.[89] Nevertheless, all types of crypto assets are token-like financial properties under the definitions by the FCA.

[88] <https://www.fca.org.uk/consumers/cryptoassets> accessed 13 May 2019.

[89] FCA, ‘Guidance on Cryptoassets Feedback and Final Guidance to CP 19/3’ (n 35).

Put all three definitions together, the terms of 'crypto assets', 'digital money', 'virtual currency', 'crypto-currencies' and 'crypto tokens' contain the main properties of the popular Fintech products underpinned by the DLT, which are investable, exchangeable and convertible whereas not are an official representative or replacement of fiat money or legal tender.

The divergent definitions of crypto assets raise concerns over the consistency of the regulations in the EU. Crypto assets regulated in one country might be unregulated in another. Additionally, inconsistency may occur in regulatory perimeters and business practice in EU member states and could lead to disputes over jurisdictions.[90] Moreover, the various classifications of crypto assets across EU nations require further clarifications. The inconsistencies and unclarified terms and definitions of crypto assets in the EU countries may place obstacles to the compliance measures of firms and expose consumers to risks. The risks are greater when crypto assets businesses are operating internationally under the EU single market system. For example, the UK defines crypt assets that present e-money-like properties as 'e-money tokens', which are detached from the EU classifications.[91] This means e-money token businesses may be able to obtain a licence in the UK and operate in other EU countries, whereas some EU countries may have not yet permit e-money crypto asset businesses. In addition, exchange tokens (defined by the FCA) that fall outside the regulatory perimeters of the FCA may be able to obtain business licences to operate in some EU countries, such as Germany. These UK unregulated exchange tokens are still able to operate in the UK or through the internet under the single market system, subject to the length of transaction period of Brexit.[92]

---

[90] 'Public blockchains have nodes which are often located in various jurisdictions across the world. This feature, once again a badge of decentralisation, causes issues with recent data regulation GDPR applies to the processing of personal data affecting EU citizens wherever the processing is taking place, as well as other EU-related jurisdictional provisions. The effect is that the Regulation will bite on blockchain with only passing links to the EU. However, once it bites, all of the issues relating to compliance are present. Further, all of the data transfer provisions, where minimum standards must be met, come into play. Whilst, again, a private blockchain may govern such transmission from a central point under binding terms and conditions, that is unlikely to be the case of public blockchains. The results, again is a lack of ability to comply'. Dean Armstrong QC, Dan Hyde and Sam Thomas, *Blockchain and Cryptocurrency: International Legal and Regulatory Challenges* (Bloomsbury Professional 2019). para. 3.49. at p. 33.

[91] FCA, 'Guidance on Cryptoassets Feedback and Final Guidance to CP 19/3' (n 35). para. 2.25. at pp. 13 - 14.

[92] ibid. paras. 1.32 - 1.35. at p. 7.

Although authorities have tried to define crypto asset according to its technology, applications and functions, accordingly, it is unclear whether to categorise crypto assets businesses as financial firms or technology firms. On the one side, it is possible that Fintech firms only provide technical support to financial firms, such as trading/exchange platform and database establishment and maintenance. Additionally, Fintech firms may carry out ICOs to fund their projects. These two types of firms presumably can be classified as technology firms. On the other side, Fintech firms may provide services for crypto asset exchange, trading or wallet custody, which could be classified as financial service providers. Since there have no clear boundaries to directly categorise these Fintech firms into traditional industries or sectors, some authorities have simply defined all Fintech firms into one special group and regulate them separately from traditional businesses and financial firms, such as Malta. However, existing Laws and Regulations may not be applicable to these new businesses or activities straightaway. The establishment or amendment of laws and regulations across industries require a comprehensive understanding of the complexity of crypto asset related activities and need time to catch up with the pace of technology developments.

## 2.3 The Properties of Crypto Assets

By reason of that crypto assets are a nascent product to the financial markets, the majority of existing studies focus on the technological concepts and applications of crypto assets (see section 2.1 of this thesis). The relevant literature of the Laws and Regulations on crypto asset in the UK and the EU is sparse. Some studies provide a brief examination of the regulations of crypto assets from a global point of view. For instance, the Norton Rose Fulbright (a global law firm) provided an introduction of the legal framework of crypto assets in 2015.[93] The Law Library of Congress studied the regulation of crypto assets around the world in 2018.[94] The Cambridge Centre for Alternative Finance published an overview of crypto assets around the world in 2019.[95] Dean and others listed the issues that crypto assets may bring to the financial systems.[96] However, these studies offer a general overview of the regulatory status in selected countries whereas have not provided an in-depth analysis of the adequacy and consistency of the crypto asset regulations in the UK and the EU countries. Besides, official publications of

[93] Norton Rose Fulbright, 'Deciphering Cryptocurrencies: A Global Legal and Regulatory Guide' 20.

[94] The Law Library of Congress, 'Regulation of Cryptocurrency Around the World' (2018) < https://www.loc.gov /law/help/cryptocurrency/cryptocurrency-world-survey. pdf > accessed 23 April 2019.

[95] Blandin and others (n 73).

[96] Dean Armstrong QC, Dan Hyde and Sam Thomas (n 90).

the UK and EU authorities are either at their consultation stage, such as France or at their initial stage, such as the UK. These official working papers focus on the interpretations of the aims, scope and process of the regulatory frameworks, whilst the assessment of the effectiveness and consistencies of these regulatory policies have not put in progress.

Traditionally, it has been banks and financial institutions to provide transaction services and to be obliged for recordkeeping and reporting suspicious transactions. Banks have acted as third parties carrying out transaction services like a central hub and have been regulated by the central banks and relevant regulatory agencies, accordingly. In contrast, the Block Chain and the DLT offer peer-to-peer networks for payment transactions without the involvement of a third party, such as banks and other traditional payment platforms. Therefore, the intermediation role of banks is no longer seen as necessary hence the notion of financial decentralisation has come into usage.[97]

However, the concerns over financial decentralisation are technically unnecessary. In fact, almost all crypto assets activities such as mining, transaction or trading, require a third party to provide relevant services. For instance, crypto assets owners need exchange platforms for transactions and trading and require custody wallet providers for crypto assets storage. These service providers establish their own user groups, like small central hubs. Additionally, some service providers apply centralised mixing services to improve transaction anonymity. These centralised mixing services create a centre for each transaction group within their service platforms. For example, Bitcoin Fog, a Bitcoin service provider, has applied a central mixing hub to obfuscate original user's information and stated it is somewhat contradictory with the initial intention of Bitcoins.[98] Similarly, Seo and others explain the technology applied for the

[97] Dryall (n 59); Yannan Li and others, 'Toward Privacy and Regulation in Blockchain-Based Cryptocurrencies' [2019] IEEE Network 1; The World Bank (n 58).; Walch (n 5).

[98] 'The idea behind a mixing service is to run a centralized mix by some external observers where users can put some money in and the money will be mixed with other users' funds and then returned to a fresh address to obfuscate the original source'. Li and others (n 97). at p. 2.

establishment of a centralised mixing service for a crypto asset user hub.[99] Consequently, crypto asset service providers are actually creating central hubs for their users, which is similar to the intermediary roles of banks and financial institutions.

The DLT and Block Chain have been challenging the traditional financial services and offered alternative intermediation of exchanges that is not only more secure and efficient. Traditionally, banks and financial institutions are responsible to verify user information, such as legal identities and residential information of their customers and to carry out due diligence measures, including recordkeeping and reporting suspicious transactions. In contrast, user information on Block Chain remains anonymous and transactions are made through encrypted and authorised keys held by payers and payees only. Although the Distributed Ledgers (DLs) retain transaction records whereas do not necessarily take into account the identities of users. Thus, unless required, the details of online transaction, such as real trading parties and objects are even not accessible to those service providers. This is supposed to enhance user confidentiality against data leak and cyber-attack. In addition, the irreversible nodes on the DLT make transactions more transparent and traceable although transaction parties remain anonymously.[100]

Thus, crypto assets have combined properties consisting of anonymity, efficiency and security. The combined properties make the DLT beneficial to both criminals and regulators. From the perspectives of financial crimes, anonymity complicates the process of identifying suspicious transactions and the traceability to link illicit activities to relevant persons in real life. In addition, free (no exchange rate, no bank commissions and no services charge on pure peer-to-peer networks) and efficient online cross-border transactions of crypto assets benefit financial crimes and global money laundering. Moreover, the absence of market oversight heightens the

[99] 'Bitcoin does not require much information, unlike other payment methods. The user can send Bitcoin using only the private key, and the user's privacy exposure is minimized. However, transaction information including the user's identification number (which is the wallet address) is recorded in Bitcoin's blockchain and is kept permanently. And anyone who knows the transaction id can see the transaction information. For this reason, the transaction with Bitcoin is said to have a pseud-anonymity rather than a complete anonymity'. Junwoo Seo and others, 'Money Laundering in the Bitcoin Network: Perspective of Mixing Services', *2018 International Conference on Information and Communication Technology Convergence (ICTC)* (IEEE 2018) <https://ieeexplore.ieee.org/document/8539548/> accessed 21 March 2019. 1403-1405 at p. 1405.

[100] Thomas Buocz and others, 'Bitcoin and the GDPR: Allocating Responsibility in Distributed Networks' [2019] Computer Law and Security Review; Niels Vandezande and KU Leuven Centre for IT & IP Law, *Virtual Currencies : A Legal Framework* (Intersentia 2018); World Bank (n 58); Dryall (n 59).

probability of using crypto asset platforms to transfer illicit earnings.[101] These characteristics of crypto assets inevitably are attractive to global grouped criminals.

From perspectives regulatory agencies, the DLT can be used to enhance information security and monitor transaction activities. Reyes suggests that utilising Block Chain technology in financial regulations could help to improve security as transaction data is only accessible with paired encrypted keys.[102] Utilising the DLT for bank transactions also reduces the cost of data submission, management and storage for central banks since the data will be stored and submitted simultaneously on DLs while transactions taking place. In addition, the DLT will allow central banks to access personal data timely without the involvement of third parties. This direct access could help to avoid duplications and delay in transaction reports.[103] The current reporting process in many countries request banks to identify suspicious transactions then submit them to central banks. It is somehow time-consuming and sometimes causes duplications if the suspicious transactions are reported by both banks of the payers and payees. With the DLT, the central banks can identify abnormal online activities using algorithms without delay instead of relying on third parties, including banks and financial institutions.[104]

The Bank for International Settlements (BIS)[105] and the European Commission[106] are aware of the increasing popularity of crypto asset products and services and published consultation paper in December 2019, respectively, inquiring feedback and comments in relation to the regulatory frameworks of commercial activities of crypto assets.

Some central banks have started to examine the benefit and possibility of applying DLT to issue Central Bank Cryptocurrency (CBCCs). For instance, the BIS published a working paper

---

[101] George Forgang, 'Money Laundering through Cryptocurrencies' [2019] Economic Crime Forensics Capstones. at pp. 6 - 9.

[102] Carla Reyes, 'Conceptualizing Cryptolaw' [2017] SSRN 1. at p. 5.

[103] As discussed previously, the DLT can detect double-reporting and all transaction records are immutable from deleting or rewriting. Brown (n 15). 327-339 at pp. 331 - 332.

[104] Alexandra Sims, Kanchana Kariyawasam and David Mayes, *Regulating Cryptocurrencies in New Zealand* (The Law Foundation New Zealand 2018). at pp. 113 - 122.

[105] Basel Committee on Banking Supervision, 'Designing a Prudential Treatment for Crypto-Assets' (2019) < https://www.bis.org/bcbs/publ/d490.pdf > accessed 22 March 2020.

[106] 'Financial Services – EU Regulatory Framework for Crypto-Assets' <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12089-Directive-regulation-establishing-a-European-framework-for-markets-in-crypto-assets> accessed 13 April 2020.

in 2017 to discuss the challenges and benefit of issuing CBCCs;[107] the BoE, The FCA, the HMT and the Financial Action Task Force (FATF) have discussed the impact of the DLT on the financial system in 2015;[108] the Bank of England studied the benefit of issuing Central Bank Cryptocurrency to economic growth and efficiency gains in 2016[109] and published a discussion paper inquiring public opinions in March 2020;[110] on 21st January 2020, the central bank of the UK, Canada, Japan, Sweden, Swaziland and the European Central Bank, together with the BIS, created a group to share experiences and assess the potential for central bank digital currency (CBDC) in their home jurisdictions.[111] Other EU countries haven't started moving forward with the ideas of CBCCs.

That is not to say however that account anonymity means distributed ledgers are immune to cyber threats. Internet hackers may prefer to obtain all transaction data on the peer-to-peer networks through a single ledger, rather than hacking into different bank servers.[112] User information, such as Internet Protocol (IP) address, locations and devices, is likely exposed to internet cyberattack.[113] In addition, crypto assets owners may face additional issues, such as data damage, crypto asset businesses shutdown and internet thefts.[114] Current regulatory schemes of crypto assets in the UK and some EU countries have covered several aspects,

[107] Morten Bech and Rodney Garratt, 'Central bank cryptocurrencies' (2017) September BIS Quarterly Review 55 < https://www.bis.org/pub l/qtrpdf/r_qt1709f.pdf > accessed 14 February 2020.

[108] Financial Action Task Force, 'Guidance for A Risk-Based Approach, Virtual Currencies' (2015) < https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf > accessed 14 February 2020.

[109] John Barrdear and Michael Kumhof, 'The Macroeconomics of Central Bank Issued Digital Currencies' (2016) Bank of England Staff Working Paper No. 605 < https://www.bank ofengland.co.uk/-/media/boe/files/working-paper/2016/the-macroeconomics-of-centr al-bank-issued-digital-currencies > accessed 10 August 2019.

[110] Bank of England, 'Central Bank Digital Currency, Opportunities, Challenges and Design' (2020) < https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf> accessed 20 March 2020.

[111] 'Central Bank Group to Assess Potential Cases for Central Bank Digital Currencies | Bank of England' <https://www.bankofengland.co.uk/news/2020/january/central-banks-group-to-assess-digital-currencies?sf116286084=1> accessed 25 January 2020.

[112] Each bank has its own servers and store data of their own customers. Distributed ledgers are an open source and all notes (transaction records) are connected, therefore, hackers can obtain the all dataset through breaking into one note on the networks. Sims, Kariyawasam and Mayes (n 104). at pp. 65 - 70.

[113] Li and others (n 97). at p. 4.

[114] Brown (n 15). at p. 330.

including registration, issuance, tax treatment and money laundering. More studies are needed to make regulatory regimes adequate and effective.[115]

## 2.4 The Role of Crypto Assets in Financial Crime

The popularity of crypto asset products and services are challenging the traditional financial services of banks and money businesses. It offers alternative intermediation of exchange that is more secure and efficient through user the encrypted keys.[116] However, the anonymity of crypto assets (both products and services) also provides a simpler and efficient approach for financial crime, for instance, laundering illicit earnings. There are two representative cases in the US regarding crypto assets relating to financial crime. The first case is the arrest of Matthew Jones, a user of a marketplace – Silk Road, in 2013 for distribution of a controlled substance in violations of "Prohibited acts A", 21 U.S. Code §841 (a) (1) and (b) (1) (C).[117] The second case involves two former Federal agents who were charged with Theft of Government Property (18 U.S. Code §641), Wire Fraud (18 U.S. Code §1343), Money Laundering (18 U.S. Code §1956{h)) and Stealing Digital Currency (18 U.S. Code §208) during their investigation of a dark web – the Silk Road.[118] The stolen crypto assets in the second case were worth over $1.5 million US Dollars and the majority of illicit earnings were laundered in Japan, the country that has seen a high incidence of money laundering cases so far. According to the Japan Times, there were 669 cases reported with money laundering activities using crypto assets in Japan

[115] Blandin and others (n 73). at p. 55.

[116] Thomas Buocz and others, 'Bitcoin and the GDPR: Allocating Responsibility in Distributed Networks' [2019] Computer Law and Security Review; Niels Vandezande and KU Leuven Centre for IT & IP Law (n 100); World Bank (n 58); Dryall (n 59).

[117] Code §841 (a) (1): '(a) **Unlawful acts** Except as authorized by this subchapter, it shall be unlawful for any person knowingly or intentionally — (1) to manufacture, distribute, or dispense, or possess with intent to manufacture, distribute, or dispense, a controlled substance'; 21 U.S. Code §841 (b) (1) (C) is the sentencing standards, accordingly. United States v Matthew Jones [2014] No.6:14-mj-1233, So. 1 (M.D. Fla.) <https://www.justice.gov/sites/default/files/usao-mdfl/legacy/2014/05/30/20140530_Jones_Complaint.pdf> accessed 10 Oct 2019. 21 U.S.

[118] United States v Shaun W. Bridges and Carl Mark Force IV, Defendants [2015] No.3-15-70370 Cal.Rptr. 1 (N.D.Cal.) <https://www.justice.gov/usao-ndca/file/765686/download> accessed 10 November 2019.

between April and December 2017.[119] The number of suspected cases of crypto asset money laundering in Japan increased significantly about 10 times in 2018 to over 7,000.[120]

Crypto assets related financial crimes have demonstrated a global touch.[121] Other than the cases mentioned above that originated in the US and laundered in Asian countries, there were considerable amounts of crypto assets stolen in the EU and the US between 2014 and 2017. The illicit earnings were laundered on crypto asset markets in multiple countries. According to the European Union Agency for Law Enforcement Cooperation (Europol), a cross-border and large-scale money laundering group was shut down in 2017, and 23 members of the gang were arrested. The involved amount was around €2.5 million Euros, and the members of the group were mainly from Spain, Colombia and Venezuela.[122] Again, in earlier 2019, the Europol, Canada and the US Joined Forces targeted the users of controlled products on dark web marketplaces, 61 people were arrested, and 50 illicit dark web accounts were closed. The involved amount was over €6.2 million Euros. The case judgements haven't been made public at the time of writing. There are possibilities that the arrests may not go to court or perhaps the prosecution is still ongoing.[123]

The global networks and the anonymity of crypto asset suggest that preventing crypto assets crimes should prioritise the regulations of the channels of transactions and ensuring the traceability of both payers and payees. Some authorities have announced regulatory rules for crypto assets business registration and recordkeeping. For instance, crypto assets service

---

[119] 'NPA Cryptocurrency Tips Point to 669 Suspected Money-Laundering Cases from April to December | The Japan Times' <https://www.japantimes.co.jp/news/2018/02/22/business/npa-cryptocurrency-tips-point-669-suspected-money-laundering-cases-april-december/#.XK8r3dVKjIU> accessed 11 April 2019.

[120] 'Cases of Money Laundering Linked to Cryptocurrency in Japan up Tenfold in 2018 | The Japan Times' <https://www.japantimes.co.jp/news/2019/02/28/national/crime-legal/cases-money-laundering-linked-cryptocurrency-japan-tenfold-2018/#.XLBfGdVKjIU> accessed 12 April 2019.

[121] Many financial crimes and money laundering activities regarding crypto assets involve worldwide individual/grouped criminals and victims, such as Japan, the US, UK, Germany, Columbia, Spain. See discussion in the previous paragraph of this section.

[122] 'Cryptocurrency Laundering as a Service: Members of a Criminal Organisation Arrested in Spain | Europol' <https://www.europol.europa.eu/newsroom/news/cryptocurrency-laundering-service-members-of-criminal-organisation-arrested-in-spain> accessed 15 June 2019.

[123] Europol, 'Global Law Enforcement Action against Vendors and Buyers on the Dark Web' (26 March 2019) <https://www.europol.europa.eu/newsroom/news/global-law-enforcement-action-against-vendors-and-buyers-dark-web> accessed 10 November 2019.

providers are requested to keep user information and transaction records and report suspicious transactions under anti-money laundering regulations in Japan[124] and several states in the US. Taking New York as an example, the regulatory schemes of crypto assets businesses in New York[125] are relatively stricter than other states of the US. All crypto – assets businesses must apply for a BitLicense in order to operate in New York or provide services for New York residents, regardless of their real business locations. BitLicense licensees must comply with the anti-money laundering measures under the 23 CRR-NY § 200.15 — Part 200 Virtual Currencies. It is worth to mention that the legal system of the US gives specific power to the Federal government while granting some powers to individual states.[126] The Banking Law, Bankruptcy Law and Criminal Law are under the Federal level, and the business contract and minor criminal matters are under the state level. This parallel legal system sometimes causes conflicts between Federal Laws and State Laws. For instance, crypto asset businesses established under state Laws may not comply with the banking regulation at Federal level, therefore, crypto asset enterprises may be unable to open a business bank account under the Banking Law. Another inconsistency is that crypto asset businesses are regulated in one state may be unregulated in another whereas still can carry out commercial activities under the business practice across the US. Therefore, consumers in those states that haven't had crypto asset regulatory policies are exposed to risks.[127]

Similarly, the EU sets up a parallel legal structure consisting of the national Laws and the EU Laws, and the situation in the EU is more complicated than in the US. The EU Laws are not simple supplementary provisions of the national Laws. EU member states are required to implement EU Laws within a given deadline while EU Laws do not necessarily cover the overall wrongdoings of crypto assets. Thus, both commercial and non-commercial activities uncovered by the EU Laws shall comply with the national Laws. Meanwhile, the EU Laws

[124] Financial Services Agency, 'Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism' (2018).

[125]'Virtual Currency Businesses | Department of Financial Services' <https://www.dfs.ny.gov/apps_and_licensing/virtual_currency_businesses> accessed 21 May 2019.

[126] 'The U.S. Constitution establishes a federal system of government. The constitution gives specific powers to the federal (national) government. All power not delegated to the federal government remains with the states. Each of the 50 states has its own state constitution, governmental structure, legal codes, and judiciary'. Federal Judicial Center, 'The U.S. Legal System: A Short Description' (2016) < https:// ar.usembassy.gov/wp-content/uploads/sites/26/2016/03/U_S__Legal_System_Englis h07 .pdf > accessed 20 June 2019.

[127] James V. Calvi and Susan E Coleman, *American Law and Legal Systems* (Longman 2012).

mainly focus on commercial activities, especially cross-broad trade and trade-related activities. This includes banking and financial regulation, carrying on business internationally and anti-money laundering. EU member states have agreed with the single market or one passporting system within the EU. The single market system allows free movement of goods and services within the EEA (European Economic Area).[128] The single market benefits to the EU member states in reducing the barriers and costs of international trade. The harmonised and standardised regulations have been adopted for banking and financial sector since free movement of money is as important as the free movement of goods for international trade. All EU member states shall comply with the EU Laws and Regulations as well as their national Laws. The single market system has been working effectively so far over two decades to some extents. However, the nascent product, crypto assets, that inherit the properties of both financial and commodity sectors incur inconsistencies in the existing regulatory framework.

The inconsistency in the current regulation of crypto assets in the EU is triggered by the diverse national Laws and EU regulations under the one passporting system. The EU member states hold diverse opinions on crypto asset products and services and have established different regulatory schemes, accordingly. In addition, the EU allows a flexible process for member countries to decide the time lengths and methods to implement EU Laws as long as all member states can achieve the regulatory requirements within a given time horizon.[129] The possible gaps in the time frames of implementing EU directives and the different understanding of EU requirements may further cause inefficiency in regulatory procedures within the EU.

Irwin and Dawson[130] analyse if global regulation of crypto assets can assist in investigating cybercrime. The analytical results show that the existing regulations of crypto assets in countries is often costly to firms in terms of implementation of compliance measure and

[128] European Commission (n 10).

[129] 'Types of EU Law | European Commission' <https://ec.europa.eu/info/law/law-making-process/types-eu-law_en> accessed 5 November 2019.

[130] 'These regulatory pitfalls are substantiated by the continuing difficulty faced by law enforcement agencies, in identifying individual Bitcoin users and separating those that are using them for nefarious purposes from those that are using them for legitimate ones. These challenges appear to grow exponentially when it comes to prosecuting criminals for Bitcoin-related offences, due to the enormous lack of agreement within the justice system of most countries as to the appropriate legal definition for Bitcoin'. Consistency, clarity and cost-effective implementation are the three vital characteristics to the success of regulatory frameworks. Angela SM Irwin and Caitlin Dawson, 'Following the Cyber Money Trail: Global Challenges When Investigating Ransomware Attacks and How Regulation Can Help' (2019) 22 Journal of Money Laundering Control. at p. 1.

restrains crypto assets market growth, which means less effective. They suggest that the ineffective regulation of crypto assets has caused difficulties for law enforcement agencies. The paper also addresses the importance of a unified legal definition for Bitcoin and of a clarified justice system of most countries. The paper highlights that consistency, clarity and cost-effective implementation of the regulatory frameworks globally need to be enhanced. The analytical results carried out in this paper is consistent with the finding of this thesis.

All in all, crypto assets are commonly used as an example of Fintech products that bring out the controversy over the regulatory policies among EU member states. For example, Germany and Malta encourage financial inclusion and see crypto assets as an approach to attract investors and start-ups; Italy is in the process gaining more relevant information of crypto assets; Spain simply ignores the impacts of crypto assets. The regulations across EU countries may become less controversial when the markets are more mature and regulatory technology are improved.

# 3 The Development of Anti-Money Laundering Regulations

In addition to the inconsistencies in regulatory regimes of commercial activities of crypto assets in the EU, there are concerns over global anti-money laundering regulation. The EU has updated the anti-money laundering schemes in 2018 and included crypto asset activities in the Fifth EU Anti-money Laundering Directive (5AML).[131] The 5AML Directive specifically requires the attention to crypto asset business and services, such as exchanges and custody wallet providers. All EU member states must implement the 5AML by 10 January 2020. The UK complies with the 5AML during the transition period of Brexit by December 2020. The 5AML givens regulatory instructions of commercial activities in terms of crypto assets and focuses on certain types of crypto asset businesses and services. Despite the fact that crypto assets are continuously gaining popularity around the world and have been used as a vehicle for financial crimes, prudential regulations shall assist with preventing misuse of the Fintech products and protecting the markets and consumers to some extents.

## 3.1 Initiatives of Anti-Money Laundering in the UK and EU

### 3.1.1 Money Laundering Regulation in the UK

Money laundering in the UK was initially regulated under Section 26B of the Drug Trafficking Offences Act 1986, 'Money laundering and other offences' of the Criminal Justice Act 1988, and Section 52 of the Drug Trafficking Act 1994 before 2002. It appeared difficult for the court to pinpoint the appropriate Act for charging purposes, for example, drug dealing money laundering under the Drug Trafficking Act 1994 and non-drug offences under the Criminal Justice Act 1988.[132]

The money laundering in the UK then legalised under the Proceeds of Crime Act (POC) 2002 Chapter 29 Part 7. Part 7 of the POC Act 2002 came into force on 24 February 2003. One of the aims of this Act was to 'make provision about money laundering, to make provision about investigations relating to benefit from criminal conduct or to property which is or represents

[131] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU [2018] OJ L156/43. recitals (8) - (11) and (16), at pp. 44 - 46.

[132] 'Proceeds Of Crime Act 2002 Part 7 - Money Laundering Offences | The Crown Prosecution Service' (2018) <https://www.cps.gov.uk/legal-guidance/proceeds-crime-act-2002-part-7-money-laundering-offences> accessed 3 February 2020. at 'The new principle money laundering offences – General'.

property obtained through unlawful conduct or to money laundering'. Part 7 of the POC Act 2002 provides the principle and guidance of money laundering activities. The Act explains that money laundering is a series of sophisticated activities that may involve 'Incentivises crime by rendering it profitable; provides domestic and transnational organised crime with a cash flow to perpetrate further crimes; and threatens the financial system and its institutions, both domestic and international'. Therefore, the main purpose of the Act is to make the process of money laundering more difficult, to deter professional launderers and to protect the integrity of financial institutions.[133] The provision of Part 7 of the POC Act 2002 was updated in 2003 under the Proceeds of Crime Act 2002 (Crown Servants) Regulations 2003. The amended Act extended the regulatory scope to Director of Savings and all employees or people who engaged in the Director of Savings.[134]

In addition, the Act established the rules for reporting, controlling and preventing money laundering under Section 330-333. These sections define the offences of failure of the regulated sector, nominated officers in the regulated sector, other nominated officers and tipping off.[135] The Act further gives an instruction to identify whether the required disclosure has been made for the purposes.[136]

Soon after, the HM Treasure published a report in 2004 to provide three principles of the anti-money laundering strategies in the UK. The three principles are effectiveness, proportionality and engagement. The three principles note that the UK shall maintain effective control of anti-money regulation in a cost-effective way and engage with all stakeholders and ongoing communication. Maintaining high international standards and ensuring effective enforcement are particularly highlighted in the report.[137] The report also instructs the regulatory structure of money laundering in the UK, including the primary legislation – Proceeds of Crime Act 2002; the secondary legislation – Money Laundering Regulations 2003; the industry and professional guidance, such as the Joint Money Laundering Steering Group (JMLSG) Guidance and the Institute of Chartered Accountants in England and Wales (ICAEW)

[133] Proceeds of Crime Act 2002 c. 29. pt. 7.

[134] The Proceeds of Crime Act 2002 (Crown Servants) Regulations 2003, SI 2003/173. reg. 342.

[135] Proceeds of Crime Act 2002 c. 29. ss. 330 - 333.

[136] ibid. s.339ZD.

[137] Home Treasury, 'Anti-Money Laundering Strategy' (2004) < http://wgfacml.asa.gov.eg/en/doc_interest/doc_sais/0%20UK%20Treasury%20AML%20strategy.pdf> accessed 8 January 2020. at p. 7.

Guidance; and relevant authorities. The FCA (former FSA) has been given the powers to prosecute criminally breaches of the money laundering regulations.[138]

The Money Laundering Regulation (MLR) was firstly adopted in 1993 and is updated progressively in 2001, 2003, 2007, 2011, 2017 and 2019, accordingly. Financial institutions and money business firms are required to submit suspicious transaction report since the MLR 1993. Particularly, the MLR 2003 first time includes e-money and dematerialised instruction in its regulatory scope.[139] Currently, firms are complying with the MLR 2017 and are adapting to their compliance process to the MLR 2019 (EU Exit).

The MLR 2003[140] defines money laundering as an act which falls within of the Proceeds of Crime Act 2002, s. 340 (11)[141] or an offence under of the Terrorism Act 2000 s.18.[142] It covers a wide range of relevant business activities, such as taking deposits, offering long-term insurance, providing investment-related services and issuing e-money. Interestingly, two provisions of the MLR 2003 may lead to difficulties in making adjudication. The first issue is the definition of money laundering under the Terrorism Act 2000 s.18(2) – 'It is a defence for a person charged with an offence under subsection (1) to prove that he did not know and had no reasonable cause to suspect that the arrangement related to terrorist property'. This may encourage defendants to provide misleading evidence to a great extent since it is difficult to identify if a person 'knew' or had 'no reasonable cause to suspect'. The second issue is that the MLR 2003 exclude mortgage from the regulated business activities in terms of money laundering regulation.[143] One could assume that it would lead to a large amount of illegal

[138] ibid. at p.14.

[139] The Money Laundering Regulations 2003, SI 2003/3075. reg. 2 (2).

[140] ibid. reg. 2 (1).

[141] '(11) Money laundering is an act which — (a) constitutes an offence under section 327, 328 or 329, (b) constitutes an attempt, conspiracy or incitement to commit an offence specified in paragraph (a), (c) constitutes aiding, abetting, counselling or procuring the commission of an offence specified in paragraph (a), or (d) would constitute an offence specified in paragraph (a), (b) or (c) if done in the United Kingdom'. Proceeds of Crime Act 2002 c. 29. s. 340 (11).

[142] '(1) A person commits an offence if he enters into or becomes concerned in an arrangement which facilitates the retention or control by or on behalf of another person of terrorist property — (a) by concealment, (b) by removal from the jurisdiction, (c) by transfer to nominees, or (d)in any other way. (2) It is a defence for a person charged with an offence under subsection (1) to prove that he did not know and had no reasonable cause to suspect that the arrangement related to terrorist property'. Terrorism Act 2000 c. 11. s. 18.

[143] The Money Laundering Regulations 2003, SI 2003/3075. reg. 2(3).

money flowing into the real estate markets and being laundered through a series of commercial activities.

In 2017, the legislative system brings two Regulations to anti-money laundering. The two Regulations are the Oversight of Professional Body Anti-Money Laundering and Counter Terrorist Financing Supervision Regulations 2017 (SI 2017/1301) and the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (SI 2017/692). The Oversight of Professional Body Anti-Money Laundering and Counter Terrorist Financing Supervision Regulations 2017[144] defines the supervisory duties and the powers of the financial authority, the FCA, in money laundering regulation under the Financial Services Act 2012[145] and FSMA2000.[146] The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017) effective on 26th June 2017.

The MLR 2017 provides a wider scope of the requirements for recordkeeping and transaction reporting of financial firms and banking and money businesses. It implements the EU fourth Anti-Money Laundering Directive and is in line with the Standards and Recommendations of the FATF. The Regulation requires high value dealers, casinos and auction platforms to carry out customer due diligence measures for cash payment in one or multiple linked transactions exceeding €10,000 Euros and €15,000 Euros for non-high value dealers.[147] However, exemptions apply for occasional financial activities if the annual turnover of firms/individuals is less than £100,000 and with other criteria are met or the occasional financial activity does not exceed 5% of the person's total annual turnover.[148] In addition, the MLR 2017 applies for credit institutions, financial institutions auditors, insolvency practitioners, external accountants and tax advisers, independent legal professionals, trust or company service providers, estate

[144] The Oversight of Professional Body Anti-Money Laundering and Counter Terrorist Financing Supervision Regulations 2017, SI 2017/1301. reg. 3.

[145] 'An Act to amend the Bank of England Act 1998, the Financial Services and Markets Act 2000 and the Banking Act 2009; to make other provision about financial services and markets; to make provision about the exercise of certain statutory functions relating to building societies, friendly societies and other mutual societies; to amend section 785 of the Companies Act 2006; to make provision enabling the Director of Savings to provide services to other public bodies; and for connected purposes'. Financial Services Act 2012 c. 21. at Introductory Text.

[146] The Financial Services and Markets Act 2000 c. 8.

[147] The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017/692. reg. 27(b).

[148] ibid. regs. 15 (3) (a) and 15 (3) (c).

agents, high value dealers, casinos, as well as electronic money issuers.[149] Moreover, firms must establish an internal compliance measure to carry out a risk assessment in relation to money launderings, such as policies, controls and procedures and relevant training.[150] E-money issuer and payment service providers must appoint a person to act as a central contact in the UK for its supervisory authority on any issue relating to the prevention of money laundering, including any e-money issuer or payment service provider established in the UK or has its head office in an EEA state. Branches of e-money issuer or payment service provider are not included in the requirement.[151]

The UK has updated two versions of the MLR in 2019, one is updated for adopting the EU fifth Anti-money Laundering Directive[152] and another one is for the EU Exit.[153] The Money Laundering and Terrorist Financing (Amendment) Regulations 2019 came into force on 10 January 2020, while the UK left the EU on 31 January 2020, I shall review the MLR 2019 (Amendment) and the MLR 2019 (EU Exit), respectively.

The MLR 2019 (Amendment) implements the EU Fifth AML Directive in the UK.[154] The regulation first time includes crypto asset exchange providers and custodian wallet provider in the regulatory scope in the UK under the category of Credit Institution.[155] This is in line with the requirement of the EU fifth AML Directive. The FCA is the supervisory authorities of crypto asset exchange providers and custodian wallet provider in terms of anti-money laundering.[156]

The MLR 2019 (Amendment) also widens the regulatory scope in terms of commercial activities, such as land letting agent and art market participants.[157] It adopts more strict due diligence measures, including a requirement of reporting to Companies House about the

[149] ibid. reg. 8.

[150] ibid. reg. 21.

[151] ibid. reg. 22.

[152] The Money Laundering and Terrorist Financing (Amendment) Regulations 2019, SI 2019/1511.

[153] The Money Laundering and Transfer of Funds (Information) (Amendment) (EU Exit) Regulations 2019, SI 2019/253.

[154] The Money Laundering and Terrorist Financing (Amendment) Regulations 2019, SI 2019/1511. reg. 3 (1) (c).

[155] ibid. reg. 14A.

[156] ibid. regs. 7(1), 54 (1A) and 58.

[157] ibid. regs. 13 and 14.

information discrepancies between customer due diligence and business registration;[158] the requested report of the minimum amount of electronic money transactions;[159] payment using an anonymous prepaid card issued in a third country[160] (the regulation of anonymous prepaid cards comes into force on 10th July 2020); [161] all transaction records shall be kept for five years.[162] The recordkeeping requirement is interpreted under the MLR 2019 (Amendment) s. 74.[163]

The MLR 2019 (EU Exit) came into force on 31st January 2020 when the UK left the EU.[164] The MLR 2019 (EU Exit) is amended based on the MLR 2017.[165] The regulation substitutes provisions that are in line with the EU Laws and Directives previously, such as the EU fourth Anti-money laundering Directive.[166] It also removes the power of the European Supervisory Authorities and some influences of the single market system, accordingly. The FCA is the authority carrying out the money laundering regulation under the FSMA 2000 and the RAO 2001.[167] Crypto assets are not yet included in the MLR 2019 (EU Exit). Since the MLR 2019 (Amendment) is still in force during the transition period of Brexit until December 2020, the money laundering regulation in the UK may be adjusted, accordingly.

In addition, under UN Charter article 41 of the United Nations Act 1946, the UK government has been empowered to give effect to decisions on economic sanctions in relation to money laundering. The current sanctions about money laundering adopted in the UK are the Sanctions and Anti-Money Laundering Act 2018. The Act rules illicit activities concerning money laundering and terrorist financing complying with the United Nations obligations and other international obligations. This Act indicates the standards and international obligations of the UK in terms of money laundering regulation and how the UK authorities regulate money laundering activities in the British Overseas Territories. The Act aims to enhance national and

[158] ibid. reg. 30 (A).

[159] ibid. regs. 38 (1) and 38 (2).

[160] ibid. reg. 38 (4).

[161] ibid. reg. 5 (5) (c)

[162] ibid. reg. 45 (G).

[163] See detailed discussion and analysis in the section 5.4.3, "Anti-money laundering in the UK" of this thesis.

[164] The Money Laundering and Transfer of Funds (Information) (Amendment) (EU Exit) Regulations 2019, SI 2019/253. reg. 1 (2).

[165] ibid. reg. 2.

[166] ibid. reg. 3 (3).

[167] ibid. reg. (3) (f) (ii).

international peace and security for furthering foreign policy objectives and to strengthen the anti-money laundering and terrorist financing policies and the integrity of the international financial system in line with the standards of the FATF.[168] The provisions of Part 2 of this Act specifically refer to money laundering. It clarifies the purposes of making the provision; the referencing laws that define "money laundering", such as the Proceeds of Crime Act 2002, s.340(11); the reporting requirements for register of beneficial owners of overseas entities; the requirements of assisting in detection, investigation or prevention of money laundering for public registers of beneficial ownership of companies in British Overseas Territories, such as establishing a publicly accessible register in each government's jurisdiction under the provisions of Part 21A of the Companies Act 2006.[169]

Although the UK left the EU on 31st January 2020, the UK authorities are expected to maintain the highest standard of the legislative system without ruining the EU treaties after the transition period. Therefore, the UK authorities may restructure a comprehensive agreement to ensure a smooth transition and continuously cooperate with the EU in terms of the international anti-money laundering regulation.

Currently, UK firms comply with the MLR 2019.[170] I will provide intensive discussion accordingly in Section 5.4.3 of this thesis.

### 3.1.2 Money Laundering Regulation in the EU

The EU has made a progressive amendment of the Anti-money Laundering (AML) Directives along with the market alteration and technology development since the first AML Directive was adopted on 10 June 1991. At the time of writing, the EU member states have adopted the Fifth AML Directive by 10 January 2020.

The Directive 91/308/EEC of 10 June 1991[171] known as the first AML Directive of the EU. The Directive gives the definition of credit and financial institution and defines money laundering in accordance with the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1998. It established a framework of the coordination and cooperation within the EU member states in relation to international money laundering. It

[168] Sanctions and Anti-Money Laundering Act 2018 c. 13. at Introductory Text.

[169] ibid. regs. 49-51.

[170] The Money Laundering and Terrorist Financing (Amendment) Regulations 2019, SI 2019/1511.

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

requires banks and financial firms to submit transaction reports and being responsible for recordkeeping. The Directive requested credit institutions and financial institutions of the EU member states to guard against money laundering by checking identities of customers, monitoring transactions and reporting suspicious transactions to the authorities. Credit institutions and financial institutions must carry out oversight procedures for transactions exceeding €15,000 Euros unless the customer is also a credit institution or financial institutions.

The Directive 2001/97/EC of 4 December 2001[172] known as the second AML Directive of the EU extended the regulatory scope of anti-money laundering in the EU. The Directive covered the regulated activities of money laundering beyond drug offences, like gambling and casinos. It also included a wider range of businesses other than financial institutions and credit institutions, such as investment firms, currency exchange offices and money transmitters. The Directive also clarified of the jurisdictions regarding the reporting process. For example, competent authorities in member states for receiving suspicious transaction reports from branches of credit and financial institutions having head office in another member state. Professions that are vulnerable to money laundering are requested to carry due diligence measures including customer identification, record keeping and the reporting of suspicious transactions to a limited number of activities. Professions include notaries and independent legal professionals who providing consultancy services in financial or corporate transactions.[173]

The Directive 2005/60/EC of 26 October 2005[174] known as the third AML Directive of the EU. The Directive started focusing on international coordination and cooperation following the recommendations of the FATF and establishing international standards for due diligence measures of customers. The standardised due diligence measures include entities, individuals and ultimate beneficial owners, as well as sources of funds and transaction objects. Also, property transactions and related services, such as real estate agents and insurance intermediaries, are embodied in the regulatory scope. The Directive also requests entities appointing appropriate persons to be responsible to carry out internal due diligence measures

[172] Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering [2001] OJ L344/76.

[173] ibid. at recitals.

[174] Directive 2005/60/EC of the European Parliament and of The Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing [2005] OJ L 309/15.

and submit suspicious transaction report to the FIUs, accordingly. A new EU Committee on the Prevention of Money Laundering and Terrorist Financing was established under this Directive and the regulation of terrorist financing was introduced in the regulatory scope.[175]

The Directive 2015/849/EU of 20 May 2015 known as the Fourth AML Directive enacted in 2015.[176] The Fourth AML Directive first time mentioned electronic money[177] and data protection[178] in the regulatory framework of the anti-money laundering regulation. It indicates the importance of timely and efficient access to data and information between FIUs within the Union due to the transnational character of money laundering and terrorist financing. It introduced enhanced due diligence measures complying with the international standards and the revised FATA Recommendations of February 2012.[179] For instance, improving the efficiency of the due diligence measures on beneficial ownership. It also introduced stricter provisions to the use of cash combating money laundering, such as lowering the thresholds of monitoring payment to €10,000 Euros.[180]

The Directive 2018/843/EU of 30 May 2018 known as the Fifth AML Directive came into force in 2018 and all member states are requested to implement the Directive into their national laws by 10 January 2020. The Directive interprets the role of crypto assets in the financial system and indicates the related risks to anti-money laundering regulation. The Directive requests member states carrying out regulatory schemes for crypto assets exchanges and wallet providers, such as business registration and recordkeeping.[181] The Directive again emphasises the importance of coordination and cooperation between member states and urges a standardised database for efficient information sharing within the FIUs, especially crypto assets transactions (detailed discussion see the section 4.3 illicit activities of crypto assets in the EU

[175] ibid. recital (44) and Art. 41. at pp. 19 and 31.

[176] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council and Commission Directive 2006/70/EC [2015] OJ L141/73.

[177] ibid. ch. II, Art 12. at pp. 91 - 92.

[178] ibid. ch. V. at pp. 101 - 102.

[179] ibid. recital (4). at p. 74.

[180] ibid. art. 2 para. 1 (3) (e) and art. 11(c). at pp. 84 and 91.

[181] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU [2018] OJ L156/43.

of this thesis). However, the Directive regulates money laundering activities of only one type of crypto assets – the exchange tokens, member states shall establish regulatory schemes for other types of crypto tokens, accordingly, such as security or investment tokens and utility tokens.

I will provide a detailed discussion of the 5AML Directive and crypto assets businesses in Section 6.3.1 of this thesis.

## 3.2 The Role of Crypto Assets in Money Laundering

Money laundering is a process that transits illicit proceeds into the financial system for legitimate use.[182] The anonymity of crypto assets weakens the identifiability and traceability of transactions. The encrypted and unrecorded/unreported transactions through peer-to-peer networks create new obstacles to anti-money laundering investigations.[183] Besides, some countries have set up crypto-Automatic Telling Machine (ATM) for purchasing and transferring crypto assets in addition to online exchanges. Although it is too early to say if these crypto-ATMs have been used for illicit activities, they create a conduit between offline cash and online crypto assets. According to 'Coin ATM Radar.com', North America and Europe have held roughly 95.6% of the crypto-ATMs in the world in 2019, and the number of crypto-ATM has been growing over time.[184] Either online or offline, the anonymity and unregulated transactional networks of crypto assets have created a new platform for financial crimes, including money laundering.

The EU and the US member states have established Intelligence Agencies to monitor and trace crypto assets related crimes – the Financial Intelligence Units (FIUs) in the EU and the Financial Crimes Enforcement Network (FinCEN) in the US, and have successfully combated several organised criminal groups that engage in money laundering using crypto assets. However, the different Laws and regulatory rules across jurisdictions can cause obstacles and delay in the investigation given the fact that money laundering using crypto assets is likely to be a cross-border activity. Although some countries, such as EU member states, have agreed to share relevant information within the FIUs, it takes time to create unified databases and a

[182] Waleed Alhosani, *Anti-Money Laundering : A Comparative and Critical Analysis of the UK and UAE's Financial Intelligence Units* (Palgrave Macmillan 2016). at pp. 3 - 4.; Ryder (n 13). at p. 12.

[183] Alhosani (n 182); Forgang (n 101).

[184] https://coinatmradar.com/charts/ accessed 14 April 2019. (n/d).

harmonised legal system to deter money laundering crimes and to clarify jurisdictions, legal provisions and sentencing standards within the EU.

Laundering illicit earnings consists of three stages: placement, layering and integration. The placement stage describes the introduction of illegal money obtained from predicate offences (such as drug dealing) into the financial system. The layering stage aims to distance the money from the predicate offences. The final stage is to reintegrate the laundered money back into financial systems.[185]

Crypto assets may come into play in the placement stage. First, crypto assets may be used to distribute illicit earnings from predicate offences into the financial system anonymously and in an untraceable manner. Illicit earnings of crypto assets include stealing crypto assets and selling controlled products – selling drugs at online marketplaces, to give one obvious example.

Normally, stealing crypto assets is considered stealing virtual property and misusing computers in the stage of 'placement',[186] whereas adopting crypto assets to distribute or to dispense prohibited goods is treated differently by the Law. The activity of distributing or dispensing prohibited goods does not necessarily involve accessing unauthorised computers and data, while crypto assets can be used as a means of payment to collect illicit earnings. For example, the case of United States v Matthew Jones [2014],[187] where the defendant was charged with selling and distributing prohibited goods under 21 U.S. Code § 841 – 'Prohibited acts A' instead of a violation of misusing computers.

The stage of layering and reintegration are closely related to the financial system. It is very likely that electronic transaction activities, such as online banking, online gambling and online auctions, are involved in these stages – anonymity is an important incentive for money launderers. Crypto assets play an important role in the stages of layering and reintegration. The anonymity and efficiency of crypto asset transactions collectively create an ideal shield for secluding illicit earnings from transaction parties. It is perhaps a preferable approach for money launderers. For instance, instead of offering commissions to individuals, launderers can transfer small amounts of money that are below the reporting thresholds of regulatory requirements through a large number of pseudonymous accounts to segregate illicit money,[188] Meanwhile,

[185] Waleed Alhosani (n 182), pp.3 - 4. Forgang (n 101).

[186] Murray (n 55). at Part III: Digital Content and Intellectual Property Rights.

[187] United States v Matthew Jones [2014] No.6:14-mj-1233, So. 1 (M.D. Fla.).

[188] Ryder (n 13). note 21. at p. 12.

launderers can set up automatic transaction orders using software that works 24/7. Besides, the crypto assets ATMs provide an additional channel to convert offline cash to crypto assets anonymously. Since the anonymity of crypto assets is the key characteristic that assists launderers to distance illicit earnings from predicate offences, the regulatory rules in many countries are set for crypto assets business registration to ensure account identification and transaction recordkeeping.

In June 2015, the Financial Action Task Force (FATF) published a guidance paper on the global Anti-Money Laundering (AML) and counter-terrorist financing (CFT) to national authorities worldwide.[189] The guidance paper prospectively identified the associated risks of crypto assets to the AML/CFT measures and clarified the relevant FATF Recommendations to convertible crypto assets exchanges. The guidance paper provides explanations and interpretations of the technological applications and functions of crypto assets and establishes a standard to help authorities to address the risks of crypto assets in relation to AML and CFT as well as to develop regulatory frameworks. The existing FATF Recommendations are applicable to some countries, including Canada, China, EBA, France, Germany, Italy, Russia, Singapore, South Africa, Switzerland, the UK and the US. Of which, the EBA is the European Banking Authority.

Additionally, the FATF guidance paper focuses on convertible crypto assets and related AML/CFT matters due to its higher risks and differentiates the types of crypto -assets to centralised and decentralised crypto assets. The guidance paper defines convertible crypto assets are 'the virtual currency can be exchanged for fiat currency' and classifies the convertible crypto assets (CCAs) into centralised and decentralised. Of which, the centralised CCAs refer to crypto assets that have a single administrator. The single administrator can be a third party who controls the system, such as issuing crypto assets and maintaining a central payment ledger, and holding authority to redeem the crypto assets; decentralised crypto assets are 'distributed, open-source, math-based peer-to-peer virtual currencies that have no central

[189] 'FATF is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standards'. Financial Action Task Force (n 108). at. p. 1.

administrating authority, and no central monitoring or oversight'.[190] Under this classification, Bitcoins are defined as convertible and decentralised crypto assets.

Moreover, the FATF suggests that countries shall all carry out a Risk-Based Approach (RBA) Following the FATA Recommendations 2012[191] and ensure measures associated with preventing or mitigating global money laundering and terrorist financing risks are commensurate with the risks identified.[192] The Recommendations for national authorities combating AML/CFT in terms of crypto assets embodies: a) identifying, clarifying and assessing the types of crypto assets (convertible or unconvertible, centralised or decentralised) and associated risks; b) cooperation and coordination; business registration for legal or natural persons; c) monitoring new financial technology developments; d) monitoring cross-border wire transfers; e) adequate regulation and supervision of convertible crypto assets; f) establishing sanctions to deal with natural or legal persons that fail to comply with the AML/CFT requirements; g) efficient and effective international cooperation.[193]

The guidance paper also gives Recommendations specifically to convertible crypto assets exchanges and any other types of entities. These Recommendations are a) identifying, clarifying and assessing the types of crypto assets and associated risks; b) undertaking customer due diligence measures for a one-off transaction greater than USD/EUR 15,000 and Recommendation 16; and c) recordkeeping and suspicious transaction reporting; d) monitoring financial technology innovation.[194]

The abovementioned Recommendations provided by the FATF are the guidelines of the EU Fifth Anti-Money Laundering Directive[195] and the UK Sanctions and Anti-Money Laundering

[190] ibid. pp. 23 and 27.

[191] FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - The FATF Recommendations' (2012).

[192] Financial Action Task Force (n 108). para. 23.

[193] FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - The FATF Recommendations' (n 191). Recommendations 1, 2, 14, 15, 16, 26, 35 and 40.

[194] ibid. Recommendations 1, 10, 11, 15, 20 and 22.

[195] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU [2018] OJ L156/43. recitals (4) and (18). at pp. 44 and 46.

Act 2018.[196] However, the guidance paper only addresses AML/CFT related matters and risks. General regulations such as consumer protection and prudential regulation, as well as other none-AML/CFT related measures like anti-fraud and cybersecurity are not included.

The FATF Recommendation is updated in June 2019[197] and the guidance on crypto assets and service providers is amended accordingly.[198] The updated FATF Recommendations regarding crypto assets are minor mainly in Recommendation 15. The Recommendation 15 revises the definition of 'virtual asset" and "virtual asset service provider' to clarify how AML/CFT requirements apply in the context of crypto assets[199] and inserts a new interpretive note to sets out the application of the FATF Standards to crypto asset activities and service providers.[200] The revised Recommendations define a virtual – asset as 'a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations'.[201] Under this definition, 'new virtual assets' underpinned by the DLT are distinguished from existing catalogues of payment methods and financial instruments. This also means crypto assets shall be treated separately from traditional financial products regardless of their functions or applications.

The updated Recommendations define "the virtual asset service provider" as 'any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural

[196] Sanctions and Anti-Money Laundering Act 2018 c. 13. at Introductory Text.

[197] FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - The FATF Recommendations Updated June 2019' (2019).

[198] FATF, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' (2019) <https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf>accessed 14 February 2020.

[199] FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - The FATF Recommendations Updated June 2019' (n 197). at pp. 126 - 127 and 132.

[200] ibid. at pp. 70 - 71, and 132.

[201] ibid. at p. 126.

or legal person." Generally, the "virtual asset providers" include crypto assets exchanges, custody wallet providers, transaction service providers and ICOs'.[202]

Furthermore, the new 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, 2019' provides a more detailed interpretation of the changes in the FATF Recommendations 2019. For example, a threshold of occasional transactions of USD/EUR 1,000 is added to the FATF Recommendation 10. In addition, the Guidance Paper 2019 gives examples of the jurisdictional approaches and the Laws and enforcement processes in some countries for AML/CFT with respect to the FATF Recommendations, such as Italy and Japan, and highlights the importance of international cooperation and coordination.[203]

Although the AML Directive of the EU[204] and the MLR 2019 of the UK[205] have not yet revamped the regulatory requirements in accordance with the updated FATF Recommendations 2019,[206] the majority of crypto assets related activities in relation to money laundering are covered by these existing regulations. For instance, ICOs are regulated under national Laws[207] and crypto assets exchanges, transaction service providers and custody wallets providers are regulated under the Fifth AML Directive implemented in the national Laws.

[202] The FATF defines that 'virtual asset service providers include i. exchange between virtual assets and fiat currencies; ii. exchange between one or more forms of virtual assets; iii. transfer of virtual assets; iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset'. ibid. at p. 127.

[203] FATF, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' (n 198). at pp. 46 - 54.

[204] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU [2018] OJ L156/43.

[205] The Money Laundering and Terrorist Financing (Amendment) Regulations 2019, SI 2019/1511.

[206] The 'Guidance paper' was published in June 2019 after the EU Fifth AML Directive promulgate in May 2018. FATF, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' (n 198).

[207] For example, the Companies Act 2006 c. 46. and The Financial Services and Markets Act 2000 (Regulated Activities) Order 2001, SI 2001/544.

# 4 Central Bank Cryptocurrency

## 4.1 The Concept and Underlying Rationale

Crypto assets have started challenging legal tender issued by central banks through their unique features and global networks offered by the DLT and Block Chain.[208] First, legal tender plays the role of intermediation for value exchange over centuries in almost every country in the world. Second, the value carried by national currencies varies across countries and the value differences between currencies are converted by international currency exchange rates.[209] Central banks make monetary policies to ensure the stability of their national economies and financial systems. However, crypto assets create new intermediation of exchange that is accepted within their worldwide networks and does not require currency exchange in cross-country transactions.

Even though crypto assets present advantages over legal currencies for being more efficient and more secure, they are neither issued nor circulated by central banks. The most discussed issues of crypto assets in the banking and financial sector are their roles in the financial system and the decentralisation of the banking system caused by the DLT, as the DLT offers a unique way to issue, distribute and transact crypto assets without requiring a third party, such as banks. In addition, the anonymous of payers and payees, as well as unknown transaction objectives, of crypto assets has caused obstacles in financial regulation, although it is supposed to enhance user confidentiality. Therefore, almost all countries have announced that crypto assets are not legal tender or a representative of fiat currency. However, this has not stopped crypto assets becoming popular in the financial sector due to the distinct properties of crypto assets, including efficiency, confidential and irreversible recordkeeping.[210]

These distinct properties of crypto assets can be used not only by market participants but also by regulatory agencies. The DLT and Block Chain make transactions easier and more economical,[211] which will benefit the public. Additionally, with the DLT, central banks can access personal data without inquiring third parties, which helps to avoid duplications in

[208] Claudio Borio and others, 'Central Bank Cryptocurrencies' (2017) BIS Quarterly Review.

[209] Adam Smith, *The Wealth of Nations* (Bantam Classics 1776). Book One, Chapter 4 - Chapter 7.

[210] Li and others (n 97). at pp. 4 - 5.

[211] Forgang (n 101). at pp. 6 - 7.

transaction reports.[212] Meanwhile, regulators can set up alerts using algorithms and Artificial Intelligence (AI) to monitor all abnormal transactions on distributed ledgers directly and timely – existing oversight of suspicious transactions is relying on reports submitted by banks and payment platforms on a regular basis.[213] Moreover, the irreversible and immutable transaction records on peer-to-peer networks can make recordkeeping more transparent. These properties of the DLT can make oversight scheme and reporting processes simpler and less costly (if not considering the cost of data storage and maintenance).

Other than the efficiency improvement and cost-saving in terms of market oversight and facilitate payments, DLT can also assist in preventing transaction fraud. It is because only relevant transaction parties can access paired encrypted keys that are more difficult to duplicate or counterfeit, at least cannot be done by the current technology. In the meantime, the digital currency underpinned by the DLT also gives chances to countries that plan to eliminate the influence of US dollars on their international trade. For instance, Venezuela has struggled trading crude oil due to economic sanctions of the US since 2017. The economic sanctions have caused incredible depreciation of Venezuelan Bolívar (VEF) against US Dollars. Such deprecation has driven the value of Venezuelan currency away from the physical value of crude oil and almost wiped Venezuela from the markets despite the high international demand for crude oil. Thus, the Venezuelan government created government cryptocurrency against crude oil to battle with the issue.[214] Although this may be an extreme case, it could be a sign of the desires of establishing a new order for international trade and decoupling from US Dollars. Therefore, central bank cryptocurrencies may be a new way to protect the values of domestic goods in the situation of currency depreciation against US Dollars.

## 4.2 Current Plans of Central Banks

The benefit of the DLT has led to some central banks started to evaluate the possibility of issuing Central Bank Crypto Currencies (CBCCs) to enhance information security and monitor

[212] 'all transactions in a blockchain are stored onto a single ledger. As transactions are ordered by time, the present state of the system (in the case of a financial blockchain, the collection of all users' balances) is uniquely determined by the ledger. Storing all transaction history has other benefits such as increased regulatory compliance and the ability to determine the state of the system at any specified moment of time by "replaying" corresponding transactions'. BitFury Group and Garzik (n 56). at p. 6.

[213] Sims, Kariyawasam and Mayes (n 104). at p. 24 - 25. Brown (n 15). at p. 333. ibid. at p. 13.

[214] 'Venezuela Petro Cryptocurrency (PTR)--English White Paper' (n 34).

transaction activities. The UK has taken the initial step and launched a study inquiring the possibilities of applying DLT to issue CBCCs in March 2020.[215]

Reyes suggests that applying Block Chain technology into financial regulation could help to improve security while identifying abnormal online activities.[216] However, CBCCs are not easy to be issued straightaway like cash. Central banks may have to examine the balancing point between the amounts issued for cash and CBCCs in terms of monetary policies. This is essential to national currency circulation and financial stability. Additionally, central banks need to evaluate the capacity of data storage and the cost of database maintenance. CBCCs may require an infinite capacity to store transaction data. This is because the DLT generates multiple nodes for each transaction thus needs more data capacities than normal bank recordkeeping, and transaction records on Distributed Ledgers (DL) are not supposed to be removable.[217] This may cause an issue in data protection as users shall have the right to remove their data.[218] Therefore, it is anticipated that the datasets of CBCCs transaction would be larger than those in each bank. Furthermore, central banks must assess network security against cyberattack. Unlike traditional recordkeeping carried out by individual banks, the data stored on the DL contain transactions records of all banks and are accessible at any node on the DL. Therefore, ensuring the security of CBCCs is vital to financial stability and user confidentially. Meanwhile, the global impact of CBCCs issuance also needs to be taken into account.

The BIS published a working paper to discuss the challenges and benefit of issuing CBCCs in 2016.[219] This working paper studies a taxonomy of money and identifies two types of CBCCs – retail CBCCs and wholesale CBCCs. The paper differentiates the two types of CBCCs from other forms of central bank money including cash and reserves and differentiates the characteristics of CBCCs from existing payment methods. The paper also discusses the solutions to utilise the alleged advantages of DLT for CBCCs retail or wholesale users such as anonymity, by having a central bank account and giving access to it. The paper also suggests that given the fact that cash usage is declining in many countries, central banks may consider issuing digital currencies alternative to cash for consumer preferences like privacy and efficiency in terms of payment, clearance, and settlement. However, central banks must ensure

[215] Bank of England (n 110).

[216] Reyes (n 4). at pp. 9 - 12.

[217] Nakamoto (n 65). at pp. 1 - 2.

[218] Data Protection Act 2018 c.12. s. 59 (6) (d).

[219] Bech and Garratt (n 107).

financial and monetary stability from a global point of view, as well as enhance the cyber-resilience of CBCCs.

The Bank of Japan also published a working paper in 2019 regarding the possibility and benefits of applying DLT to issue CBCCs.[220] Although Japan has demonstrated great financial inclusions of digital innovation and embraced the emergence of crypto assets, the Bank of Japan stated that Japan has no immediate plans to set up an alternative payment method to replace paper-based banknotes, such as CBCCs. The Bank of Japan has recognised the beneficial aspects of crypto assets, such as efficiency improvement for payments and transactions, whereas also acknowledged related risks that associate to monetary policies, for instance, liquidity risks and cybersecurity. Additionally, the Bank of Japan has realised that along with the information technology development, new types of money with the variety of functions may be possible to emerge in the future. These functions include but not limited to payments, information attached to payments and executing transactions. The bank of Japan has also emphasised the possible impacts of CBCCs on financial structure and economy, as well as on the utilisation of data and the dynamics of network externality.

Bank of England studies the benefit of issuing CBCC to economic growth and efficiency gains in 2016.[221] The working paper looked into the macroeconomic impacts of issuing CBCCs. In this paper, CBCCs are defined as 'universally accessible and interest-bearing central bank liability, implemented via distributed ledgers, that competes with bank deposits as medium of exchange'. The paper employs a monetary-financial DSGE model and simulates the situation of issuing CBCCs into the economy of the United States between 1990 and 2006, the period of the pre-crisis. The paper discovers that introducing CBCCs can boost nearly 3% of GDP due to reductions in real interest rates, distortionary taxes, and transaction costs and CBCCs used as a second monetary policy instrument may enhance the ability central banks to stabilise their business cycles.

A joint report of the BoE, The FCA and the HMT in 2018 discusses the impact and risks of the DLT and crypto assets products on the financial system and underlines that crypto asset is not

[220] Noriyuki Yanagawa and Hiromi Yamaoka, 'Digital Innovation, Data Revolution and Central Bank Digital Currency' (2019) 19-E-2 Bank of Japan.

[221] Barrdear and Kumhof (n 109).

a currency nor legal tender.[222] The Bank of England also underlines that the Bank has no immediate intention to issue CBCCs although some research is set in progress.[223]

On 12 March 2020, the BoE published a discussion paper on the CBCC, or Central Bank Digital Currency (CBDC) named by the BoE.[224] The discussion paper aims to consult whether the UK central bank should embrace the new financial technology and provide the public electronic money, the Central Bank Digital Currency (CBDC), as a complement to paper-based banknotes. The BoE recognises the benefits of the CBDC saying that it could provide a privately issued and risk-free form of money to households and businesses with a new way to make payments. The BoE suggests that the CBDC could also 'contribute to a more resilient, innovative and competitive payment system for UK households and businesses'. In the meantime, the BoE is aware of the risks and challenges for maintaining monetary and financial stability with the CBDC. The Bank claimed that the CBDC will be carefully designed since it has high relevance to almost of everything that the Bank is doing every day. Nevertheless, the BoE has not yet made the decision of issuing the CBDC.

The financial markets seem keen to see a central bank currency or an official crypto currency emerging. Rumours are going around on the internet about CBCCs issuing. The biggest rumour was China issuing its own CBCCs in 2019 and was reported by reputable mass media around the world, such as the Financial Time,[225] the CNBC[226] and the Forbes.[227] The mass media even specified the companies and banks that would be selected in the first cohort to distribute the CBCCs in China. It turned out a piece of groundless information and the Central Bank of China, the People's Republic Bank of China (PBOC), had to make an official announcement to refute

[222] HM Treasury, FCA and Bank of England (n 82). para. 2.13 at p. 12.

[223] 'Digital Currencies | Bank of England' (n 87).

[224] Bank of England (n 110).

[225] 'What Is China's Digital Currency Plan? | Financial Times' <https://www.ft.com/content/e3f9c3c2-0aaf-11ea-bb52-34c8d9dc6d84> accessed 3 March 2020.

[226] 'China Central Bank Close to Releasing Digital Currency: PBOC Official | CNBC' <https://www.cnbc.com/2019/08/12/china-central-bank-close-to-releasing-digital-currency-pboc-official.html> accessed 3 March 2020.

[227] 'Alibaba, Tencent, Five Others To Receive First Chinese Government Cryptocurrency | Forbes' <https://www.forbes.com/sites/michaeldelcastillo/2019/08/27/alibaba-tencent-five-others-to-recieve-first-chinese-government-cryptocurrency/> accessed 3 March 2020.

the fraudulent news on 13 November 2019.[228] However, the official announcement of the PBOC somehow is not displayable on Google search results. The fraudulent information is still ongoing outside China. This situation may raise concerns over international counterfeiting and fraudulence of CBCCs, as well as ICOs. Authorities may have to become more vigilant in order to protect investors and consumers.

In spite of the fact that the DLT may bring the alleged beneficial to the financial system and the public, most of the central banks have clarified that they have no plans to introduce a DLT-based digital currency to replace paper-based banknotes. Alternatively, the central banks are carrying out intensive research to understand more about the new financial product and its impact. It is too soon to make a conclusion whether the national central banks should adopt the DLT to issue CBCCs and if it benefits the financial markets and consumers, as well as national economies. Other than being proficient in the technology that applies to CBCCs, issuing a legal tender also requires thorough studies to evaluate the impact of CBCCs on financial stability, economic growth, social networks, cybersecurity and data protection, legislation and enforcement, international recognition, property rights and so on. There are possibilities to study the effectiveness of legislative frameworks regarding issuing CBCCs if official progress made public.

[228] 'Announcement on Fraudulence of Issuing and Promoting Digital Fiat Currency in the Name of PBC | the People's Republic Bank of China' (2019) <http://www.pbc.gov.cn/en/3688110/3688181/3921119/index.html> accessed 3 March 2020.

# 5 An Insight into the Regulation of Crypto Assets in the UK

## 5.1 The Legal Basis of Crypto Assets Regulation in the UK

The UK financial markets are regulated by two authorities, the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA). The FCA is 'the conduct regulator for financial services firms and financial markets in the UK and the prudential regulator'.[229] The FCA has been given the power to regulate crypto assets activities in 2019 and has established a regulatory framework of crypto assets under relevant primary and secondary legislation. The fundamental Laws and Regulations applied to crypto assets regulation include the Financial Services and Markets Act (FSMA) 2000,[230] The Perimeter Guidance manual (PERG) 2019,[231] the Financial Services and Markets Act 2000 (Regulated Activities) Order (RAO) 2001,[232] The Electronic Money Regulations (EMR) 2011[233] and the EU Market in Financial Instrument Directive II (MiFID II).[234] The 'UK implements the MiFID II through the form of a combination of legislation made by HM Treasury, including a number of Acts, Statutory Instruments and rules embodied in the FCA Handbook and the PRA Rulebook'.[235] These include the FSMA 2000, RAO 2001, the Recognised Investment Exchanges (REC) 2020,[236] the Market Abuse Regulation (MAR) 2014[237] and the Data Reporting Services Regulations (DRSR) 2017,[238] There are other authorities involved in crypto assets activities due to the complexity of the combined features of information technology and finance. These authorities are the Bank of England and Her Majesty's Treasury.

The first official assessment of crypto assets in the UK takes place in October 2018 – A joint publication of the Her Majesty's Treasury (HMT), the Financial Conduct Authority (FCA) and the Bank of England (BoE) titled "Crypto assets Taskforce: Final Report".[239] Following the

[229] <https://www.fca.org.uk/about/the-fca> accessed on 11 November 2019

[230] The Financial Services and Markets Act 2000 c. 8.

[231] FCA, 'The Perimeter Guidance Manual' (n 42).

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

[233] Electronic Money Regulations 2011, SI 2011/99.

[234] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU [2014] OJ L173/349.

[235] FCA, 'The MiFID 2 Guide' (2020).

[236] FCA, 'Recognised Investment Exchanges' (2020).

[237] The Financial Services and Markets Act 2000 (Market Abuse) Regulations 2014, SI 2014/3081.

[238] The Data Reporting Services Regulations 2017, SI 2017/699.

[239] HM Treasury, FCA and Bank of England (n 82).

Crypto assets Taskforce Report, the UK authorities have started setting up regulatory schemes progressively for crypto assets products and services.

Soon after, the FCA published a consultation paper in January 2019 titled "CP19/3: Guidance on Cryptoassets UK" aiming to collect suggestions and comments on the initial regulatory frameworks.[240] Within six months, the FCA received feedback from 92 parties of 10 sectors in the markets, including large banks, trade associations, consultancies, fintech firms, crypto assets issuers, crypto asset exchanges, custody service providers, law firms, technology firms, academia and individuals. There are approximately nine firms in each sector on average. Based on the feedback, the FCA finalised the guidance of crypto assets businesses in July 2019 by virtue of a document titled 'Guidance on Crypto assets Feedback and Final Guidance to CP 19/3'. The objective of the final guidance is to provide clarification on the types of crypto assets falling within and outside the regulatory remits of the FCA, meanwhile, to set forth the obligations on market participants in relation to crypto asset businesses. Ensuring consumer protection is also one of the main objectives of the final guidance paper.[241]

The guidance paper provides instructions for firms to identify if their token businesses require authorisation. Firms shall identify firstly if they are carrying on activities by way of business in the UK under the PERG 2019.[242] For example, person/persons offering goods or services for regular gain in the UK is/are considered Carrying on Regulated Activities by Way of Business under the EPRG "2.3 the business element" and Section 22 "Regulated activities", Section 418 "Carrying on regulated activities in the United Kingdom" and Section 419 "Carrying on regulated activities by way of business" of the FSMA 2000. Of which, Section 22 of the FSMA 2000 provides general definitions of the regulated activities;[243] Section 418 of the FSMA clarifies whether person/persons is/are carrying on regulated activities in the UK. This includes the place of business registration and operation, managers and overseas business providing

[240] FCA, 'CP19/3: Guidance on Cryptoassets UK' (n 83).

[241] FCA, 'Guidance on Cryptoassets Feedback and Final Guidance to CP 19/3' (n 35).

[242] FCA, 'The Perimeter Guidance Manual' (n 42).

[243] '(1) An activity is a regulated activity for the purposes of this Act if it is an activity of a specified kind which is carried on by way of business and — (a) relates to an investment of a specified kind; or (b) in the case of an activity of a kind which is also specified for the purposes of this paragraph, is carried on in relation to property of any kind; and (4) "Investment" includes any asset, right or interest. (5) "Specified" means specified in an order made by the Treasury'. Under this definition, specified investments are Regulated Activities by Way of Business in the UK. The Financial Services and Markets Act 2000 c. 8. s. 22.

goods and services in the UK;[244] Section 419 gives the regulatory flexibility to identify carrying on regulated activities by way of business.[245]

In addition, Schedule 2 of The FSMA 2000 sets forth the provision supplementing as 'Dealing, Managing Arranging deals in investments, Investment advice, Deposit taking, Safekeeping and administration of assets, Establishing collective investment schemes and Using computer-based systems for giving investment instructions'.[246] This pinpoints that the regulatory objectives of crypto assets are for business or business-like activities operating in the UK no matter where the business venues are registered. Thus, these businesses can register in the UK or overseas and provide products and services for UK residents. It also includes firms registered in the UK providing products and services to overseas customers. However, individuals (excluding self-employed or freelancers) and non-profit institutions that conduct irregular commercial activities of crypto assets, such as investment advice, are not considered Carrying on Regulated Activities by Way of Business, therefore do not require authorisation.[247]

---

[244] '[F]or the purposes of this Act, to be regarded as carrying it on in the United Kingdom. (2) (a) his registered office (or if he does not have a registered office his head office) is in the United Kingdom; (b) he is entitled to exercise rights under a single market directive as a UK firm; and (c) he is carrying on in another EEA State a regulated activity to which that directive applies. (3) (a) his registered office (or if he does not have a registered office his head office) is in the United Kingdom; (b) he is the manager of a scheme which is entitled to enjoy the rights conferred by an instrument which is a relevant Community instrument for the purposes of section 264; and (c) persons in another EEA State are invited to become participants in the scheme. (4) (a) his registered office (or if he does not have a registered office his head office) is in the United Kingdom; (b) the day-to-day management of the carrying on of the regulated activity is the responsibility of—(i) his registered office (or head office); or (ii) another establishment maintained by him in the United Kingdom. (5) (a) his head office is not in the United Kingdom; but (b) the activity is carried on from an establishment maintained by him in the United Kingdom. (6) For the purposes of subsections (2) to (5) it is irrelevant where the person with whom the activity is carried on is situated'. ibid. s. 418.

[245] '(1) The Treasury may by order make provision—(a) as to the circumstances in which a person who would otherwise not be regarded as carrying on a regulated activity by way of business is to be regarded as doing so; (b) as to the circumstances in which a person who would otherwise be regarded as carrying on a regulated activity by way of business is to be regarded as not doing so. (2) An order under subsection (1) may be made so as to apply—(a) generally in relation to all regulated activities; (b) in relation to a specified category of regulated activity; or(c) in relation to a particular regulated activity. (3) An order under subsection (1) may be made so as to apply—(a) for the purposes of all provisions; (b) for a specified group of provisions; or (c) for a specified provision'. ibid. s. 419.

[246] ibid. sch 2.

[247] FCA, 'The Perimeter Guidance Manual' (n 42). section. 2.3.

The second step requests firms to identify if their crypto assets can be treated as specified investments under Part 3 of the RAO SI 2001/544. Part 3 of the RAO 2001 gives detailed definitions and interpretations about specified investments in the UK.[248] Other than the specified investments, some financial instruments defined under the MiFID 2 are recognised as certain types of investments and mapped to the RAO 2001.[249]

If crypto assets products fall outside the categories of specified investments under the RAO SI 2001/544, firms come into the final step to identify whether their crypto assets products fall within the definition of e-money under the EMR 2011[250] (see detailed discussion in the next subsections). If crypto assets products fall outside both the definitions of specified investments and e-money, they will be categorised as unregulated tokens. Although unregulated tokens do not require authorisation at the present, they shall still comply with the Company Act and other provisions of the PERG 2019 and FSMA 2000, accordingly.

Moreover, the FCA guidance paper defines the territoriality of the crypto asset activities under the PERG 2.4, "Link between activities and the United Kingdom". The PERG 2.4 sets out that the regulated activities in the UK shall refer to both the location of business registration and the commercial activities are taking place. For instance, a firm that is registered and established a business venue in the UK shall comply with the Carrying on Regulated Activities by Way of Business regardless of the locations of its clients. The same rule applies to overseas businesses that carry out regulated activities of by way of business in the UK, although this requires further clarifications.[251] For example, the PERG 2.4.6 gives instructions on overseas business operating in the UK through the internet, which is the main channel that crypto asset businesses rely on.

> 'A person based outside the United Kingdom may also be carrying on activities in the United Kingdom even if he does not have a place of business maintained by him in the United Kingdom (for example, by means of the internet or other telecommunications system or by occasional visits). In that case, it will be relevant to consider whether what

[248] The Financial Services and Markets Act 2000 (Regulated Activities) Order 2001, SI 2001/544. pt. 3.

[249] FCA, 'Guidance on Cryptoassets Feedback and Final Guidance to CP 19/3' (n 35). Appendix 1, para. 2. at p. 29.

[250] ibid. at. p. 30.

[251] FCA, 'The Perimeter Guidance Manual' (n 42). at section 2.4 – Link between activities and the United Kingdom.

he is doing satisfies the business test as it applies in relation to the activities in question. In addition, he may be able to rely on the exclusions from certain regulated activities that apply in relation to overseas persons'.

Moreover, Section 2.9.15G of the PERG provides further clarification of 'overseas persons'. It includes 'agreeing to carry on the regulated activities of managing investments, arranging (bringing about) deals in investments, making arrangements with a view to transactions in investments, assisting in the performance and administration of a contract of insurance, safeguarding and administering investments or sending dematerialised instructions'. This definition seems exhaustive, however, e-commerce (except insurance businesses) from the EEA member states is exceptional to this requirement in accordance with the single market system under 2.9.18G of the PERG.[252]

It is also said that persons that carry on regulated activities shall require relevant permission from authorities under Section 19 "The general prohibition", and Section 23 "Offences" of the FSMA 2000. In the meantime, legal or natural persons shall comply with the regulations on financial promotion under Section 21 of the FSMA 2000.[253] Similarly, it may also inquire further clarity that how to deal with persons who carry on unregulated activities of crypto assets in the UK, which do not require authorisation at the present. This situation is likely to happen

[252] '(1) In accordance with article 3(2) of the E-Commerce Directive, all requirements on persons providing electronic commerce activities into the United Kingdom from the EEA are **lifted,** where these fall within the co-ordinated field and would restrict the freedom of such a firm to provide services. The coordinated field includes any requirement of a general or specific nature concerning the taking up or pursuit of electronic commerce activities. Authorisation requirements fall within the coordinated field. The services affected are generally those provided electronically, for example through the Internet or solicited e-mail. (2) The Regulated Activities Order was amended by the Financial Services and Markets Act 2000 (Regulated Activities) (Amendment) (Electronic Commerce Directive) Order 2002 (SI 2002/2157). This Order creates a **general exclusion** from regulated activities (except for the regulated activities of effecting or carrying out contracts of insurance). Where activities consist of **electronic commerce activities, an incoming ECA provider will not require authorisation for such activities in the United Kingdom.** This does not extend to the regulated activity of effecting or carrying out contracts of insurance falling under the Solvency II Directive. However, services provided off-line in the United Kingdom (that is, other than as an electronic commerce activity) by such a firm which amount to regulated activities still require authorisation'. ibid. sections. 2.9.15G, 2.9.18G (1) and 2.9.18G (2).

[253] FCA, 'Guidance on Cryptoassets Feedback and Final Guidance to CP 19/3' (n 35). Appendix 1, paras. (26), (27) and (32).

given the fact of diverse regulatory requirements among the EU member states and the one passporting system (more discussions see the thesis Chapter 6, Regulation in the EU).

The FCA's guidance paper shows that the UK authorities haven't yet found a plausible solution to deal with the anonymity of crypto assets and to regulate those businesses that provide crypto assets products and services. The thesis has discovered several inconsistencies in existing regulatory schemes, whilst the complicated regulatory schemes somewhat weight down the efficiency and effectiveness of the existing regulations. First, the current regulatory perimeters manifest a narrow scope applying to only the minority of crypto asset products. Second, the complicated classification of crypto assets products and services indirectly raise the administrative cost of firms and the chances of misidentifying and miscategorising crypto assets by firms themselves are high. Third, the absence of regulatory schemes of exchange tokens and utility tokens leads to the majority of crypto asset products and service providers unregulated. Fourth, the loose regulations on firms that registered in the EEA member states may expose domestic consumers to risks. Finally, the referencing Acts are somehow inconsistent in terms of identifying types of crypto tokens. For instance, security tokens under Regulation. 76 of the RAO SI 2001/544 – "specified investment".

According to the FCA's finalised guidance paper, the classification of crypto asset regulation is likely based on contractual rights and ownership rights, such as investment contracts and shareholding. Crypto tokens that show clear ownership rights or contractual rights are regulated in the UK. The ownership rights can be possessed through firm ICOs and or transferred on capital markets, similar to traditional capital investment. The contractual rights clarify the agreed business investment agenda and holding rights of investors other than ownerships. Under contractual rights, crypto asset owners may receive commissions, dividends or share profits on a periodic basis whereas without voting rights. In addition, crypto tokens that possess the similar property of e-money may be categorised as e-money tokens under the EMRs SI 2011/99. However, the FCA will have to identify the e-money tokens on a case by case basis since the criteria of e-money tokens are not clear. Thus, only those investment-like tokens and e-money-like tokens are falling within the FCA's regulatory perimeters and request authorisation, outside the regulatory perimeters otherwise.[254]

As stated in the Final Guidance, 'the location of the regulatory perimeter is a matter for legislation and the courts, and we can only provide guidance on how we believe the current

[254] ibid. at pp. 14 and 34 - 39.

perimeter applies to crypto assets'. the FCA has established the guideline of crypto assets business and consumer protection based on its best understanding about the new technology and it is to the legislation system and the courts to make final decisions on whether crypto asset activities are lawful. The FCA will keep improving the regulatory regime while the markets are maturing.[255] Thus, the property rights seem to become the key element to identify the legal identity of crypto assets at the time of writing, especially those unregulated tokens. In the following chapter, I will critically analyse the current regulations of crypto tokens that lie within the FCA's regulatory perimeters and assess other laws and acts that are relevant to unregulated tokens.

The FCA initially categorises crypto assets into four types of tokens: 'exchange tokens', 'utility tokens', 'security tokens' and 'e-money tokens' following the EU regulatory recommendation, whilst the 'exchange tokens' and 'utility tokens' are grouped in the category of unregulated tokens in the final guidance paper. Generally, the exchange tokens refer to crypto assets used as a means of remittances, including purchasing and selling goods and services, which are not included in the regulatory perimeters; the utility tokens are crypto assets that allow holders to have access to current or prospective product or services with agreed conditions, which are not included in the current regulatory perimeters; the security tokens refer to crypto assets presenting similar characteristics as traditional shares or debentures, which fall within the regulatory perimeters; the e-money tokens are the crypto assets that fall into the definition of e-money and this type of token is regulated under E-Money Regulations (EMRs).[256]

## 5.2 Regulated Crypto Tokens

There are two types of crypto-tokens falling within the FCA regulatory perimeters, security tokens and e-money tokens. Crypto assets token holders may participate in multiple crypto assets businesses, only tokens fall within the definition of security tokens and e-money tokens are regulated and the token holders shall provide full information of their identities under a contractual agreement.[257]

[255] ibid. at pp. 16 and 23.

[256] ibid. Appendix 2, para. 7. at p. 30.

[257] ibid. at pp. 40 - 48.

### 5.2.1 Security Tokens

The regulation of security tokens follows the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (RAO). The FCA guidance paper defines security tokens as:

> 'Security tokens are those tokens that provide rights and obligations akin to specified investments as set out in the RAO excluding e-money. These tokens may also be financial instruments under MiFID II. For example, these tokens have characteristics which mean they are the same as or akin to traditional instruments like shares, debentures or units in a collective investment scheme'.[258]

The definition focuses on the legal titles of crypto assets investments and whether the legal titles are negotiable and transferable on the capital markets. The term of transferable in this definition does not refer to money transactions and remittance among individuals, which separates the security tokens from e-money tokens and exchange tokens. Specified investments of the kind include shares, debentures, warrants and units in collective investment schemes.

#### *5.2.1.1 Shares*

The FCA identifies whether crypto assets are shares of specified investments under Regulation 76 of the RAO SI 2001/544.[259] This means the crypto asset shareholders of an entity shall be conferred the same rights as normal shareholders. Therefore, these crypto assets are registered under the names of a natural person/persons or legal person/persons, which provide clear identity information of the ownership of the shares. The entity can be any person in the UK or overseas constituted under the law of the country. However, Regulation 76 (3) of the RAO SI 2001/544 excludes open-end investment companies, a building society, industrial and provident societies and credit unions in the UK or the EEA member states from the definition.[260]

There is an inconsistency in Regulation 76 of the RAO SI 2001/544. The Regulation 76 (2) (b) of the RAO states that UK and EEA firms relating to industrial and provident societies or credit unions are included in art s 76 (1), "shares or stock in the share capital of". However, Regulation 76 (3) (c) and (d) of the RAO excludes those UK and EEA firms from Regulation 76 (1) of the RAO. Thus, identical types of firms are included and excluded in Regulation 76 (1) at the same time. Such inconsistency may cause confusion to firms at all stages of their

[258] ibid. Appendix 2, para 64. at p. 40.

[259] The Financial Services and Markets Act 2000 (Regulated Activities) Order 2001, SI 2001/544. reg. 76.

[260] ibid. reg. 76.

crypto asset businesses. It affects the stage of ICOs as crypto asset issuers and investors are unable to identify if the issued tokens can be treated as share capital; it affects the business operating stage because of the compliance of such tokens are ambiguous; it affects the stage of business shutdown since the legal rights of the tokens are yet clearly identified in the issuing stage. It may also leave token investors at a vulnerable circumstance if tokens being identified as regulated token shares under Regulation 76 (2) (b) of the RAO by an issuer at an ICO stage, whilst treated as unregulated share tokens under Regulation 76 (3) (c) (d) of the RAO by the regulator after the ICO.

'76.— (1) Shares or stock in the share capital of—

(a) any body corporate (wherever incorporated), and

(b) any unincorporated body constituted under the law of a country or territory outside the United Kingdom.

(2) Paragraph (1) includes—

(b) any transferable shares in a body incorporated under the law of, or any part of, the United Kingdom relating to industrial and provident societies or credit unions, or in a body constituted under the law of another EEA State for purposes equivalent to those of such a body.

(3) But subject to paragraph (2) there are excluded from paragraph (1) shares or stock in the share capital of—

(c) a body incorporated under the law of, or any part of, the United Kingdom relating to industrial and provident societies or credit unions;

(d) any body constituted under the law of an EEA State for purposes equivalent to those of a body falling within sub-paragraph (b) or (c)'.

Additionally, the FCA emphasises that shareholders of crypto assets must hold some rights of control. Having a right of voting does not confer a right of control.[261] This means that crypto assets of non-controlling interest shareholders may not fall within the regulatory perimeters, means that minority crypto assets shares with only voting rights are unregulated, for instance,

[261] FCA, 'Guidance on Cryptoassets Feedback and Final Guidance to CP 19/3' (n 35). at p. 41.

a company may issue crypto assets share as one share per person, each person holds one voting right whereas does not have the rights of controlling the company.

Some situations have not yet been taken into consideration in the regulatory perimeters of the FCA. For instance, crypto asset shares that are negotiable and transferable on the capital markets may fall within the definitions of both specified investments and financial instruments under MiFID II, such as transferable securities. Thus, these types of crypto assets require further clarification of whether they fall within the regulatory perimeters of investments or financial instruments. However, the opposite situation may not be applicable. Crypto assets that identified as transferable securities are not necessarily falling within the regulatory perimeters of specified investments since many transferable securities are not shares of capital that have clear entitlements. Besides, the investment activities shall also comply with company laws regardless of how the shares of capital are collected and processed.

#### *5.2.1.2 Indebtedness*

The debentures represented by crypto assets shall comply with Regulation 77 of the RAO SI 2001/544 for 'instruments creating or acknowledging indebtedness'. Indebtedness refers to debentures, debenture stock, loan stock, bonds, certificates of deposit and any other instrument creating or acknowledging indebtedness. This does not include borrowed money for defraying or paying goods or services and heritable security which might be payable using crypto assets,[262] and it does not include government and public securities.[263] The certificates of deposit are unlikely to be recognised as crypto assets are not yet treated as deposits.

Similarly, crypto assets referring to negotiable and transferable indebtedness on capital markets can be treated as security tokens under MiFID2. Again, the negotiability and transferability of crypto assets do not necessarily confirm that they are security tokens unless the legal titles of token holders are clear or identifiable and have the rights to trade on capital markets.[264]

#### *5.2.1.3 Warrants*

Crypto assets acting as warrants follow the definition "Warrants" under Regulation 79 of the RAO SI 2001/544, 'investments giving entitlements to investments'.[265] Warrants give the rights to crypto assets holders to access specified investments, including token-like shares and

[262] The Financial Services and Markets Act 2000 (Regulated Activities) Order 2001, SI 2001/544. reg. 77.

[263] ibid. reg. 78.

[264] FCA, 'Guidance on Cryptoassets Feedback and Final Guidance to CP 19/3' (n 35). at pp. 42 - 43.

[265] The Financial Services and Markets Act 2000 (Regulated Activities) Order 2001, SI 2001/544. reg. 79.

debentures under Regulation 76 and Regulation 77 of the RAO SI 2001/544. Warrants refer to the rights that the token issuer grants token holders to participate in new specified investments directly. Existing specified investments do not fit into this definition under reg. 76 and 77 of the RAO SI 2001/544.

#### *5.2.1.4 Units in Collective Investment Schemes*

This type of tokens refers to pooled investments including internet-based crowdfunds. Units in collective investment schemes give definitions to Investors that gain benefit from the rising income/profit of specified investment based on the proportions of their token shares under Regulation 80 and Regulation 81 of the RAO SI 2001/544. The pooled investments mean only one specified investment at a time, investing in multiple specified investments shall be treated as acting in each specified investment separately, even the investments are operated by the same issuer.[266] The legal titles of the tokens shall be clearly identified and are transferable from one person to another.

However, whether the agreements or prospectus of collective token investment falling within the regulatory perimeters of the FCA depends on the contents written in the agreements or prospectus. For example, open-end token investments are excluded from the category of collective token investment.[267] Meanwhile, collective investments involve exchange tokens or utility tokens are also excluded since the two types of tokens fall outside the regulatory perimeters of the FCA. Therefore, this type of specified investments will be likely assessed on a case by case basis.

### 5.2.2 Analysis of the Effectiveness of the Security Token Regulation

The FCA is aware of the importance of a harmonised framework for crypto assets regulation. In the meantime, the FCA has acknowledged that an unharmonised framework would possibly incur risks of speculative firms gaming with the regulatory system and cause inconvenience for firms establishing business networks across different jurisdictions. However, the FCA seemly has not had solutions to structure a harmonised legal/regulatory framework for crypto assets regulation as there are some "inherent structural differences" amongst securities markets. The FCA did not clarify which securities markets they referring to but mentioned several regulatory agencies to work together on this regard both bilaterally and multilaterally. These regulatory agencies include the Global Financial Innovation Network (GFIN), the International

[266] ibid. regs. 80 and 81.

[267] FCA, 'Guidance on Cryptoassets Feedback and Final Guidance to CP 19/3' (n 35). at p. 44.

Organization of Securities Commissions (IOSCO), the European Commission (EC) and the European Supervisory Authorities (ESA).

The FCA inquired in January 2019 whether their classification of specified investment or financial instrument in the category of security tokens is feasible.[268] The summarised feedback in July 2019[269] shows that the definition of security tokens was agreed by most of the respondents in terms of the holding rights of crypto assets. The finalised regulatory framework ensures the ownership of crypto assets and correct permissions under relevant rules and requirements akin to specified investments. However, some respondents requested further clarification on the issues of a harmonised framework across jurisdictions, a clearer boundary between security tokens and utility tokens and further guidance on custody wallets of crypto assets, respectively.

The FCA acknowledged that the services of crypto assets custody wallets are different from traditional securities and delineated this situation falling outside the scope of the regulatory perimeters. It says that the diagnosed issues are caused by technology applications rather than perimeter issues, as relevant activities are affected by the use of DLT systems, not the products. The FCA 'believes' the final guidance for security tokens is sufficient to market participants in terms of clarity especially regulated activities of security tokens and will continuously monitor the developments in the unclarified areas while the market is maturing.[270] However, firms need to identify and ensure appropriate permissions about both the clarified and unclarified issues of their token businesses. It is understandable that the FCA intends to observe the nascent market and design appropriate regulatory policies accordingly. I assume that the FCA believes the unclarified issues will not cause significant impacts to market participants in practice as well as consumers.

Other than those unclarified areas pointed out by the respondents, there are more unclarified issues in the regulation of security tokens. The first unclarified issue is how to differentiate specified investments and financial instruments within the category of security tokens. The FCA classifies security tokens following the RAO SI 2001/544, the PERG 2019[271] and the

[268] FCA, 'CP19/3: Guidance on Cryptoassets UK' (n 83).

[269] FCA, 'Guidance on Cryptoassets Feedback and Final Guidance to CP 19/3' (n 35).

[270] ibid. p. 23.

[271] FCA, 'The Perimeter Guidance Manual' (n 42).

MiFID II.[272] Unlike traditional specified investment or financial instruments, crypto assets can be used as both the methods of issuing the shares of specified investments and the objects of the specified investments. Thus, the holding rights of token owners may vary along with different investment structures and agreements. In this situation, an investor can be a shareholder of crypto assets and allow to trade them as financial instruments on capital markets. Since the two types of investments (equity and financial instruments) are regulated under different Laws, a clearer definition will assist firms to clarify their prospectuses for ICOs and specify rights and responsibilities.

Another issue that requires further clarification is how to distinguish financial instrument tokens (in the group of security tokens) and exchange tokens. Crypto assets that present characteristics of financial instruments may fall within the definitions of both security tokens under MiFID II and exchange tokens. Financial instruments that have clear and identifiable ownership are categorised in security tokens. This includes tokens that represent derivatives, options and futures. Alternatively, tradable and transferable tokens on the financial markets without clear ownership rights or identifiable holding rights fall within the definition of financial instruments are grouped in exchange tokens. This includes Bitcoins. Identifying the token types of financial instruments seemly depends on if the tokens are the references to the financial instruments or the trading objects on the financial markets. The former is regulated tokens whereas the latter is not. The FCA recognises this ambiguity in the token classification and suggests firms to require consultancy on a case by case basis.[273]

The third issue is how to comprehend the situation of using unregulated tokens to invest authorised ICOs. According to the units in collective investment schemes, tokens issuers presumably can accept all payments as long as their value transactions are valid. Thus, investors can purchase shares and claim equities with cash or crypto assets may or may not disclose their legal identities. This kind of specified investment is partially falling within the regulatory perimeters of the FCA, subject to the investment structures and agreements of an authorised ICO. However, the crypto assets used to purchase the shares are not necessarily regulated tokens. The FCA needs to clarify if unregulated tokens can be used to purchase regulated tokens and if the regulatory status transfers while the holding rights are transferred.

[272] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU [2014] OJ L173/349.

[273] FCA, 'Guidance on Cryptoassets Feedback and Final Guidance to CP 19/3' (n 35). at pp. 40 and 45.

In addition, crypto asset shares/debentures can be treated as security tokens only if the investment structure falls within the definitions of specified investments under Part 3 of the RAO SI 2001/544 and the regulatory perimeters of the FCA. This means investments outside the definition will request no authorisation. Under this situation, investors and consumers need to be given sufficient information to understand the impacts of authorised and unauthorised tokens, respectively, on their token investments, such as ICOs or holding rights transfer. Insufficient information on unregulated tokens certainly will have a negative effect on market integrity and consumer protections.

Besides, although holding shares and indebtedness could confirm the legal rights of the token holders, the current definition does not consider the value volatility of crypto assets. The value of shares made through crypto assets may vary if these tokens are not value stabilised against fiat currencies. Therefore, the total amounts of an investment may or may not meet the requirement of investment capital, subject to the value variation of the tokens. Besides, the regulated security tokens focus on shares and debentures of entities under the By Way of Business and financial instruments under the MiFID II. This excludes crypto assets exchange platforms that do not hold crypto shares of entities, however, possibly have a strong impact on the price volatility of security tokens trade on the capital markets.

Moreover, the channels that carry out the value transactions from investors to token issuers could be crypto asset exchanges, which fall outside the regulatory perimeters of the FCA regulatory perimeters. This means the specified investment is regulated whereas the conduits of realising shareholding are not.

Consequently, the current regulation on security tokens is insufficient with clarity, comprehensibility and thoroughness. There is large room for improvements. Authorities need to carefully examine the dynamic connections between the products and the financial markets and make the definition and regulatory scope more practical and easier to understand to market participants.

### 5.2.3 E-money Tokens

The FCA classifies certain types of crypto assets as e-money tokens under the consultation feedback received in July 2019. The e-money tokens are a special category that is different from the classification of the EU and other EU countries regarding crypto assets. The UK is the only nation that defines e-money tokens at the time of writing. The FCA defines e-money

tokens under the Electronic Money Regulations (EMRs) and Regulation 9b of the RAO SI 2001/544.[274] E-money token shall present:

> '1) Issued on receipt of funds for the purpose of making payment transactions
>
> 2) Accepted by a person other than the electronic money issuer
>
> 3) Not excluded by regulation 3 of the EMRs'[275]

The EMRs SI 2011/99 interpret the characteristics that permitted e-money should have. E-money is issued against users' funds for making payments and should be accepted among users except for functions of e-money included in Regulation 3 of the EMRs SI 2011/99. The Regulation excludes possible applications that narrow the use of e-money. For example, electronic money can only be used in or on issuer's premises, or only accepted within a limited network or limited range of service providers, or the issuers providing services more than just a transaction intermediator.[276] Meanwhile, Regulation 2 and Regulation 3 of the EMRs SI 2011/99 ensure authorised e-money to be a representative equivalent to the value of users' funds and to be widely accepted in society.

In addition, Regulation 9b of the RAO SI 2001/544 is considered by the FCA in defining crypto e-money tokens, which is under Chapter 2 of the RAO 2001 – 'Accepting Deposits'.[277] Chapter 2 of the RAO 2001 firstly defines the activities of accepting deposits under Regulation 5, then specifies exclusions in Regulation 6 to Regulation 9.

The definition of 'accepting deposits' under Regulation 5 of the RAO SI 2001/544 clarifies the scope of e-money tokens. The purposes of taking deposits are lending to others, and any other activities of the person who is accepting deposits shall be financed out of the capital or interest on money received by way of deposit. Also, deposits shall be repaid with or without interest or premium by the person who is accepting deposits under contracts or agreements of the sum of deposited amounts. The deposits shall not be referred to the provision of property, services or the giving of securities.[278]

---

[274] ibid. at p. 40.

[275] Electronic Money Regulations 2011, SI 2011/99. reg. 2.

[276] ibid. reg. 3.

[277] FCA, 'Guidance on Cryptoassets Feedback and Final Guidance to CP 19/3' (n 35). para. 70, at p. 45.

[278] The Financial Services and Markets Act 2000 (Regulated Activities) Order 2001, SI 2001/544. reg. 5.

Regulation 9b of the RAO SI 2001/544 refers to one of the exclusions of the activities of accepting deposits, 'Sums received in consideration for the issue of debt securities'. The Regulation 9b excludes the following activities from the category of accepting deposits: a) activities of specified investments under Regulation 77 or Regulation 78 of the RAO 2001; b) or commercial paper issued to persons whose ordinary activities involve specified investments under Regulation 77 or Regulation 78 of the RAO 2001; c) and the redemption value of the commercial paper is greater than £100,000 or an equivalent amount of other currencies.[279]

Furthermore, following the definition in the EMRs SI 2011/99, the identification criteria of e-money tokens focus on the purposes and structures of token issuance and token applications. The criteria accept crypto assets issued on receipt of funds, transferable among individuals. E-money token issuers shall comply with the EMRs 2011requirements, like capital requirement, recordkeeping and money laundering monitoring. It requires e-money issuers to be and only to be third parties in providing transaction services with stabilised rates against fiat money.

Additionally, e-money token issued by credit institutions, credit unions and municipal banks for the purpose of debt securities, shall meet a minimal value of redemption is £100,000 or equivalent value of other currency[280] and shall have an office situated in the UK.[281]

The criteria of e-money tokens may assist crypto asset issuers to structure the ICO processes in order to operate regulated crypto asset businesses in the future. However, consumers may not easily understand the differences between e-money tokens and well-structured unregulated crypto assets.

The FCA will identify whether crypto assets can be accepted as e-money tokens on a case by case basis. There are possibilities of not being recognised as e-money tokens even crypto assets may present characteristics that fall within the definition of e-money under the EMRs and meet abovementioned criteria.[282]

### 5.2.4 Analysis of the Effectiveness of the E-Money Token Regulation

The FCA has established a category of e-money tokens in the UK based on feedback received from the majority of respondents in response to a question about certain types of crypto assets

[279] ibid. reg. 9.

[280] ibid. reg. 9 (b).

[281] Electronic Money Regulations 2011, SI 2011/99. reg. 6.

[282] FCA, 'Guidance on Cryptoassets Feedback and Final Guidance to CP 19/3' (n 35). para.72. at p. 45.

that used as e-money or financial instruments. These types of tokens are previously categorised in utility tokens under the EMRs or security tokens under the MiFID II following EU classifications. The previous classification was seen misleading and led to confusion about complying with appropriate rules and correct permissions regarding certain types of crypto assets that fall within the definition of both categories of regulated and unregulated tokens. Further clarification was required for the classification of stabilised tokens that present e-money-like properties whereas falling within the category of unregulated utility tokens or regulated security tokens.

The FCA is aware of that the value stabilisation of crypto assets can be achieved via various ways, such as backing with fiat funds and a basket of crypto assets and/or other types of assets, as well as through algorithms. However, the FCA deems that the attempted value stabilisation does not change the purpose and the varying structure and arrangement of crypto assets, which can fall under the definition of either of e-money or security tokens. Therefore, the classification of 'stabilised tokens' needs to be considered on a case by case basis.

Therefore, the FCA defines e-money tokens under the EMRs SI 2011/99 and interprets the definition in the FCA guidance paper.[283] Under the definition, only tokens that possess characteristics identical to traditional electronic money except the technology used (DLT). E-money token issuers shall issue and operate token businesses under the EMRs 2011 and the RAO SI 2001/544. It seems the main difference between e-money and e-money tokens is the technology that creates it as long as e-money token issuers carry out businesses under the regulatory requirements, such as verifying user identity and recordkeeping.

However, there are ambiguities in the e-money token definition. These ambiguities may cause difficulties to firms and consumers to identify the regulatory positions of crypto-tokens or crypto-token businesses, therefore, require further clarification. The exclusion in Regulation 3 of the EMRs SI 2011/99 is insufficient to determine the regulatory position of some crypto assets that present similar characteristics to e-money. For instance, some crypto assets that can be purchased against fiat money and used for making payments or purchasing goods and services are accepted by many individuals and businesses whereas excluded in the regulatory perimeters of the FCA, such as Bitcoins. Consumers and firms need to consult additional

[283] ibid. at pp. 45 - 46.

information to identify the regulatory status of these types of crypto assets, such as the Company Act.

In addition, although the FCA requests firms that engage in Regulated Activities by Way of Business to require authorisations or registrations, such as crypto assets trading and exchange platforms, payment providers, custody wallet providers and other intermediation, it leaves room for firms gaming with the regulatory system. For instance, firms may comply with the requirements of authorisations and registrations whereas operate both regulated and unregulated crypto assets at the same time. Moreover, less clarification on e-money tokens and utility tokens may also cause firms to operate both regulated and unregulated tokens unintentionally. It is also unclear how to regulate firms that registered e-money token business in the UK whereas operating in other EU countries where do not permit e-money tokens since these firms can provide products and services overseas under the one passporting system and through the internet.

## 5.3 Unregulated Crypto Tokens

The FCA previously classified certain types of crypto assets into exchange tokens and utility tokens in accordance with the EU regulation.[284] The two groups of tokens fall outside the regulatory perimeters of the FCA and are unregulated tokens. The current regulation classifies crypto assets that present unclear ownership rights and trade on anonymous networks as unregulated tokens and differentiates these crypto assets from identifiable e-money tokens under the EMRs SI 2011/99 and security tokens under the RAO SI 2001/544 – 'specified investments'. Unregulated tokens contain the most popular crypto assets and token services that manifest characteristics of decentralisation and anonymity and conduct direct transactions among token users.

### 5.3.1 Exchange Tokens and Relevant Regulations

Exchange tokens refer to crypto assets used for payment transactions or trading on crypto asset exchanges or stored on custody wallets. The owners of this type of crypto assets are normally anonymous, while exchange tokens are the most popular crypto assets on the markets.

The feedback the FCA received on exchange tokens agreed that exchange tokens would not need existing regulatory permissions while other rules in the financial sector that may apply to authorised financial firms operating or using unregulated crypto assets. These rules include the

[284] FCA, 'CP19/3: Guidance on Cryptoassets UK' (n 83). paras. 2.5, 2.6, 2.36 and 3.2. at pp. 8 - 9 and 14 - 16.

Principles for Business (PRIN)[285] for commercial conduct and the Senior Managers and Certification Regime (SMCR)[286] for individual conduct, as well as the Banking: Conduct of Business sourcebook (BCOBS)[287] for banks financial firms. These rules are applicable to insurers and other FCA regulated firms with activities under the definition of 'SMCR financial activities' including regulated activities and activities in connection with a regulated activity no matter when the connection takes place.

The FCA has recognised that exchange tokens are the major growing area for crypto assets and DLT technology, however, the volatility and anonymity of crypto assets, as well as other potential issues made these tokens falling outside the existing regulatory perimeters of the FCA. The FCA requests that firms using crypto assets to facilitate regulated payments must have the correct permissions and follow the relevant rules and regulations. This includes, but is not limited to, the PSRs, and from 1 August 2019, PRIN and BCOBS. Moreover, certain activities of exchange tokens are regulated under the EU Fifth Anti-Money Laundering Directive.

### 5.3.2 Utility Tokens and Relevant Regulation

Utility tokens refer to crypto assets that used like 'a current or prospective product or service and often grant rights similar to pre-payment vouchers'.[288] This type of token carries values in accordance with pre-agreed rights on products or services. Utility token owners can be anonymous and trade or exchange their tokens on the secondary markets and use their tokens for speculative investment purposes. Utility tokens have wider range characteristics that cover crypto assets similar to e-money tokens and security tokens, as well as exchange tokens. Therefore, further clarification of utility tokens is needed, including identifying utility tokens that meet the definition of e-money and distinction between utility tokens and exchange tokens. There are also call for utility token regulation.

### 5.3.3 Analysis of Unregulated Tokens and Potential Issues

The unregulated tokens possess similar characteristics to regulated tokens and have possibilities falling within the regulatory perimeters of the FCA subject to the situation of individual cases. For instance, the FCA set a regulatory sandbox that has been used to observe

[285] FCA, 'Principles for Businesses' (2020).

[286] FCA, 'The Senior Managers and Certification Regime: Guide for FCA Solo-Regulated Firms' (2019).

[287] FCA, 'Banking: Conduct of Business Sourcebook' (2020).

[288] FCA, 'CP19/3: Guidance on Cryptoassets UK' (n 83). para 48. at p. 36.

how unregulated crypto assets could facilitate international money remittance, one of the regulated payments services. The FCA elaborates that unregulated crypto assets may not fall within the scope of regulated payments services under Schedule 1, Paragraph 1 and 2 of the PSR if unregulated crypto assets are irrelevant to cash deposits and withdrawals, card issuing, merchant acquiring and money remittance. However, a payment service using crypto assets that relate to funds will be in the scope.[289] The regulated payments services refer to payments services to clients, such as individuals, and exclude payments transactions between payments providers, such as inter-bank settlement, central counterparties and clearinghouses.[290] Therefore, token issuers or token service providers shall consult the FCA if unsure about the regulatory positions of their businesses.

This situation may cause uncertainty in the regulatory framework. For example, token issuing may fall within the regulatory perimeters whereas the token transaction channels may not. Besides, firms may be overconfident in their judgements whereas accidentally operating unregulated token businesses under regulatory licence obtained by their regulated token businesses. This wrongdoing can be intentionally or unintentionally.

Moreover, falling outside the regulatory perimeters of the FCA does not suggest that those token issuers and service providers are allowed to operate businesses without consulting other Laws and Acts. Token services providers firstly shall follow the regulation of commercial activities by way of business as normal investment/financial firms.[291] Consumers must be cautious if businesses are relating to unregulated crypto tokens and these businesses may have the potential to be involved in unlawful activities. For instance, the user data may be under threat of financial criminals, such as online fraud and stealing. Given the fact that businesses usually prefer to cover as many product scopes as possible to enlarge profits,[292] the possibility of firms operating both unregulated and regulated tokens businesses is high when relevant regulation is absent no matter their intentions. If so, consumers will be exposed to risks.

[289] FCA, 'Guidance on Cryptoassets Feedback and Final Guidance to CP 19/3' (n 35). Appendix 1, paras 58 - 60. at p. 39.

[290] FCA, 'The Perimeter Guidance Manual' (n 42). section 15.5Q37.

[291] The Financial Services and Markets Act 2000 (Carrying on Regulated Activities by Way of Business) (Amendment) Order 2018, SI 2018/394.

[292] Smith (n 209). Book One, Chapter 9.

There has been an increasing number of crimes involving illicit activities of crypto assets since 2017. The current regulatory frameworks in the UK cover small strands of crypto asset activities and focus on commercial conduct of financial and technology firms. Unlawful activities of crypto asset users, issuers, service providers and maintainers will refer to other Laws and Acts in addition to the regulatory perimeters of the FCA. The illicit activities of crypto assets are usually the internet based with little geographical boundaries. Typical violations consist of online scam and fraud, cyber-attack and stealing, as well as money laundering that assists online and offline illicit earnings entering legal circulation.

## 5.4 Illicit Activities of Crypto Assets in the UK

This section discusses the Laws and Acts that apply to crypto asset violations. There are many ways for offenders to produce illicit earnings. Offenders may directly generate illicit earnings via selling prohibited goods, such as drugs and fake passports, on dark webs or indirectly obtain crypto assets through breaking into crypto assets wallet apps or exchange platforms, for instance, stealing crypto assets through cyber-attack. The former illicit activities are related to the Criminal Law Act 1977[293] and the Serious Crime Act 2007,[294] and the latter may require the Laws in relation to information and technology, as well as computer misuse. Whatever what kind of unlawful activities that offenders carry out to breach the law, the final step that offenders have to deal with is to recognise illicit earnings to be legal tender through money laundering.[295]

An arrest taking place early this year can be a good example to see how these Acts and Regulations apply to crypto assets related crimes. In January 2019, the UK's South East Regional Organised Crime Unit (SEROCU) arrested an individual in Oxford on suspicion of crypto assets fraud, theft and money laundering. This arrest was in cooperation with the Hessen State Police (Germany), the UK's National Crime Agency (NCA) and Europol. The offender illegally accessed the digital keys (81 keys stored in the background of the server) of crypto asset holders to visit their crypto asset wallets without authorisation on IOTA,[296] a DLT firm that provides crypto asset related services registered in Berlin, Germany. The offender stole the value of €10 million Euros from over 85 victims worldwide and then laundered the illicit

[293] Criminal Law Act 1977 c. 45.

[294] Serious Crime Act 2007 c. 27.

[295] Alhosani (n 182). at p. 12.

[296] <https://www.iota.org/> accessed 11 November 2019.

earnings into financial channels between January 2018 and January 2019.[297] There have no formal decisions been made public, thus it is yet to know of the offender were prosecuted in the UK under the UK Laws or in Germany under the EU laws. If the prosecution is taking place in the UK, the offender may be charged on suspicion of fraud, online stealing and money laundering under the Theft Act 1968/1978 for stealing digital properties, Computer Misuse Act 1990 for accessing unauthorised computers, and Proceeds of Crime Act 2002 for money laundering.[298] While the IOTA may have to face charges on suspicion of breach the Data Protection Act 2018[299] and the Privacy and Electronic Communications (EC Directive) Regulations 2003[300] by allowing access to personal data, such as the user account info and transaction keys.

Digital crimes involve less in-person contact and the internet has become an ideal shelter to allow criminals hiding behind screens. The largely unregulated crypto asset businesses (exchange tokens and utility tokens) have become the most preferred transaction methods for illegal activities, for instance, Dark Webs. Nevertheless, no matter what channels and methods are applied, criminals have to realise illicit earnings and spend them in real life. Therefore, monitoring money laundering is essential to prevent unlawful activities and to protect uninformed consumers. The UK has not yet issued its crypto asset anti-money laundering schemes. Thus, it shall follow relevant requirements under the Sanctions and Anti-Money Laundering Act 2018 and the EU Fifth AML Directive. The FCA has implemented the EU Fifth AML Directive effective on 10th January 2020[301] and in force till the end of 2020 after the transition period of EU Withdrawal.[302]

The following subsections discuss the direct and indirect unlawful activities in relation to crypto assets and applicable Laws and Acts in the UK.

---

[297] 'Cryptocurrency IOTA: International Police Cooperation Arrests Suspect Behind10 Million EUR Theft | Europol'<https://www.europol.europa.eu/newsroom/news/cryptocurrency-iota-international-police-cooperation-arrests-suspect-behind-10-million-eur-theft> accessed 15 October 2019.

[298] The Crown Prosecution Service (n 33). (n/d).

[299] Data Protection Act 2018 c.12. s. 45.

[300] The Privacy and Electronic Communications (EC Directive) Regulations 2003, SI 2003/2426. reg. 6.

[301] The Money Laundering and Terrorist Financing (Amendment) Regulations 2019, SI 2019/1511.

[302] FCA, 'Guidance on Cryptoassets Feedback and Final Guidance to CP 19/3' (n 35). at p. 7.

### 5.4.1 Direct Unlawful Activities

The Crown Prosecution Service clarifies crypto asset related unlawful activities. Based on the guide on the webpage of Crown Prosecution Service, direct violations, such as selling controlled goods on online marketplaces, can be prosecuted under the Criminal Law Act 1977 c. 45 and the Serious Crime Act 2007 c. 27.[303]

The Criminal Law Act 1977[304] is used 'for restricting the use or threat of violence for securing entry into any premises and for penalising unauthorised entry or remaining on premises in certain circumstances'. The Act identifies that all parties involved in offences are guilty of conspiracy, including intentions of carrying out the agreement of offences.

> 'Subject to the following provisions of this Part of this Act, if a person agrees with any other person or persons that a course of conduct shall be pursued which will necessarily amount to or involve the commission of any offence or offences by one or more of the parties to the agreement if the agreement is carried out in accordance with their intentions, he is guilty of conspiracy to commit the offence or offences in question'. [305]

Under this definition, both buyers and sellers of prohibited goods are treated as guilty of conspiracy regardless of the original ownership rights of the prohibited goods and the delivery methods. Prohibited goods include but not limited to offensive weapons, explosive substances, illegal drugs and indecent and obscene materials.[306]

In addition, the Serious Crime Act 2007 defines activities that encourage and assist offences as serious violations and makes prevention orders. The assistance of unlawful activities also refers to information sharing and data matching for fraud or intentions relating to proceeding crimes. To decide the intention relating to proceeding serious offence, the court must ignore the reasons that offenders provide in the circumstances and offenders mental state. Individuals under 18 have an exemption from the Orders.[307]

[303] The Crown Prosecution Service (n 33). (n/d). No paragraph or sections numbers on this webpage.

[304] Criminal Law Act 1977 c. 45.

[305] ibid. s.1 (1).

[306] ibid. ss. 8, 16, 52 and 53.

[307] Serious Crime Act 2007 c. 27. ss. 4 (2), 6, and 44.

Therefore, either intentional or unintentional activities that aid and abet offences are treated as guilty of serious crime. Moreover, indirectly encouraging and assisting offences, such as approving or allowing unauthorised accessing is also a violation of the Law.[308]

Thus, direct unlawful activities may use crypto assets as a means of transactions and a tool for concealing the real identities of both parties. The main purposes and consequences of illicit actions are no different than offences that apply for other payment methods. Indeed, the absent responsibilities of recordkeeping and reporting and the anonymity of crypto asset businesses add difficulties to the investigations and identifications of crypto asset crime. However, the court will draft their judgements based on the actions and intentions, as well as expressions rather than transaction methods alone.

Other activities of crypto assets may also breach the Laws, such as infringements of copyrights of DLT coding and software/apps and the fraudulence of crypto assets ICOs and certificates, which would come within the general domain of the Information Technology Law and the Intellectual Property Law, as well as the Prevention of Fraud (Investments) Act 1958. Besides, manipulating crypto assets markets and connected primary and secondary markets using algorithms may have to be taken into consideration in the future.

### 5.4.2 Indirect Unlawful Activities

According to the Crown Prosecution Service, virtual properties are protected under the Theft Act 1968,[309] Theft Act 1978, Computer Misuse Act 1990, Forgery and Counterfeiting Act 1981 and Proceeds of Crime Act 2002.[310]

The Theft Act 1968 defines theft as a person ‘dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it”, regardless of the person’s intention.[311] Under the Act, property “includes money and all other property, real or personal, including things in action and other intangible property’.[312] This definition covers both tangible and intangible items belonging to a person or persons, which crypto assets can fit within the definition. The Theft Act 1968 also states that an offence is committed if a person agrees to be

[308] ibid. s. 66.

[309] Theft Act 1968 c. 60.

[310] The Crown Prosecution Service (n 33). (n/d).

[311] Theft Act 1968 c. 60. s. 1.

[312] ibid. s. 4 (1).

involved in online stealing, such as unreported suspicious activities or leaving out unauthorised access.

'Encouraging or assisting offences believing one or more will be committed'. [313]

The Computer Misuse Act 1990 identifies the unlawful activities of accessing unauthorised computers and data and with intent to commit or facilitate the commission of further offences.[314] Misusing computer may accompany the intention of stealing data or intangible properties stored on the computer or make changes of access permissions of the data, such as crypto asset custody wallets or exchange accounts. Unauthorised use of computers also includes a) authorised person/persons accessing unauthorised computers. For instance, a person from another department of an organisation; b) authorised person accessing authorised computers for unauthorised purposes of use of information. For example, a police officer accesses the police station database for personal use or for the purpose of leaking data. Accessing unauthorised computers with the aim of stealing or facilitating commissions of further accessing unauthorised data or information or intangible properties shall be considered under the Theft Act 1968.[315]

Similar activities that involve encouraging or cooperating with misuse of computers undertaking by a person or persons of authorised organisations are covered by the Police and Justice Act 2006.[316] This is important as authorities hold more sensitive information and officials can easily request to access relevant databases. Such convenience of accessing valuable information may motivate unlawful activities. Section 37 (4) of the Police and Justice Act 2006 identifies the leaking information (called "article" in the section) as any program or data held in electronic form. This includes programs that run or access the data, however, does not include the indicative information of unauthorised use of programs or data. For example, giving instructions on how to access unauthorised information. Authorities should consider improving the definition of "article" in art s37 (4) since many programs may be downloadable elsewhere and data can be accessed externally using internal indicative information.

In addition, Section 5 of the Forgery and Counterfeiting Act 1981 refers to 'Offences relating to money orders, share certificates, passports, etc'. Specifically, section 5 (5) of the Forgery

[313] Serious Crime Act 2007 c. 27. s. 46.

[314] Computer Misuse Act 1990 c. 18. ss. 1 and 2.

[315] Theft Act 1968 c. 60. s. 4 (1).

[316] Police and Justice Act 2006 c. 48. s. 37.

and Counterfeiting Act 1981 refers to misconduct in custody and money orders, such as money orders, share certificates and credit cards. This can be used for wrongdoings of crypto asset issuers, exchanges and custodian wallets. The forgery and counterfeiting documents consist of share certificates and passports, as well as credit cards, which to some extents are related to the Criminal Law Act 1977 and the Serious Crime Act 2007 defined as prohibited goods, subject to the usage of prohibited goods. Some activities are illegal under the definition of the Forgery and Counterfeiting Act 1981, including forging authorised documentation, custody or control of the machine, implement, paper or material for making counterfeiting documents.[317] Apart from forging and custody false documents or controlling of forging and custody false documents and the machine that makes it, persons who know or should know such illicit activities are also guilty under the Act.[318] The related wrongdoings of crypto assets can involve false authorised investment prospectuses and other supporting documents, cloned transaction orders or exchange platforms, and counterfeited certificates of authorising crypto asset businesses. The list is not exhaustive as there may be unidentified or undiscovered wrongdoings in relation to crypto asset crimes.

The Proceeds of Crime Act 2002 provides guidance on the sentencing of illicit earnings. The Act gives instructions on the procedures of assets recovery, confiscation, civil recovery, recovery of cash, forfeiture of money, and other related investigatory, enforcement and prosecution activities.[319] Since crypto assets possess combined features of information technology and finance and are widespread applications on the internet, the related crimes are likely transnational activities and may be carried out by individuals or organised criminal groups. Therefore, international coordination and cooperation, as well as data sharing have become essential combating against crypto asset crimes. In addition, the jurisdictions of prosecutions and law applications, as well as the sentencing standards also vary across countries.[320] This situation makes the proceeding of such crimes more complicated.

Illicit activities of crypto assets may also breach the Data Protection Act 2018 and The Privacy and Electronic Communications (EC Directive) Regulations 2003. The Data Protection Act 2018 defines the Personal data breach as ‘a breach of security leading to the accidental or

[317] Forgery and Counterfeiting Act 1981 c. 45. s. 5.

[318] ibid. s. 5 (1).

[319] Proceeds of Crime Act 2002 c. 29.

[320] Ryder (n 13). notes 1, 55 and 311. at pp. 10, 17 and 50.

unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.[321] This ensures that personal information, such as usernames and digital keys stored or safeguarded on a third party or a platform, is under protection. The Privacy and Electronic Communications (EC Directive) 2003 is a parallel regulation to the Data Protection Act 2018 and 'does not relieve the obligations under Data Protection Act 1998 in relation to the processing of personal data'.[322] Regulation 6 of the Privacy and Electronic Communications (EC Directive) 2003 — 'Confidentiality of communications' identifies misconduct of storing information or accessing stored information. It specifies that firms that store information shall inform users about the clear purposes of storing or accessing information and allow users to refuse to store or access their information.[323]

The abovementioned Acts are existing Laws that can be applied to make judgements for wrongdoings in relation to crypto assets activities. Either using crypto assets as a means of value transactions for illicit earnings or counterfeiting of documents regarding crypto assets activities, such as certificates of shares and exchange platforms, has been covered by these Acts. In addition, encouraging and controlling or having intentions to encourage and control misdeeds are also covered by the laws. Given the fact that money laundering is usually the last step for offenders to depart their illicit earnings from the origins, monitoring crypto assets related money laundering can be used as an efficient way to prevent financial and other crimes or reduce such intentions.

### 5.4.3 Anti-Money Laundering in the UK

On 10th January 2020, the FCA announced to be the anti-money laundering and counter terrorist financing supervisor of UK crypto asset activities under the amended Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2019 (MLRs).[324] The FCA requires crypto asset businesses to identify and assess the risks of money laundering in relation to their businesses; complying with anti-money laundering check to mitigate the possibility of the business being used for money laundering; appointing a senior manager to be the compliance

[321] Data Protection Act 2018 c.12. pt. 3, s. 33.

[322] The Privacy and Electronic Communications (EC Directive) Regulations 2003, SI 2003/2426. reg. 4.

[323] ibid. SI 2003/2426, regs. 6 (1) and 6 (2).

[324] The Money Laundering and Terrorist Financing (Amendment) Regulations 2019, SI 2019/1511. pt. 3.

officer with the MLRs; undertake customer due diligence; an enhanced due diligence check is required when dealing with customers who may present a higher money laundering risk.

The UK has been the central hub of the financial markets in the world over a few decades. This has attracted a large number of investors and traders, as well as speculators. Meanwhile, the vivid financial markets with considerable numbers of market participants also imply more chances to people who conduct wrongful businesses. Although crimes may happen in any kinds of forms, such as stealing and drug dealing, money laundering is a key conduit routing illicit earnings to the legal financial system. Thus, loose anti-money laundering compliance heightens the incentives of taking part in unlawful activities.

Crypto assets businesses shall comply with the requirements of registration, reporting and recordkeeping under the newly amended MLR 2019[325] in accordance with the Fifth EU AML Directive of the EU.[326] The EU 5AML Directive requests crypto asset businesses to comply with the requirements of the recordkeeping and reporting within the EU,[327] which includes some unregulated tokens in the UK, such as token custody wallet providers and token exchange platforms. The EU 5AML Directive is discussed in the Chapter of EU regulations in this thesis.

Therefore, the MLR 2019 extends the UK regulatory framework to some unregulated tokens defined by the FCA,[328] and the regulatory requirements are set for crypto asset exchanges and

[325] ibid. regs. 14A, 56A, 58A, 60A, 74A and 74B.

[326] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU [2018] OJ L156/43.

[327] FCA, 'Guidance on Cryptoassets Feedback and Final Guidance to CP 19/3' (n 35).

[328] The FCA final guidance paper on crypto assets excludes exchange tokens and utility tokens from its regulatory perimeters and categorises them as unregulated tokens. This means the requirements for business registration and the recordkeeping and reporting only apply to e-money tokens firms in the UK under the PSR 2017 and the Electronic Money, Payment Services and Payment Systems (Amendment and Transitional Provisions) (EU Exit) Regulations 2018. ibid.

custody wallets providers, including crypto asset businesses and individual practitioners.[329] However, there are levels of uncertainty about the cross-border regulation of money laundering in the UK due to the blurred circumstances of the Brexit, such as information sharing and jurisdictions.

The MLR 2019[330] is in force until the end of December 2020. In the meantime, the MLR (EU Exit) 2019[331] is enacted and may enforce after the transition period of the withdrawal of the UK from the EU. However, the MLR (EU Exit) 2019[332] is amended based on the MLR 2017 in accordance with the Fourth EU AML Directive and removes the power of EU Laws, thus, regulations on crypto asset have not yet been included. Therefore, crypto asset businesses shall comply with the MLR 2019[333] in 2020 and subject to change after December 2020. During the transition period between 10 January 2020 and 31 December 2020, the UK will continuously

[329] '14A.—(1) In these Regulations, "cryptoasset exchange provider" means a firm or sole practitioner who by way of business provides one or more of the following services, including where the firm or sole practitioner does so as creator or issuer of any of the cryptoassets involved, when providing such services—(a) exchanging, or arranging or making arrangements with a view to the exchange of, cryptoassets for money or money for cryptoassets, (b) exchanging, or arranging or making arrangements with a view to the exchange of, one cryptoasset for another, or (c) operating a machine which utilises automated processes to exchange cryptoassets for money or money for cryptoassets. (2) In these Regulations, "custodian wallet provider" means a firm or sole practitioner who by way of business provides services to safeguard, or to safeguard and administer—(a) cryptoassets on behalf of its customers, or (b) private cryptographic keys on behalf of its customers in order to hold, store and transfer cryptoassets, when providing such services. (3) For the purposes of this regulation—(a) "cryptoasset" means a cryptographically secured digital representation of value or contractual rights that uses a form of distributed ledger technology and can be transferred, stored or traded electronically; (b) "money" means—(i) money in sterling, (ii) money in any other currency, or (iii) money in any other medium of exchange, but does not include a cryptoasset; and (c) in sub-paragraphs (a), (b) and (c) of paragraph (1), "cryptoasset" includes a right to, or interest in, the cryptoasset'.The Money Laundering and Terrorist Financing (Amendment) Regulations 2019, SI 2019/1511. regs. 14A.

[330] ibid.

[331] The Money Laundering and Transfer of Funds (Information) (Amendment) (EU Exit) Regulations 2019, SI 2019/253.

[332] ibid. pt. 3.

[333] The Money Laundering and Terrorist Financing (Amendment) Regulations 2019, SI 2019/1511.

act as a participant and a member state of the FIUs, the Interpol and the Europol,[334] and follow the NIS requirements.[335]

The FCA has decided to adopt stricter Anti-Money Laundering regulations than the EU requirements in relation to crypto assets. For example, entities that carry on several activities will be requested to comply with AML regulation, including a) exchange and transaction services among crypto assets businesses; b) crypto asset ATMs; c) transfer crypto assets on behalf of individuals or legal persons; d) ICOs; and e) open-source software, such as custodian wallet software.[336]

The FCA believes that crypto assets hold relatively smaller shares of the financial markets in the UK and Fintech firms demand a relaxed and innovative environment to incubate technology developments. Although the FCA recognises the insufficiencies in the existing regulatory framework, it will update the regulation of crypto asset gradually when the market becomes more mature.[337] The UK Europol has explored increasing numbers of cases in relation to crypto assets taking place in the UK, and there have been arrests of crypto assets related money laundering.[338] However, relevant trials or cases have not been reported publicly at the time of writing. I once had an opportunity to speak to officers from Europol, Interpol and NCA on 14th November 2019 at a University event.[339] I queried why no further information made public after those arrests. I was told that unreleased reports on some cases are perhaps because of the pending decision on the dates or jurisdictions of trials given the complexity of the international involvement. In addition, court proceedings may be filed as highly confidential, therefore, not appropriate to be public.

---

[334] FCA, 'Payment Services and Electronic Money – Our Approach The FCA's Role under the Payment Services Regulations 2017 and the Electronic Money Regulations 2011' (2018).; and <https://www.europol.europa.eu/partners-agreements/member-states/united-kingdom> accessed 17 April 2019.

[335] https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018

[336] FCA, 'Guidance on Cryptoassets Feedback and Final Guidance to CP 19/3' (n 35). para. 46. at p. 36.

[337] ibid. at pp. 16 and 23.

[338] 'Cryptocurrency Laundering as a Service: Members of a Criminal Organisation Arrested in Spain | Europol' (n 122). 'Cryptocurrency IOTA: International Police Cooperation Arrests Suspect Behind10 Million EUR Theft | Europol' (n 297).

[339] National Crime Agency - An International Perspective organised by Target Connect, Bangor University.

# 6 Regulation of Crypto Assets in the EU

## 6.1 Analysis of General Regulations

The European Banking Authority (EBA) carried out a comprehensive assessment of crypto assets in early 2019.[340] The EBA assessment paper explicates the characteristics and risks of crypto assets in the financial systems and emphasises the importance of coordination among member states. Under the assessment, the EBA categorises crypto assets into three groups: exchange/payment/currency tokens, investment tokens and utility tokens. This classification indicates that the identification of crypto assets is based on property rights and applications. Of which, the investment tokens relate to property rights and the other two types of tokens are to-date the main applications of crypto assets. The EBA also clarifies the EU financial services laws applicable to commercial activities of crypto assets. For instance, certain types of crypto assets that fall within the ambit of electronic money and financial instruments are regulated under the second Electronic Money Directive (EMD2), the second Payment Services Directive (PSD2) and the Markets in Financial Instruments Directive (MiFID II).[341] The EMD2 sets out the rules for the business practices and supervision of electronic money institutions;[342] the PSD2 regulates new payment services and promotes digital payment competition and user protection within the EU;[343] the MiFID II aims to strengthen investor protection and improve the efficiency, transparency and resilience of financial markets within the European Commission.[344]

Under these Laws and Regulations, regulated crypto assets in the EU must consist of specific properties. For example, crypto assets that present characteristics of e-money, such as pegging against fiat currency and for making payments, fall within the regulations of EMD2 and

[340] EBA, 'Report with Advice for the European Commission on Crypto-Assets' (2019) <https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf> accessed 16 December 2019.

[341] ibid. para 4. at p. 6.

[342] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC [2009] OJ L267/7. recitals.

[343] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L337/35. recitals.

[344] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU [2014] OJ L173/349. recitals.

PSD2;[345] crypto assets that meet the definition of transferable securities may be qualified as financial instruments under the MiFID II.[346] However, the Laws haven't yet set rules for the utility and exchange types of crypto assets.[347] Therefore, regulations of other types of crypto assets are subject to national Laws and national implementation of EU Laws of each member state.[348]

In addition, the EBA defines crypto assets that possess security-like properties as investment tokens. These tokens must be negotiable and transferable on capital markets, such as shares of investment, bonds and debts. The definition of transferable securities follows the MiFID II:

> 'transferable securities means those classes of securities which are negotiable on the capital market, with the exception of instruments of payment, such as:
>
> (a) shares in companies and other securities equivalent to shares in companies, partnerships or other entities, and depositary receipts in respect of shares;
>
> (b) bonds or other forms of securitised debt, including depositary receipts in respect of such securities;
>
> (c) any other securities giving the right to acquire or sell any such transferable securities or giving rise to a cash settlement determined by reference to transferable securities, currencies, interest rates or yields, commodities or other indices or measures'.[349]

The EBA report emphasises the detriments to consumer protection and market integrity that crypto assets may bring about. First, consumers may invest in crypto assets for value appreciation with unclear information about the regulatory status of the invested crypto assets or trading platforms. Invested crypto assets may fall outside existing regulatory frameworks and authorised businesses may operate unregulated crypto assets. Thus, investors' rights are

[345] EBA, 'Report with Advice for the European Commission on Crypto-Assets' (n 340). section 2.1. at pp. 12 - 15.

[346] ibid. paras 19 and 71 at pp. 12 and 29.

[347] ibid. para 66. at p. 28.

[348] ESMA, 'Advice Initial Coin Offerings and Crypto-Assets' (2019) <https://www.esma .europa.eu/sites/default /files/library/esma50-157-1391_crypto_advice.pdf> accessed 18 July 2019. para 80. at p. 19; ibid. para 28. at p. 15.

[349] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU [2014] OJ L173/349. art. 4 (1) (44).

not fully protected. This places some investors in an unfavourable position even not to mention the drastic price fluctuations of crypto assets. Meanwhile, unregulated crypto assets face greater business uncertainty than regulated ones. Unregulated crypto asset businesses may be banned or shut down due to policy change. For example, the UK authority, the FCA, has considered banning the sale of derivatives linked to certain types of unregulated crypto assets to retail clients.[350] Additionally, the one passporting system within the EEA and the diverse domestic regulations of crypto assets may cause inconsistency between the national and EU regulations. Crypto asset businesses authorised/licensed in one country may be unregulated or even banned in another country. The typical example is the exchange tokens allowed in Germany[351] operating in the UK.[352]

Second, operating unregulated crypto asset products or services does not necessarily mean breaching the laws as unregulated crypto assets have not yet been treated as illegal/prohibited products. Consumers are exposed to risks. Businesses provide crypto assets products and services are usually regulated under Commercial/Company Laws of member states. Such businesses comply with business registration carry out daily operations as traditional firms, including product promotion. However, business registration does not stop a business providing both regulated and unregulated crypto assets products and services. Consumers may be unable to identify the regulatory status of crypto asset. A trickier situation is that crypto asset businesses are licensed in one country but operating in another within the EU under different regulatory schemes and the single market system. This is especially worrisome for EU countries that haven't yet established regulatory regimes for crypto asset businesses/products.

In addition, the EBA report underlines the importance of the establishment of a consistent accounting standard for crypto asset businesses and products.[353] A standardised accounting report can assist with identifying the rights and interests of crypto asset shareholders and investors, in the meantime, it can clarify the corporate assets of crypto asset businesses. The

[350] FCA, 'Guidance on Cryptoassets Feedback and Final Guidance to CP 19/3' (n 35). para. 1.37. at p. 8.

[351] Exchange tokens like Bitcoins are specified as financial instruments in Germany. 'BaFin - Virtual Currency' (n 46).

[352] Exchange tokens fall outside the regulatory perimeters of the FCA and are categorised as unregulated crypto assets in the UK. FCA, 'Guidance on Cryptoassets Feedback and Final Guidance to CP 19/3' (n 35). paras. 43 - 47. at pp. 35 - 36.

[353] EBA, 'Report with Advice for the European Commission on Crypto-Assets' (n 340). para 72. at p. 29.

EBA report suggests a possible accounting standard for security/investment/debt types of crypto assets. These types of crypto asset must be value-stabilised and converted against fiat currency and fall within the regulated crypto assets under the EBA regulation recommendations. Thus, these types of crypto assets are recommended to be treated as tangible assets or liability.[354] However, it is unclear whether to treat crypto assets as intangible assets at firms that invest in crypto asset products given the digital properties of such investments.

## 6.2 Analysis of Crypto Assets Regulations in EU Countries

The regulation of crypto assets cannot simply follow the regulations of traditional financial products. Traditional financial products are regulated by central banks and financial market authorities under the one passporting system and the EU Laws. Whilst the regulation of crypto asset within the EU is not yet harmonised across member states. This challenges the EU single market system if firms operate crypto asset businesses in more than one EU countries. This section provides an insight into the crypto asset regulation and status in some economies in the EU, including Germany, Malta, France, Italy, Spain and Ireland. Of which, Germany and Malta have promulgated Laws and Regulations on crypto assets; France and Italy are in the process of introducing the regulations on crypto assets; Spain and Ireland have not yet demonstrated intentions to establish a regulatory regime.

### 6.2.1 Germany

Germany is the first EEA member that has recognised crypto assets since 2013 by the Federal Financial Supervisory Authority (BaFin) and has established regulatory schemes under the German Banking Act 1998 amended in 2014.[355] The German authorities define crypto assets as financial instruments under the Banking Act 2014 regardless of the technology applied. Under this definition, exchange tokens like Bitcoins are recognised as financial instruments.[356] The establishment of regulatory regimes of crypto asset indicates the business inclusion of new technologies and has attracted many DLT related investors and developers coming to set up their businesses in Germany.[357]

[354] ibid. section 4.3. at pp. 26 - 27.

[355] 'Banking Act (KWG)' (n 28).

[356] 'BaFin - Virtual Currency' (n 46).

[357] BaFin (n 53). at p. 46.

The Banking Act 2014 defines financial instruments in the German financial system, and it is applicable to German or foreign legal person/persons.[358] The Act defines financial instruments as: a) shares, certificates representing shares or comparable to shares; b) investment products except of stakes in a cooperative society; c) debentures and bonds which are tradable in the capital markets, except payment instruments; d) purchase or sale rights in accordance with shares, investments and debentures/bonds; e) collective investments; f) money market instruments except for payment instruments; g) foreign exchange or units of account; g) derivatives.[359] The Act excludes the Deutsche Bundesbank, the banking group, the Federal Employment Agency, insurance undertakings and risk capital investment companies from credit institutions and financial services institutions.[360]

Following the definition, German authorities treat majority types of crypto assets as financial instruments because they are 'Units of account are comparable to foreign exchange; value units which function as private means of payment in barter transactions that is used as means of payment'.[361] However, the Banking Act excludes payment instruments from the definition of financial instruments. Therefore, the German authorities do not treat crypto assets as e-money under the German Payment Services Supervision Act 2009,[362] because crypto assets 'do not represent any claims on an issuer, as in their case there is no issuer'.[363]

> '(3) Electronic money is all electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of fund for the purpose of making payment transactions within the meaning of section 675f subsection (3), first sentence, of the Civil Code and which is accepted by a natural or legal person other than the issuer'.

[358] '(11) Financial instruments within the meaning of subsections (1) to (3) and (17) as well as within the meaning of section 2 (1) and (6) are — 1 shares and other stakes in German or foreign legal persons, commercial partnerships and any other undertakings if these stakes are comparable to shares, as well as certificates representing shares or stakes comparable to shares'. 'Banking Act (KWG)' (n 28). s. 1, sub-s (11) 1.

[359] ibid. s.1 (11).

[360] ibid. ss. 2 (1), (2) and 2 (6).

[361] 'BaFin - Virtual Currency' (n 46).

[362] Act on the Prudential Supervision of Payment Services (Payment Services Supervision Act) 2009. ss. (1a) (1) (5) and (1a) (3).

[363] 'BaFin - Virtual Currency' (n 46).

In addition, the German central bank indicates that authorisation requirements for platforms and exchanges 'must be made between the transactions' technical execution and their individual configuration" while crypto asset platforms that carry out broking-like services "shall follow the German Commercial Code'. Individual mining and transactions between individuals do not require authorisation.[364] This means that the authorisation of the crypto asset trading platforms is considered on a case by case basis.

The regulatory regimes demonstrate that the German regulation of crypto assets focus on commercial activities rather than product types. This is a facilitating method for authorities to monitor the compliance and business practice of crypto asset firms under the speedy variation of DLT products. The BaFin published an Advisory Letter on the legal classification of ICOs and crypto assets in March 2018.[365] The Advisory Letter specifies crypto assets based on applications and services. For example, a token that is transferable and negotiable on the financial markets or capital markets is treated as security or security-like instrument, and a token that is used as proof of rights and interests at a company is treated as capital investment. In addition, the Advisory Letter sets forth and clarifies that the crypto assets are not alternative currency or representatives of legal tender. Therefore, operating crypto asset businesses like banking and financial services is not permitted in Germany and firms may face a punishment of up to five years in prison or fines, accordingly. The Advisory Letter requests 'a precise case-by-case assessment' to identify the types of crypto asset businesses, as one crypto asset product may lie in multiple classes and one firm may provide multiple crypto asset products.[366]

Although the regulation of crypto assets in Germany is clear but still has caused inconsistency to some extents. Disparate understanding of the laws has led to conflicting legal interpretations. For instance, the ambivalent interpretations of the laws in a case between a Bitcoin service provider and the public prosecutor's office of Berlin [2018].[367] Polish authorities suspected that a Bitcoin trading platform registered in Germany had been hyping up bitcoins and money laundering since March 2013. The bitcoin trading platform took legal advice to temporarily suspend its business operation and eventually closed down in April 2013, while its bank

[364] ibid.

[365] Supervisory classification of tokens or cryptocurrencies underlying "initial coin offerings" (ICOs) as financial instruments in the field of securities supervision 2018 (Universitas Nusantara PGRI Kediri).

[366] ibid. section 4. (n/p).

[367] 'Citizen Service Berlin - Brandenburg - Criminality of Trade in Bitcoins' (n 32). The court judgement is in Germany; thus, the information is based on Google translation.

account was terminated by the Polish authorities soon after on 17 June 2013. The public prosecutor's office of Berlin sued Bitcoin for alleged violations of the Banking Act 2014. The lawsuit is taking place on the ground that Bitcoins are financial instruments, therefore shall apply for a licence to provide banking services and are liable to carry out due diligence measures of anti-money laundering. However, the court does not treat Bitcoins as financial instruments and stated that Bitcoins do not need a banking licence to operate in Germany because Bitcoins are neither legal tender nor units of accounts. The court judgement is somehow inconsistent with the definition of Bitcoin-like crypto assets by the German central bank on their official website, which defines Bitcoins as financial instruments. Under this definition, Bitcoins exchanges and service providers shall operate businesses under the Banking Act 2014.[368]

The public prosecutor's office filing a lawsuit and the court making the judgement both were based on Section 1 (11) of the Banking Act 2014. The inconsistency was caused by the disparate understanding and interpretation of the 'Financial Instruments' between the court and the public prosecutor's office in terms of crypto assets. The main conflict of this case was the differences between financial instruments under the Banking Act 2014 and payment instruments under the Payment Service Act 2009. The Banking Act 2014 defines foreign exchanges, money market instruments and investment products as financial instruments exception of payment instruments. While crypto assets are neither recognised as legal tender nor accounting units in Germany, thus are not categorised as e-money and are not allowed to operate banking and financial services as e-money under the Law. In this particular case, the Bitcoin trading platform was a trading platform and an exchange broker of Bitcoins that did not provide payments services and was independent of the Bitcoins providers/issuers. The public prosecutor's office understood that the Bitcoin as a financial instrument and the exchange platform shall be responsible to apply for a banking licence. However, the court identified that the Bitcoin platform was not operating banking and financial services like e-money as Bitcoins are not legal tender nor account units and therefore, are not payment instruments under the Payment Service Act.[369] By virtue of the fact that Bitcoins exchanges and services providers do not carry on e-money and banking services, therefore, are not requested to apply for a banking licence to operate their businesses. The case also causes

[368] 'BaFin - Virtual Currency' (n 46).

[369] Act on the Prudential Supervision of Payment Services (Payment Services Supervision Act) 2009. s. (1a) (1) (5) (3).

confusion for the legal professions due to the different understanding of financial instruments and payment instruments.[370]

Nevertheless, the German laws and regulations of crypto assets have played an important role in attracting investors and innovators. The BaFin annual report stated that the number of ICOs in Germany in 2018 has shown a noticeable upward trend. For instance, the BaFin recorded an increase in the number of new authorisation queries of fintech companies, initial coin offerings (ICOs) and new payment services from 1,022 in 2016 to 1,397 in 2018.[371] Taking this as a successful precedent, other EU countries may follow the German regulations to attract investment and ICOs and encourage innovations in Fintech and new payment services.

### 6.2.2 Malta

Maltese authorities offer strong support to promote financial inclusion and innovation in terms of the DLT and crypto assets. The Central Bank of Malta asserted that Malta is the one among the first EU countries that established a regulatory regime for crypto asset businesses. The regulatory schemes include crypto asset ICOs as well as trading and exchange platforms.[372] The Maltese authorities promulgated three Acts to regulate and guide ICOs and further financial innovation. The three Acts are the Virtual Financial Assets Act 2018, the Malta Digital Innovation Authority (MDIA) Act 2018 and the Innovative Technology Arrangements and Services (ITAS) Act 2018.

The Virtual Financial Assets Act 2018 regulates 'the field of Initial Virtual Financial Asset Offerings and Virtual Financial Assets and to make provision for matters ancillary or incidental thereto or connected therewith'.[373] This Act regulates almost all types of crypto assets and related activities, including e-money tokens, financial instrument tokens, exchange tokens, utility tokens and investment tokens.[374] This Act also indicates other applicable laws that set rules for illicit activities in relation to crypto assets, such as money laundering and fraud.[375]

---

[370] 'Germany: Court Holds That Bitcoin Trading Does Not Require a Banking License | Global Legal Monitor' <https://www.loc.gov/law/foreign-news/article/germany-court-holds-that-bitcoin-trading-does-not-require-a-banking-license/> accessed 8 December 2019.

[371] BaFin (n 53). at p. 46.

[372] 'Distributed Ledger Technology and Virtual Currencies - Central Bank of Malta' (n 47).

[373] The Virtual Financial Assets Act 2018, Cap. 590. at p. 1.

[374] ibid. s. 2 (2). at. p. 3.

[375] ibid. s. 28 (5) (e), and ss. 53 (3) and 53 (5). at pp. 25 and 47.

The regulation also complies with the EU Laws, such as the 5AML Directive[376] and MiFID II.[377] Under the Laws, firms that are not complying with the domestic Laws and the EU Laws face penalties up to €150,000.[378]

The establishment of the regulatory agency, the Malta Digital Innovation Authority (MDIA)[379] marked the determination and orientation of the Maltese authorities for the national development. The MDIA regulates financial innovation under the Malta Digital Innovation Authority (MDIA) Act 2018.[380] The MDIA aims to promote developments, education and standards of innovative technology agreements and to safeguard user rights and data security.[381]

In addition, the Innovative Technology Arrangements and Services (ITAS) Act 2018 sets rules for promoting technological innovation. The Act regulates the certifying process and the standard of innovative technology and services, the registration of service providers, and the eligibility of applying for certificates and registration.[382] Meanwhile, the Act demonstrates the inclusive regulations in Malta to international investors and technology developers. The Act sets up certain criteria to allow overseas technological innovators establishing businesses in Malta.[383] For example,

> '(3) The holder of an innovative technology authorisation shall ensure that it has a validly appointed resident agent at all times when there is no person involved in the administration of the holder who is resident in Malta:
>
> Provided that:
>
> (a) if both the innovative technology arrangement and the technical administrator appointed with reference to it are not resident in Malta, the appointment of a resident agent for the technical administrator shall satisfy the requirement under this article also for the innovative technology arrangement for as long as such technical

[376] ibid. s. 2 (2). at p. 2.

[377] ibid. s. 2 (2). at p. 5.

[378] ibid. ss. 38 (5) and 48 (1). at pp. 33 and 43.

[379] https://mdia.gov.mt

[380] The Malta Digital Innovation Authority Act 2018.

[381] ibid. s. 4 (2). at p. A1357.

[382] The Innovative Technology Arrangements and Services Act.

[383] ibid. s. 15 (3) (a). at p. A1489.

administrator is engaged and the engagement of the resident agent is made by the technical administrator also for the innovative technology arrangement on being authorised to do so;'

These inclusive and open policies make Malta an attractive country for technology developers and investors. However, this inclusive environment may also be used as a convenient platform for illicit activities, such as fraudulent trading/exchange platforms. This will challenge the regulatory capacities of the authorities and Regulatory Technologies (RegTech).

### 6.2.3 France

French authorities have been trying to put crypto asset businesses in train to attract investment and promote technology innovation. The French authorities have adopted a series of actions to establish the regulatory regimes of crypto asset businesses. For example, the Action Plan for Business Growth and Transformation of France (the Plan d'Action pour la Croissance et la Transformation des Entreprises, PACTE) drafted a Bill and submitted it to the French National Assembly on 11 April 2019. The Bill sets rules for the regulation of crypto asset businesses in France and constructs the regulatory framework to facilitate access to diversified funding.[384]

The Financial Markets Authority of France (Autorité des Marchés Financiers – AMF) interprets the provisions of the regulatory regime of crypto assets. Upon the enactment of the abovementioned Bill, the French authorities will provide alternative licences for crypto asset businesses. Two alternative licences, the Optional Visa for ICOs and the Optional licence for digital assets services providers, will be available for eligible crypto asset businesses to apply for.

The Optional Visa for ICOs promotes the investments and fundraising through Initial Coin Offering (ICO). This licence is optional and the raising of funds without it will remain legal in France. However, crypto asset issuers that do not hold the licence will be unable to use general solicitation. In addition, crypto asset businesses must be a legal entity registered in France, and a detailed prospectus is required. Entities that granted the Optional Visa are responsible for

[384] 'PACTE, the Action Plan for Business Growth and Transformation in France | Gouvernement.Fr' <https://www.gouvernement.fr/en/pacte-the-action-plan-for-business-growth-and-transformation> accessed 2 January 2020.

monitoring and safeguarding the assets raised during the offering and complying with the Anti-money Laundering and terrorist financing rules.[385]

The Optional licence for digital assets services providers is applicable to crypto assets exchanges and trading platforms. The AMF defines digital assets as 'tokens issued during ICOs and virtual currencies defined by European Laws". Crypto asset services providers include "custody of digital assets for third parties; purchase or sale of digital assets against legal tender or other digital assets (broker/dealer); operation of a digital assets trading platform (stock exchange); other digital assets services such as the reception and transmission of third-party orders, third-party portfolio management, advice, underwriting and placing on or without a firm commitment basis'.[386] This definition does not distinguish types of crypto assets from one to another. Therefore, all types of crypto assets ICOs and crypto asset services providers are eligible to apply for the alternative licences, including Bitcoins. However, crypto assets that exercise like financial instruments haven't yet been included in this regime.

The AMF also specifies mandatory registration requirement for all crypto asset businesses in France regardless of whether the business obtains the optional licence. The mandatory rules consider 'the reputation and competency of their corporate officers and shareholders and the existence and implementation of Anti-money Laundering and terrorist financing procedures'. The AMF will consult the French Prudential Supervisory and Resolution Authority (Autorité de contrôle prudential et de résolution) to make decisions on accreditation of business registration.

Meanwhile, the AMF may allow certain types of funds entering crypto asset markets as fund investments. Those funds shall be professional specialised investment funds that comply with the liquidity and valuation rules and limited total investment up to 20% of their total assets. ICOs and services providers without obtaining the alternative licences, accordingly, will be prohibited from 'solicitation, patronage and sponsorship activities', except advertising. The AMF may also publish a 'blacklist' for those crypto asset businesses that do not comply with

[385] Optional Visa for ICOs. AMF, 'Towards a New Regime for Crypto-Assets in France' (2019) <https://www.amf-france.org/en_US/Reglementation/Dossiers-thematiques/Fintech/Vers-un-nouveau-regime-pour-les-crypto-actifs-en-France> accessed 2 July 2019.

[386] Optional licence for digital assets services providers. ibid.

the regulation. Additionally, the French authorities proposed the Bill to the EU committee aiming to establish a standardised ICO procedure within the EEA member states.[387]

Despite the exclusion of financial instrument type of crypto assets, the regulation of crypto asset in France mainly focuses on the business registrations and commercial practice rather than product types. This mechanism is simple and clear for regulators and businesses, as well as consumers, to identify the regulatory status of crypto assets. Nevertheless, the Bill has not been enacted or updated at the time of writing.

### 6.2.4 Italy

The regulation of crypto assets in the Italian financial system is at an early stage. The Bank of Italy analysed the risks of crypto assets and published a working paper in October 2019 concluding that crypto assets complicate the systems of laws, regulations and enforcement.[388] This paper examines the application of the DLT, and crypto assets underpinned by it. The paper uses Bitcoins as a representative of one type of crypto assets that are decentralised and permission-less and carry out transactions with private digital keys. Based on this definition, the paper claims that Bitcoin-like crypto assets are not in the category of money and financial instruments. In addition, the paper suggests taking the price fluctuation of crypto assets into consideration while making prudential decisions.

Meanwhile, the increasing popularity of crypto assets has drawn the attention of another financial authority in Italy. The Companies and Stock Exchange Commission of Italy (CONSOB) published a consultation paper in March 2019 asking for a possible framework for a national regulatory regime and views on the proposal of regulation of ICOs, exchanges and related negotiations.[389] The CONSOB recognises the inconsistent regulatory schemes among the EU member states, particularly on whether define all crypto assets as financial instruments under MiFID II or investment/shares/debts under EU legislation, such as the Packaged Retail and Insurance-based Investment Products (PRIIPs).[390]

---

[387] The possibility for certain funds to invest in digital assets and Measures to protect investors. ibid.

[388] Carlo Gola and Andrea Caponera, 'Policy Issues on Crypto-Assets' (2019) Università Cattaneo Working Papers <http://dx.doi.org/10.25428/2532-554X/7> accessed 27 October 2019.

[389] CONSOB, 'Initial Coin Offerings and Crypto-Assets Exchanges Call for Evidence' (2019) < https://www.iosco.org/library/ico-statements/Italy%20-%20CONSOB%20-%2020190319%20-%20Initial%20Coin%20Offerings%20and%20Crypto%20Assets %20Exchanges%20Call%20for%20Evidence.pdf > accessed 27 March 2020.

[390] ibid.

The CONSOB received 61 responses in June 2019 and the final decision was published on 2 January 2020.[391] The final report is not yet published in English. According to the press release on CONSOB website, the final report interprets the national regulatory regime governing the conduct of ICOs and related negotiations and clarifies the definition of crypto-assets for the purposes of the proposed legislation, the regime of ICOs, and the regulation of crypto asset exchange/trading platforms and wallet custodians. As stated on the press release, 'the objective of this exercise is to identify possible regulatory solutions to regulate some crypto activities that cannot be assimilated to financial instruments and therefore require specific discipline suitable for providing a new reference framework for operators and investors'. This raises a question if the Italian regulators treat crypto assets that present similar characteristics to current financial instruments as traditional financial instruments and regulating them under the same category and regulatory regime.

Although the Italian authorities have made an effort to identify and clarify crypto assets related businesses and activities, the crypto asset markets in Italy are still waiting for further clarification. For instance, the Cryptonomist, a website for crypto asset information in Italy, published a discussion about the final decision paper and suggested that 'the report shows that the definition of crypto assets is not clear enough, due to the difficulty in distinguishing between those that can be classified as financial instruments and those that cannot be classified as such'.[392]

Nevertheless, the regulatory scheme of crypto assets in Italy is in the initial stage. It requests time to the regulators to update their knowledge and understanding of the technology and the logic behind crypto asset products. Besides, it requires time for the markets to become mature.

### 6.2.5 Spain

The Spanish authorities haven't yet shown their interest in establishing a regulatory regime for crypto asset businesses or products. The Bank of Spain only started to study Bitcoins in 2019 and published a working paper that provides the official reviews on the basic functioning and applications, as well as the properties and characteristics of Bitcoins. The working paper of the

[391] CONSOB, 'Crypto-Activity: A Contribution for A National Regulatory Regime from Consob (Press Release January 2, 2020)' <http://www.consob.it/web/consob/dettaglio-news/-/asset_publisher/hZ774IBO5XPe/content/comunicato-stampa-del-2-gennaio-2020-hp/11973> accessed 3 January 2020.

[392] 'Italian CONSOB: Two Registers for Managing Crypto Assets - The Cryptonomist' <https://en.cryptonomist.ch/2020/01/02/italian-consob-registers-for-crypto-assets/> accessed 3 January 2020.

Central Bank denotes that crypto assets are operating on a system without scrutiny and Bitcoins present little impact on the current financial systems and payment systems compared with the current financial services that banks and financial firms are providing.[393]

Indeed, the market share of crypto assets in the Spanish financial system is barely a ripple. However, the ignorance of the new technological development may lead to the regulatory technologies of Spain lagging behind. Given the fact that some Spanish citizens were involved in several international crypto asset crimes, the regulators need to pay more attention to the Fintech development in Spain.

### 6.2.6 Ireland

The Irish authorities are also conservative in the case of crypto assets. The Central Bank of Ireland (CBI) published three announcements warning the risks of crypto asset businesses, especially risks to uninformed consumers. The first alert was announced around late 2014.[394] The other two warnings are announced (no dates were shown on the announcement webpages) following the EBA warning and opinions issued in December 2013[395] and July 2014, respectively.[396]

Although crypto assets have become popular and gone into their booming period of development, The Irish authorities are still consistent with their previous opinions on the regulatory regimes. The Central Bank of Ireland published a notice in December 2017 in terms of crypto assets ICOs. The notice emphasises the risks of crypto assets to consumer protection, such as illicit activities, price volatility and technological flaws. It concerns that consumers may be lured by the price appreciation of crypto assets, whereas becoming victims of cyberattack (online stealing), price fluctuation (on trading platforms) or crypto asset business

[393] Carlos Conesa, 'Bitcoin: A Solution for Payment Systems or a Solution in Search of a Problem?' (2019) Banco de Espana Ocassional Paper No. 1901 < https://dx.doi.org/10 .2139/ssrn.3333693 > accessed 22 May 2019.

[394] 'EBA Warning and Opinion on Virtual Currencies | Central Bank of Ireland' (2014) <https://centralbank.ie/consumer-hub/consumer-notices/eba-opinion-on-virtual-currencies> accessed 30 October 2019.

[395] EBA, 'Warning to Consumers on Virtual Currencies' (2013) < https://eba.europa.eu/sites/default/documents/files/documents/10180/598344/b99b0dd0-f253-47ee-82a5-c547e408948c/EBA%20Warning%20on%20Virtual%20Currencies.pdf?retry=1> accessed 20 December 2019.

[396] EBA, 'EBA Opinion on "Virtual Currencies"' (2014) < https://eba.europa.eu/sites/de fault/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20Currencies.pdf?retry=1 > accessed 16 July 2019. paras. 172 - 173. at p. 43.

shutdown (trading platforms/exchanges/issuers). Consumers who are lack of relevant knowledge and risk awareness are even more vulnerable.[397]

Therefore, soon after in February 2019, The Central Bank of Ireland reaffirms the abovementioned risks and urges consumers to avoid taking risky activities.[398]

### 6.2.7 Summary

The regulations of crypto assets within the EU member states demonstrate are diverse among each other. The abovementioned representative countries hold different viewpoints on both products and businesses of crypto assets. Germany and Malta are fully open to technological innovation and welcome almost all types of crypto assets as long as they follow the Laws and the requirement of business registration and compliance. Germany clearly excludes e-money like crypto assets from the regulatory categories. Crypto asset businesses that provide banking and financial services without authorisation will face serious punishments in Germany. France and Italy are embracing the waves of the technological changes in the financial sector with different paces, although their regulatory policies remain unclear to some extents; Spain has not yet paid sufficient attention to the matters of global crypto asset market growth, and does not seem to establish regulatory regimes of crypto assets in the near future.; Ireland sees crypto assets as risky products, especially to consumers. The UK holds an equivocal attitude towards crypto assets and decides to regulate specific types of crypto asset products instead of the businesses, for example, certain types of security tokens and e-money tokens.

Nevertheless, this diverse regulation across EU member states reflects some foregoing issues. The divergent regulations and laws of crypto assets across EU member states may puzzle both business providers and consumers, as well as regulators themselves. First, regulated business providers may be required to apply for multiple licences to run different crypto-tokens businesses in different countries. For instance, crypto asset businesses registered in Malta may hold both regulated and unregulated tokens when operating in the UK, thus firms need to request relevant authorisation for the regulated tokens. However, it does not stop non-UK businesses running unregulated tokens in the UK through the internet.

---

[397] 'Alert on Initial Coin Offerings | Central Bank of Ireland' (2017) <https://centralbank.ie/consumer-hub/consumer-notices/alert-on-initial-coin-offerings> accessed 30 October 2019.

[398] 'Consumer Warning on Virtual Currencies | Central Bank of Ireland' (2018) <https://centralbank.ie/consumer-hub/consumer-notices/consumer-warning-on-virtual-currencies> accessed 30 October 2019.

Second, consumers are more likely bewildered by the inconsistency between the national Laws and the EU Regulations when facing various crypto-tokens available online. These tokens may be licensed in different countries under the single market system in the EU. For instance, crypto assets issuers and exchange platforms registered in Germany are presumably able to provide such services across the EU under the single market system. This situation exposes consumers in a vulnerable position to misleading marketing or financial scams.

Third, although crypto assets are not recognised as representatives of fiat currency by any authority in any country, certain types of crypto assets behave like e-money are recognised as e-money tokens in some countries, such as the UK, whereas completely banned in others, like Germany. This situation allows a business to register e-money tokens under the UK regulation while to operate e-money business in Germany via the internet. There have been concerns over the inconsistency between the EU regulation and national regulations of crypto assets that may complicate the litigation systems, especially when it comes to cross-border financial crimes.

Besides, a consistent accounting norm in relation to crypto assets investment and businesses requires standardisation. A standardised accounting format will help to clarify investors' rights and interests. This is particularly important to the investment/security/debt types of crypto assets that are generally accepted by most of EU authorities, especially when crypto asset businesses face bankruptcy or shutdown.

All in all, the regulation of crypto assets in the EU is in the initial stage. The regulators need to update their knowledge and understanding about the new technology and enhance their relevant skills to ensure appropriate and prudential policymaking.

## 6.3 Illicit Activities of Crypto Assets in the EU

### 6.3.1 Transnational activities

As discussed in section 5.4 (illicit activities of crypto assets in the UK), illicit activities relating to crypto assets include mainly online stealing, wire fraud and counterfeit, scams, selling prohibit goods, computer misuse and money laundering. Those illicit activities are the internet-based and across countries. These internet-based crimes can easily take place within countries that speak common languages and convenient market environments. Countries that have strong economies may become the targets of financial crimes while countries that have loose regulatory schemes may be chosen to hedge and launder illicit earnings. In traditional financial markets, foreign exchange control places inconvenience for illicit earnings moving around and the anti-money laundering policies request all banks and financial firms reporting suspicious

transactions. These rules and regulations cannot stop all financial crimes but increase the cost and difficulty of crimes. However, these are no longer issues if criminals use crypto assets as the channel of moving around illicit earnings.

The European Economic Area have had free movement for goods and money within the member states since 1994. This free movement has functioned in reducing the cost and barriers of trade and establishing a harmonised legal and regulatory system for commercial activities within the EEA. However, the free movement has also created a convenient channel for international financial crimes. Financial offenders can take advantages from the free trade policies and move illicit goods and earnings around without foreign exchange controls.

Therefore, trade-off policies are inevitable. Since the main aims of the EU are for a united economic growth and trade, non-commercial crimes are normally ruled under domestic Laws, although some of those crimes have moved from offline to online. Such non-commercial crimes are commonly restricted in all countries.

The discussion of illicit activities of crypto assets in the EU focuses on anti-money laundering regulations. Anti-money laundering is crucial to prevent illicit earnings converting into legal financial circulation. A comprehensive and international anti-money laundering scheme is to deter criminal incentive and, in some ways, forestall illicit activities. It is even more crucial given the fact that money laundering has become transnational and grouped crime.[399] This requires a closer collaboration between EU member states and an efficient system for information exchange. Besides, a consistent reporting and recordkeeping scheme for anti-money laundering within the EU shall improve the communication efficiency within the EU.

### 6.3.2 Anti-Money Laundering in the EU

The European Union has updated its regulatory policies regarding online activities that involve crypto assets in a timely manner with focusing on anti-money laundering regulation. The EU included electronic money in its anti-money laundering regulation in 2015[400] and has

[399] Ryder (n 13). at pp. 10 - 19.

[400] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council and Commission Directive 2006/70/EC [2015] OJ L141/73. ch. II, Art 12. at pp. 91 - 92.

encompassed crypto assets businesses in the 'Fifth Anti-Money Laundering Directive[401] adopted on 19 June 2018. The Fifth AML Directive regulates the registration, reporting and recordkeeping for crypto assets exchanges and custody wallet providers.[402] Member states shall implement the Fifth AML Directive into national Laws by 10 January 2020.[403]

The Fifth AML Directive addresses the risks of the engagement between crypto assets and fiat currencies and emphasises the importance of extending the regulatory scope of the Directive (EU) 2015/849 (known as the Fourth AML Directive) to monitor crypto assets exchange businesses and custody wallet providers, thereby, to ensure the level of transparency in the area of alternative finance.[404] It underlines the necessity of registering the identities of owners of crypto assets, and clarifies the role of crypto assets in the financial system:[405]

> 'Member States shall ensure that providers of exchange services between virtual currencies and fiat currencies, and custodian wallet providers, are registered, that currency exchange and cheque cashing offices, and trust or company service providers are licensed or registered, and that providers of gambling services are regulated'.[406]

The Fifth AMLD elaborates the roles and duties of the Financial Intelligence Units (FIUs) in EU member states and the necessity of exchanging information within the EU. The FIUs are given unfettered access to relevant information held by EU member states, such as abnormal transactions. Identification of transaction parties, such as, bank account holders and payment accounts, shall be recorded under the Regulation (EU) No 910/2014[407] and accessible on the

---

[401] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU [2018] OJ L156/43.

[402] ibid. arts. 1. (1) (c) and (2) (d). at pp. 53 - 54.

[403] ibid. art. 4. 1. at p. 73.

[404] ibid. recital. (8), at p. 44.

[405] ibid. recitals (9) and (10). at pp. 44 - 45.

[406] ibid. art. 1 (29). at p. 67.

[407] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L257/73. recital (17). at p. 75; Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU [2018] OJ L156/43. recital (53). at p. 52.

European Central Platform under the Directive (EU) 2017/1132.[408] The Fifth AMLD also requires EU member states to cooperate with FIUs and comply with due diligence measures.[409] Meanwhile, the Fifth AML Directive suggests to include the regulatory mechanism of virtual currencies in the first report and to be completed by 11 January 2022. The report shall include the 'empowerments to setup and maintain a central database registering users' identities and wallet addresses accessible to FIUs, as well as self-declaration forms for the use of virtual currency users'.[410] Besides, the Fifth AML Directive necessitates EU member states to standardise data formats and reporting mechanisms for data storing and reporting, [411] although it may take time to conform.

Apart from the data and information sharing within the EU, jurisdictions for crypto assets cases are another issue to clarify. Given the fact that crypto assets crimes usually take place internationally through the internet, either offenders or victims are likely outside the EU or in different EU countries. Illicit activities can be processed overseas totally or partially. For instance, in the case of USA v Shaun W. Bridges and Carl Mark Force [2015],[412] the two Federal agents stole crypto assets from a Dark Web – the Sill Road via unauthorised access and converted the illicit earnings to fiat currency on Japanese crypto assets exchanges. The involved user accounts were anonymous and multinational. The offenders were US residents and lived in the US, therefore, this case was prosecuted under Federal Laws in the US. On the contrary, a knocking down of a criminal organisation in Spain in 2017 for crypto asset money laundering involved wrongdoers from Spain, Colombia and Venezuela.[413] This has raised a question about the prosecution process and jurisdictions. There were no official case reports available publicly at the time of writing in terms of prosecution, court judgments, trials or

[408] Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law (codification) [2017] OJ L169/46. recital (25) at p. 49.

[409] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU [2018] OJ L156/43. recitals. (14) (17) (20) (22) (35) (37) and art. 1 (11). at pp. 45 - 47, 50 and 57.

[410] ibid. art. 1 (41). at pp. 71 - 72.

[411] ibid. recital (20). at p. 47.

[412] United States v Shaun W. Bridges and Carl Mark Force IV, Defendants [2015] No.3-15-70370 Cal.Rptr. 1 (N.D.Cal.) <https://www.justice.gov/usao-ndca/file/765686/download> accessed 10 November 2019.

[413] 'Cryptocurrency Laundering as a Service: Members of a Criminal Organisation Arrested in Spain | Europol' (n 122).

sentences as well as jurisdiction. Based on the online announcement of the arrest, I understand that these offenders breached the legal provisions of “selling prohibited goods”, “online stealing” and “money laundering” and may violate “computer misuse” and “data leaking”. Crypto assets were used as intermediation of illicit earning transactions and a channel of international money laundering in this case. The exchange platforms that executed those transactions should be liable for reporting and recordkeeping subject to national regulations of anti-money laundering. The offenders and victims, as well as the transaction intermediation, are all transnational in those crypto asset crimes. Therefore, a more harmonised anti-money laundering measures of crypto assets within and beyond the EU could assist in detection, investigation and prosecution of money laundering.

In sum, Anti-Money Regulation on crypto assets in the EU covers the most important applications of crypto assets businesses, such as exchange platforms and custody wallets providers. It also sets forth the requirements for recordkeeping and reporting. EU member states have implemented the Fifth AMLD into their national regulations by 10 January 2020. Although this is so far the only unified regulatory requirements across the EU in relation to crypto assets businesses, it has laid the foundation for curbing associated criminal motives.

# 7 Thesis Conclusions, Implications and Limitations

## 7.1 Thesis Conclusions

This thesis diagnoses several important issues in the current regulatory framework in the UK and EU. These issues bring out the inconsistencies in crypto assets regulations between the UK and other EU countries. It uncovers a lack of effectiveness in the regulations on crypto assets in the UK, including loopholes in the existing regulatory provisions. These loopholes in the legal system may bring difficulties in identifying legal liabilities of crypto assets at court, such as prosecution. The research finding of this thesis also draws attention to the impacts of the EU single market system on the regulatory perimeters of crypto assets in the UK. The research outcomes of the thesis may generate some significant impacts on the regulatory policies on crypto assets in the UK and EU.

The research outcomes pertain to the three research questions of the thesis. The analytical result of the current UK regulation shows that the newly finalised guide for regulatory perimeters in the UK is somewhat less effective and room for improvement exists. The lack of effectiveness is caused by its focuses on types of crypto assets rather than the types of business entities or business models of firms[414] (see Chapter 5 of this thesis). Given the rapid development of information technology and the increasing popularity of crypto assets products and services, the possibility of product types variation is high. Meanwhile, crypto assets businesses need to adjust product lines consistently to catch up with industrial developments and innovation under the pressure of market competition. The changing market environment could lead to a new regulatory problem that firms operate in both regulated and unregulated crypto assets products at the same time or switch from one to another. Besides, regulating the varying types of crypto assets, there lies a problem for the authorities to keep updating the regulated or unregulated crypto assets types as well as the regulatory frameworks. Under the current regulatory framework, the UK authorities must pay considerable attention to identify types of crypto assets and adjust their regulatory scheme following markets variation. This situation may incur uncertainty in devising long-term regulation.

In addition, the current regulation gives unclear instructions to market participants in terms of identifying product types and carrying out business compliance. For instance, the regulation of certain types of crypto assets constraints the flexibility of firm business models for facing

[414] FCA, 'Guidance on Cryptoassets Feedback and Final Guidance to CP 19/3' (n 35).

market variation and technology developments. Meanwhile, the complicated regulatory structure may also cause firms or individuals to misidentify the regulatory positions of the products and services that they are providing. From the point of view of crypto assets businesses, such misidentification may further affect firms' business promotion strategies and internal compliance measures. From the point of view of individuals, this misidentification may affect their investment outcomes. The complicated regulatory structure also makes firm management and compliance more costly. For example, recruiting qualified staff and providing relevant training. Consequently, both situations will deliver a negative impact on market integrity and consumer protection.

Furthermore, the analytical outcome brings to light three loopholes in the current legal framework in the UK regarding crypto asset regulation. The three loopholes are found in the secondary legislation, the RAO 2001[415] and the Perimeter Guidance Manual (PERG)[416] of the FCA, respectively. Both the RAO and the PERG are the core references of the crypto asset regulation in the UK (see the FCA's final guidance on crypto assets).[417] Two of the three loopholes are caused by the disparate regulations on crypto assets among EU member states and the single market system in the EU. Of which, one issue is the unregulated crypto asset products or services may be able to promote and operate as regulated businesses in the UK due to the EU single market system. Businesses that hold authorised business licences in EU member states are allowed to operate in the UK with lifted regulatory requirements,[418] although many unregulated activities are falling outside the current regulatory perimeters of the FCA and the Financial Services and Markets Act.[419] Another issue is the "carrying on regulated activities by way of business" of e-commerce for overseas businesses. It in principle shall apply to all overseas businesses and individuals carrying out commercial activities in the UK through the internet; however, the regulation has been lifted for EU member states under the single market system.[420] The other one of the three loopholes is the inconsistency in the definitions of specified investments under Regulation 76 of the RAO 2001.[421] Regulation 76 of the RAO

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

[416] FCA, 'The Perimeter Guidance Manual' (n 42).

[417] FCA, 'Guidance on Cryptoassets Feedback and Final Guidance to CP 19/3' (n 35).

[418] FCA, 'The Perimeter Guidance Manual' (n 42).

[419] The Financial Services and Markets Act 2000 c. 8. ss.19 and 23.

[420] FCA, 'The Perimeter Guidance Manual' (n 42). 2.9.18G.

[421] The Financial Services and Markets Act 2000 (Regulated Activities) Order 2001, SI 2001/544. reg. 76.

2001 gives identical definitions to the types of entities who carry out specified investments in two opposite provisions. This inconsistency causes conflict to not only crypto assets businesses but also all commercial activities that are involved in specified investments.

The analytical result of the EU regulation indicates an even more complicated situation due to the diverse opinions on crypto assets and regulatory structures amongst EU member states. Some EU countries, such as Germany and Malta have opened their doors to embrace financial innovation and seen financial inclusion a way to attract investors and start-ups, while other countries, including Spain and Ireland, hold alternative opinions on this cutting-edge technology. There are also some EU member states in a wait-and-see approach at the time of writing including Italy and France. The diverse opinions on crypto assets business regulations trigger the inconsistency in the regulatory framework within the EU. This inconsistent regulatory frameworks of crypto assets amongst the EU member states are now challenging the one passporting system across EU countries. Even though the Fifth Anti-Money Laundering Directive[422] unifies the requirements of due diligence measures within the EU on crypto assets businesses, including exchanges and custody wallet providers, other commercial activities of crypto assets have to be regulated under national Laws, accordingly. Other commercial activities include but are not limited to investment and initial coin offerings (ICOs). Therefore, banned crypto-assets businesses nationally in some EU countries may still be able to provide products and services from overseas through the internet.

Finally, this thesis identifies and classifies the applicable Laws and Acts to crypto assets crimes taking the UK as an example. Financial crimes are a global matter under the twin developments of information technology and the internet. Not only because it is taking place in many countries but also it has become cross-border activities. Financial technology (Fintech) products underpinned by information technologies, such as crypto assets and the DLT, provide an additional vehicle to criminals networking and allow anonymous transactions internationally. The new vehicle can simplify the processes of illicit transactions and assist in covering up the identities of offenders. Illicit transactions typically are internet-based cross-border activities, which include online stealing, selling prohibited goods on dark-webs and laundering illicit earnings. Therefore, those crypto assets crimes usually involve multiple

[422] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU [2018] OJ L156/43.

countries, either overseas victims or grouped international criminals.[423] Each country has its national Laws and Acts to combat against financial and other crimes. However, the participation of crypto assets complicates the processes of identifying, investigating and prosecuting financial crimes. Taking the UK as an example, this thesis breaks down the relevant illicit activities of crypto assets crimes and elaborates the underlying rationale. Nevertheless, the global involvement of crypto assets activities requests close coordination and cooperation between authorities and urges a broader mutual agreement for crypto assets crimes. This may include identifying jurisdiction and data sharing.

By way of preview, the current regulatory scheme of the UK presents a lack of effectiveness and it is complicated and costly to both enterprises and consumers. There is room for improvement. The EU regulations have established some unified requirements to the EU member states in terms of commercial activities of crypto assets. However, achieving a harmonised regulatory structure is still a long way away. Besides, the cross-border crypto asset violations request all countries (at least those global important economies) to reach a consensus on the matters of international Fintech crimes.

This thesis contributes to the literature in several aspects. First, the thesis discovers three loopholes as well as inconsistencies in the existing regulatory frameworks of crypto assets in the UK; second, the thesis identifies the potential issues in the EU regulation of crypto assets across member states due to unharmonised legal systems in respect to crypto asset crimes within the EU, such as prosecution jurisdiction and information sharing; third, the thesis classifies and clarifies the Laws and Acts applicable to Fintech financial crimes, particularly crypto assets. By addressing the three research questions, the thesis generates several research impacts that may aid values to the improvements of the current regulatory frameworks in the UK and the EU.

## 7.2 Research Implications

This thesis contributes to the literature with several important findings and implications in the area of financial regulation of Fintech development in the UK and EU markets. The discussion over the effects of the existing regulatory framework on firms' managerial costs and due diligence measures suggests that the regulatory agencies of the UK and EU request a more effective regulation and advanced technology. Meanwhile, international coordination and

[423] For example, an arrest in Oxford, UK in 2019 involved multiple countries and victims in Spain, Columbia, Germany and the UK. See discussion in Section 5.4 of this thesis.

cooperation are the key roles to combat financial crimes under the soaring Fintech and the popularity of the internet. The discovered loopholes and inconsistencies in the law provisions in the UK and some EU countries shall urge improvements in the existing regulatory frameworks and legal systems.

The first implication relates to the effectiveness of the current regulatory regime in the UK and the EU. The thesis critically analyses the legal provisions that have applied for crypto assets regulatory frameworks and their effects on regulatory perimeters, and further on market integrity and consumer protection. The UK authorities set two regulatory frameworks to regulate crypto assets related activities. The FCA regulates security tokens and e-money tokens under the RAO[424] and PREG[425] interpreted by the final guidance on crypto assets of the FCA[426] (crypto token in the guidance paper). Meanwhile, the FCA regulates money laundering activities under the MLR 2019[427] in accordance with the EU Fifth Anti-Money Laundering Directive.[428] The token regulation of the FCA applies to certain crypto assets products and services, whilst the majority of crypto assets products and service providers fall outside the regulatory perimeters of the FCA.[429] This regulatory scheme would increase the managerial costs of firms and expose consumers to risks. This is caused by the unclear criteria for identifying types of crypto assets. On the one hand, firms need to invest an extra amount of time and employ qualified staff to identify the regulatory positions of their crypto assets products and to carry out new compliance and due diligence measures. On the other hand, the ambiguous boundaries between regulated and unregulated crypto assets would perplex consumers when making decisions. This ambiguity can also cause incorrect marketing strategies of firms. Therefore, the authorities should work out a clearer definition and classification of crypto assets.

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

[425] FCA, 'The Perimeter Guidance Manual' (n 42).

[426] FCA, 'Guidance on Cryptoassets Feedback and Final Guidance to CP 19/3' (n 35).

[427] The Money Laundering and Terrorist Financing (Amendment) Regulations 2019, SI 2019/1511.

[428] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU [2018] OJ L156/43.

[429] The regulatory perimeters of the FCA applies to security tokens and e-money tokens, otherwise unregulated tokens, like Bitcoins are unregulated tokens.

In addition, a conflict may occur between the regulatory regime and firm compliance under the single market system. Crypto assets firms can register their business in EU countries that authorise e-money tokens or exchange tokens and then provide their products and services in the UK onsite or through the internet without authorisation under the single market system. Although all overseas businesses operating in the UK shall comply with the Carrying on Regulated Activities by Way of Business[430] in the UK, exemptions apply to EU firms. This situation may be improved after the transition period of Brexit on 31 December 2020 subject to the final EU withdrawal agreement. There are chances that the UK authorities decide to place more rigid regulation on EU firms.

Moreover, the loopholes in the current regulatory system cause concern over market integrity and consumer protection and may incur difficulties for court judgements. Firms in the UK can define crypto assets products either regulated or unregulated in terms of specified investment under Regulation 76 of the RAO.[431] Authorities should look into this inconsistency of the regulations and make appropriate adjustments, accordingly.

Furthermore, it is important for the UK and EU countries to maintain close coordination and cooperation to combat money laundering and other cross-broad illicit activities regardless of the Brexit. This may include a seamless information and data sharing scheme. Additionally, an activity authorised in one region may be charged as wrongdoing in another under the diverse regulatory regimes of crypto assets among European countries. Therefore, authorities shall clarify the jurisdiction for crypto assets cases.

## 7.3 Limitations and Further Development

Although this thesis has carried out a thorough review and analysis of crypto assets related literature, existing Laws and Regulations, as well as case studies, the research is restraint by limited journal publications and cases in the early stage of the Fintech products. The thesis references twenty primary legislation/Acts, thirty-seven secondary legislation/regulations and six cases and reviews twelve books, twenty-one journal articles, twenty-six official working papers and two conference and seminar speeches. The thesis also accesses information from thirty-three websites, such as Central Banks and International Regulatory agencies.

[430] The Financial Services and Markets Act 2000 (Carrying on Regulated Activities by Way of Business) (Amendment) Order 2018, SI 2018/394.

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

Of which, the journal articles are mainly the discussions and reviews of the technology underpinning crypto assets and the possibilities of a decentralise the financial system, as well as potential risks of cyberattacks (see the discussion in Chapter two of the thesis); the legal case studies of crypto assets are sparse, only two cases in the US and three cases in Europe are related to crypto assets and money laundering/financial crimes, while only the two cases in the US and one case in Germany have official judgements made public. The two US cases relate to financial crime and money laundering activities and the German case relates to regulations of financial instruments. Thus, the thesis refers to the two US cases as examples to discuss the Laws and Acts applicable to crypto assets related financial crimes and money laundering activities and discusses the German case to analyse the inconsistency in the regulatory system in Germany; although there are some books have mentioned crypto assets or money laundering, whilst only few provide the relevant information the thesis required.[432]

Additionally, the thesis experienced three stages of the legal system change in the UK during the time of writing. The three stages are the pre-stage of implementing the EU Fifth Anti-Money Laundering (5AML) Directive[433] before 10 January 2020, the post-stage of implementing the (5AML) Directive after 10 January 2020 and the EU Exit on 31 January 2020. During the three stages, the UK secondary legislation regarding the anti-money laundering regulation has two amendment versions, one is amended from the AML 2017[434] to AML 2019 (Amendment)[435] for implementing the EU (5AML) Directive and another one is amended from the AML to AML 2019 (EU Exit).[436] These regulatory amendments take place

[432] This is the most recent and relevant book that discusses the legal issues of the Blockchain and crypto - assets. The book listed some potential legal issues that mentioned in this thesis, for example, money laundering and data protection as well as jurisdictions, whereas does not provide analysis of the effectiveness of the existing regulatory frameworks and the classification of the crypto - assets in the UK discussed in this book is not up to date. Dean Armstrong QC, Dan Hyde and Sam Thomas (n 90).

[433] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU [2018] OJ L156/43.

[434] The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017/692.

[435] The Money Laundering and Terrorist Financing (Amendment) Regulations 2019, SI 2019/1511.

[436] The Money Laundering and Transfer of Funds (Information) (Amendment) (EU Exit) Regulations 2019, SI 2019/253.

only recently at the time of writing; thus, I am unable to provide in-depth discussions on the effectiveness of the new regulatory requirements and the reaction of the markets.

Despite the research limitations, the analysis of the legal frameworks and regulatory effectiveness of crypto assets carried out by the thesis can be extended in the future. The thesis creates an analytical framework that assists to identify other issues in the legal systems and develop the analytical scope when the market becomes more mature and there are more sources available for research. For example, analysing specific legal provisions on crypto assets crimes in the UK. These may include how the Computer Misuse Act 1990 could affect the motives of to crypto assets crimes[437] and if the Forgery and Counterfeiting Act 1981 can reduce the possibilities of fabricating ICOs.[438] Another development could include if the Data Protection Act 2018 covers the user rights of crypto assets effectively.[439]

Moreover, the diverse regulatory frameworks of crypto assets among EU countries takes the research to an international comparison (see the discussion in Chapter Six, Regulation of crypto assets in the EU). The EU Fifth AML Directive shall demonstrate its impact on crypto assets exchanges and custody wallets providers in the following years and reveal the capabilities of competent authorities in EU member states on anti-money laundering regulations. The Fifth AML Directive may affect the crypto assets businesses differently under the diverse regulatory regimes of crypto assets across EU member states. Therefore, the effectiveness of the Fifth AML Directive shall vary across the EU countries.

Furthermore, the impact of the Brexit on the EU crypto assets businesses operating in the UK and the on the EU anti-money laundering regulation may raise additional issues in the legal system. Effective coordination and cooperation between the UK and the EU regarding crypto asset financial crimes would be essential in the future, such as Law enforcement and data sharing and jurisdiction.

[437] Computer Misuse Act 1990 c. 18.

[438] Forgery and Counterfeiting Act 1981 c. 45.

[439] Data Protection Act 2018 c.12.

# Bibliography

## Acts


1. Act on the Prudential Supervision of Payment Services (Payment Services Supervision Act) 2009
2. Banking Act (KWG) [2014] Bundesgesetzblatt
3. Computer Misuse Act 1990
4. Criminal Law Act 1977
5. Data Protection Act 2018
6. Details of Screening for New Registration Application as Virtual Currency Exchange Service Provider 2017
7. Drug Trafficking Offences Act 1986 c. 32
8. Electronic Money Regulations 2011, SI 2011/99
9. Forgery and Counterfeiting Act 1981
10. Payment Services Regulations 2017, SI 2017/752
11. Police and Justice Act 2006
12. Proceeds of Crime Act 2002
13. Sanctions and Anti-Money Laundering Act 2018 c. 13
14. Serious Crime Act 2007
15. The Financial Services and Markets Act 2000
16. The Innovative Technology Arrangements and Services Act 2018
17. The Malta Digital Innovation Authority Act 2018
18. The Virtual Financial Assets Act 2018
19. Theft Act 1968
20. Terrorism Act 2000

## Regulations


1. Directives 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on Markets in Financial Instruments and Amending Directive 2002/92/EC and Directive 2011/61/EU' [2014] OJ L 173/349.

2. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L337/35.

3. Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council and Commission Directive 2006/70/EC [2015] OJ L141/73.

4. Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law (codification) [2017] OJ L169/46.

5. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU [2018] OJ L156/43.

6. Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC [2009] OJ L267/7.

7. European Commission, 'The European Single Market | Internal Market, Industry, Entrepreneurship and SMEs'<https://ec.europa.eu/growth/single-market_en> accessed 5 November 2019.

8. European Commission, 'Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions' (2013).

9. FCA, ‘Payment Services and Electronic Money – Our Approach The FCA’s Role under the Payment Services Regulations 2017 and the Electronic Money Regulations 2011’.

10. FCA, ‘Money Laundering and Terrorist Financing Risks in the E-Money Sector’ (2018).

11. FCA, ‘CP19/3: Guidance on Cryptoassets UK’ (2019).

12. FCA, ‘Guidance on Cryptoassets Feedback and Final Guidance to CP 19/3’ (2019) PS19/22.

13. FCA, ‘The Perimeter Guidance Manual’ (2019).

14. FCA, ‘The MiFID 2 Guide’ (2020).

15. FCA, ‘Banking: Conduct of Business Sourcebook’ (2020).

16. FCA, ‘The Senior Managers and Certification Regime: Guide for FCA Solo-Regulated Firms’ (2019).

17. FCA, ‘Principles for Businesses’ (2020).

18. FCA, ‘Recognised Investment Exchanges’ (2020).

19. Financial Services Agency, ‘Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism’ (2018).

20. FATF, ‘International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - The FATF Recommendations’ (2012).

21. FATF, ‘International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - The FATF Recommendations Update June 2019’ (2019).

22. Regulation (EU) No 596/2014 of The European Parliament and of the Council of 16 April 2014 on Market Abuse (Market Abuse Regulation) and Repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 200’ [2014] OJ L173/1.

23. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L257/73.

24. U.S. Commodity Futures Trading Commission, ‘CFTC Designates TrueEX LLC as a Contract Market’ (2012).

25. U.S. Commodity Futures Trading Commission, ‘Keynote Address of Commissioner Brian Quintenz before the DC Blockchain Summit’ (2018).

26. Supervisory classification of tokens or cryptocurrencies underlying “initial coin offerings” (ICOs) as financial instruments in the field of securities supervision 2018 (Universitas Nusantara PGRI Kediri).

27. The Financial Services and Markets Act 2000 (Carrying on Regulated Activities by Way of Business) (Amendment) Order 2018, SI 2018/394.

28. The Financial Services and Markets Act 2000 (Regulated Activities) Order 2001, SI 2001/544.

29. The Financial Services and Markets Act 2000 (Market Abuse) Regulations 2014, SI 2014/3081.

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

31. The Money Laundering and Transfer of Funds (Information) (Amendment) (EU Exit) Regulations 2019, SI 2019/253.

32. The Money Laundering Regulations 2003, SI 2003/3075.

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

34. The Oversight of Professional Body Anti-Money Laundering and Counter Terrorist Financing Supervision Regulations 2017, SI 2017/1301.

35. The Privacy and Electronic Communications (EC Directive) Regulations 2003, SI 2003/2426.

36. The Proceeds of Crime Act 2002 (Crown Servants) Regulations 2003, SI 2003/173.

37. The Data Reporting Services Regulations 2017, SI 2017/699.

## Cases


1. ‘Citizen Service Berlin - Brandenburg - Criminality of Trade in Bitcoins’ (2019) <http://www.gerichtsentscheidungen.berlin-brandenburg.de/jportal/portal/t/279b/bs/10/page/sammlung.psml?pid=Dokumentanzeige&showdoccase=1&js_peid=Trefferliste&documentnumber=1&numberofresults=1&fromdoctodoc=yes&doc.id=KORE223872018&doc.part=L&doc.price=0.0> accessed 8 December 2019.

2. ‘Cryptocurrency IOTA: International Police Cooperation Arrests Suspect Behind10 Million EUR Theft | Europol’ <https://www.europol.europa.eu/newsroom/news/cryptocurrency-iota-international-police-cooperation-arrests-suspect-behind-10-million-eur-theft> accessed 15 October 2019.

3. ‘Cryptocurrency Laundering as a Service: Members of a Criminal Organisation Arrested in Spain | Europol’ <https://www.europol.europa.eu/newsroom/news/cryptocurrency-laundering-service-members-of-criminal-organisation-arrested-in-spain> accessed 15 June 2019.

4. United States v Matthew Jones [2014] No.6:14-mj-1233, So. 1 (M.D. Fla.) < https://www.justice.gov/sites/default/files/usao-mdfl/legacy/2014/05/30/20140530_Jones_Complaint.pdf > accessed 10 Oct 2019.

5. United States v Shaun W. Bridges and Carl Mark Force IV, Defendants [2015] No.3-15-70370 Cal.Rptr. 1 (N.D.Cal.) <https://www.justice.gov/usao-ndca/file/765686/download> accessed 10 November 2019.

6. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 [9th Cir. 2001].


## Books


1. Adam Smith, *The Wealth of Nations* (Bantam Classics 1776).

2. Alhosani W, *Anti-Money Laundering: A Comparative and Critical Analysis of the UK and UAE’s Financial Intelligence Units* (Palgrave Macmillan 2016).

3. Calvi J V. and Coleman SE, *American Law and Legal Systems* (Longman 2012).

4. Dean Armstrong QC, Dan Hyde and Sam Thomas, *Blockchain and Cryptocurrency: International Legal and Regulatory Challenges* (Bloomsbury Professional 2019).

5. Detlef Seese, Christof Weinhardt and Frank Schlottmann (eds), *Handbook on Information Technology in Finance.* (Springer-Verlag 2008).

6. Steven Dryall, 'Cryptocurrencies and Blockchain' in S. Chishti (ed.). *The WealthTech Book* (2020).

7. Murray A, *Information Technology Law: The Law and Society* (Oxford University Press 2016)

8. Murray A, *Information Technology Law: The Law and Society* (4th edn, Oxford University Press 2019).

9. Nicholas R, *Financial Crime in the 21st Century : Law and Policy* (6th edn, Edward Elgar 2011).

10. Sims A, Kariyawasam K and Mayes D, *Regulating Cryptocurrencies in New Zealand* (The Law Foundation New Zealand 2018).

11. Thomas H Davenport, *Process Innovation: Reengineering Work Through Information Technology* (Harvard Business School Press 1993).

12. Vandezande N and KU Leuven Centre for IT & IP Law, *Virtual Currencies : A Legal Framework* (Intersentia 2018).

### Journal Articles

1. Brand O, 'Conceptual Comparisons: Towards a Coherent Methodology of Comparative Legal Studies' [2007] Brook J Int'l L 405 – 466.

2. Brown SD, 'Cryptocurrency and Criminality' (2016) 89 The Police Journal: Theory, Practice and Principles 327 – 339.

3. Buocz T and others, 'Bitcoin and the GDPR: Allocating Responsibility in Distributed Networks' [2019] Computer Law and Security Review 1 – 17.

4. Forgang G, 'Money Laundering through Cryptocurrencies' [2019] Economic Crime Forensics Capstones 1 – 4.

5. Irwin ASM and Dawson C, 'Following the Cyber Money Trail: Global Challenges When Investigating Ransomware Attacks and How Regulation Can Help' (2019) 22 Journal of Money Laundering Control 110 – 131.

6. Li Y and others, 'Toward Privacy and Regulation in Blockchain-Based Cryptocurrencies' [2019] IEEE Network 1 – 7.

7. Nakamoto S, ‘Bitcoin: A Peer-to-Peer Electronic Cash System’ [2008] 1 – 9.

8. Nelken D, ‘Comparative Legal Research and Legal Culture: Facts, Approaches, and Values’ [2016] Annual Review of Law and Social Science 45 – 62.

9. Norton Rose Fulbright, ‘Deciphering Cryptocurrencies: A Global Legal and Regulatory Guide’ [2015] 1 – 20.

10. Reyes C, ‘Conceptualizing Cryptolaw’ (2017) 96 Nebraska Law Review 1 – 63.

11. Stern R, ‘Napster: A Walking Copyright Infringement?’ [2000] Micro Law 3 – 6.

12. Shih R and Ku R, ‘The Creative Destruction of Copyright: Napster and the New Economics of Digital’ (2002) 69 The University of Chicago Law Review 263 – 324.

13. Siems M and Deakin S, ‘Comparative Law and Finance: Past, Present, and Future Research’ [2010] Journal of Institutional and Theoretical Economics 120 – 140.

14. Tribbett D, ‘Method and System for Providing Access to Remotely Hosted Services through a Normalized Application Programming Interface’ [2012] United States Patent 1 – 9.

15. Walch A, ‘The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk’ (2015) 18 New York University Journal of Legislation & Public Policy 1 – 58.

16. Landes W and Lichtman D, ‘Indirect Liability for Copyright Infringement: Napster and Beyond’ (2003) 17 Journal of Economic Perspectives 113 – 124.

17. Seo J and others, ‘Money Laundering in the Bitcoin Network: Perspective of Mixing Services’, [2018] 2018 International Conference on Information and Communication Technology Convergence (ICTC) (IEEE) 1403-1405.

18. Treleaven P, ‘Financial Regulation of Fintech’ (2015) 3 Journal of Financial Perspectives 1 – 17.

19. Van Hoecke M, ‘Methodology of Comparative Legal Research’ [2016] Law and Method 279 – 310.

20. ‘Venezuela Petro Cryptocurrency (PTR)--English White Paper’ [2018] Gobierno Bolivariano de Venezuela.

21. Yanagawa N and Yamaoka H, 'Digital Innovation, Data Revolution and Central Bank Digital Currency' (2019) 19-E-2 1 – 20.

## Working Papers

1. Bank of England, 'Central Bank Digital Currency, Opportunities, Challenges and Design' (2020) < https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf>accessed 20 March 2020.

2. BaFin, '2018 Annual Report' (2018) <https://www.bafin.de/SharedDocs/Downloads/EN/Jahresbericht/dl_jb_2018_en.pdf?__blob=publicationFile&v=3> accessed 20 November 2019.

3. Barrdear J and Kumhof M, 'The Macroeconomics of Central Bank Issued Digital Currencies' (2016) Bank of England Staff Working Paper No. 605 < https://www.bankofengland.co.uk/-/media/boe/files/working-paper/2016/the-macroeconomics-of-central-bank-issued-digital-currencies > accessed 10 August 2019.

4. Basel Committee on Banking Supervision, 'Designing a Prudential Treatment for Crypto-Assets' (2019) < https://www.bis.org/bcbs/publ/d490.pdf > accessed 22 March 2020.

5. Bech M and Garratt R, 'Central bank cryptocurrencies' (2017) September BIS Quarterly Review 55 – 70. < https://www.bis.org/pub l/qtrpdf/r_qt1709f.pdf > accessed 14 February 2020.

6. BitFury Group and Jeff Garzik, 'Public versus Private Blockchains Part 1: Permissioned Blockchains White Paper' (2015) < https://bitfury.com/content/downloads/public-vs-private-pt1-1.pdf > accessed 5 January 2020.

7. Blandin A and others, 'Global Cryptoasset Regulatory Landscape Study' (2019) Cambridge Centre for Alternative Finance < https://www.jbs.cam.ac.uk/fileadmin /user_upload/research/centres/alternative-finance/downloads/2019-04-ccaf-global-crypto asset-regulatory-landscape-study.pdf > accessed 29 February 2020.

8. Blundell-Wignall A, 'The Bitcoin Question: Currency versus Trust-Less Transfer Technology' (2014) OECD Working Papers on Finance, Insurance and Private

Pensions, No. 37 < https://www.oecd.org/daf/fin/financial-markets/The-Bitcoin-Question-2014.pdf > accessed 27 September 2019.

9. Conesa C, 'Bitcoin: A Solution for Payment Systems or a Solution in Search of a Problem?' (2019) Banco de Espana Ocassional Paper No. 1901 < https://dx.doi.org/10.2139/ssrn.3333693 > accessed 22 May 2019.

10. CONSOB, 'Initial Coin Offerings and Crypto-Assets Exchanges Call for Evidence' (2019) < https://www.iosco.org/library/ico-statements/Italy%20-%20CONSOB%20-%2020190319%20-%20Initial%20Coin%20Offerings%20and%20Crypto%20Assets%20Exchanges%20Call%20for%20Evidence.pdf > accessed 27 March 2020.

11. HM Treasury, FCA and Bank of England, 'Cryptoassets Taskforce: Final Report' (2018) < https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf> accessed 20 December 2019.

12. EBA, 'Warning to Consumers on Virtual Currencies' (2013) < https://eba.europa.eu/sites/default/documents/files/documents/10180/598344/b99b0dd0-f253-47ee-82a5-c547e408948c/EBA%20Warning%20on%20Virtual%20Currencies.pdf?retry=1> accessed 20 December 2019.

13. EBA, 'EBA Opinion On "Virtual Currencies"' (2014) < https://eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/ EBA-Op-2014-08%20Opinion%20on%20Virtual%20Currencies.pdf?retry=1 > accessed 16 July 2019.

14. EBA, 'Report with Advice for the European Commission on Crypto-Assets' (2019) <https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf> accessed 16 July 2019.

15. ESMA, 'Advice Initial Coin Offerings and Crypto-Assets' (2019) <https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf> accessed 18 July 2019.

16. Federal Judicial Center, 'The U.S. Legal System: A Short Description' (2016) < https://ar.usembassy.gov/wp-content/uploads/sites/26/2016/03/U_S__Legal_System_English07 .pdf > accessed 20 June 2019.

17. FATF, ‘Guidance for A Risk-Based Approach, Virtual Currencies’ (2015) < https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf > accessed 14 February 2020.

18. FATF, ‘Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers’ (2019) <https://www.fatf-gafi.org/media/fatf/ documents/recommendations/RBA-VA-VASPs.pdf> accessed 14 February 2020.

19. Financial Centre Futures, ‘The Global Financial Centres Index 27’ (2020) < https://www.longfinance.net/media/documents/GFCI_27_Full_Report_2020.03.26_v1.1_.pdf> accessed 30 March 2020.

20. Gola C and Caponera A, ‘Policy Issues on Crypto-Assets’ (2019) Università Cattaneo Working Papers <https://pdfs.semanticscholar.org/416d/4613e504a52c11f6bad60a60e94 83e848158.pdf > accessed 14 November 2019.

21. Holloway C, ‘State of Illinois: Request for Information (RFI) Distributed Ledger and Blockchain Applications in the Public Sector’ (2017) < https://www2.illinois.gov/sites/doit/Documents/BlockchainInitiative/RFI+Blockchain+and+Distributed+Ledger+Applications+in+the+Public+Sector.pdf > accessed 5 January 2020.

22. Home Treasury, ‘Anti-Money Laundering Strategy’ (2004) < http://wgfacml.asa.gov.eg/en/doc_interest/doc_sais/0%20UK%20Treasury%20AML%20strategy.pdf> accessed 8 January 2020.

23. OECD, ‘How to Deal with Bitcoin and Other Cryptocurrencies in the System of National Accounts?’ (2018) < http://www.oecd.org/officialdocuments/publicdisplaydocum entpdf/?cote=COM/SDD/DAF(2018)1&docLanguage=En > accessed 10 August 2019.

24. OECD, ‘Initial Coin Offerings (ICOs) for SME Financing’ (2019) < https://www.oecd.org/finance/ICOs-for-SME-Financing.pdf > accessed 22 May 2019.

25. The Law Library of Congress, ‘Regulation of Cryptocurrency Around the World’ (2018) < https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf > accessed 23 April 2019.

26. The World Bank, 'Distributed Ledger Technology (DLT) and Blockchain: FinTech Note No.1' (2017) < https://openknowledge.worldbank.org/bitstream/handle/10986/29053/WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf?sequence=1&isAllowed=y> accessed 23 April 2019.

## Conferences and Seminars

1. Brainard L, 'Cryptocurrencies, Digital Currencies, and Distributed Ledger Technologies: What Are We Learning?', Decoding Digital Currency Conference Sponsored by the Federal Reserve Bank of San Francisco (2018). <https://www.federalreserve.gov/newsevents/speech/files/brainard20180515a.pdf> accessed 17 June 2019.

2. IMF, 'Private Crypto Assets and Central Bank Digital Currencies' (2018) < https://www.imf.org/en/News/Seminars/Conferences/2018/07/24/2018-seminar-on-law-and-financial-stability > accessed 15 January 2020.

## Websites

1. 'Alert on Initial Coin Offerings | Central Bank of Ireland' (2017) <https://centralbank.ie/consumer-hub/consumer-notices/alert-on-initial-coin-offerings>accessed30 October 2019.

2. AMF, 'Towards a New Regime for Crypto-Assets in France' (2019) <https://www.amf-france.org/en_US/Reglementation/Dossiers-thematiques/Fintech/Vers-un-nouveau-reg ime-pour-les-crypto-actifs-en-France> accessed 2 July 2019.

3. 'Announcement on Fraudulence of Issuing and Promoting Digital Fiat Currency in the Name of PBC | the People's Republic Bank of China' (2019) <http://www.pbc.gov.cn/en/3688110/3688181/3921119/index.html> accessed 3 March 2020.

4. 'Anti-Money Laundering Supervision: Guidance for High Value Dealers' (2018) <http://www.jmlsg.org.uk/industry-guidance/article/jmlsg-guidance-current> accessed 24 November 2019.

5. 'Alibaba, Tencent, Five Others To Receive First Chinese Government Cryptocurrency | Forbes' <https://www.forbes.com/sites/michaeldelcastillo/2019/08/27/alibaba-tencent-five-others-to-recieve-first-chinese-government-cryptocurrency/> accessed 3 March 2020.

6. ‘Alipay Account Service Agreement’ (2016) <https://render.alipay.com/ p/f/agreementpages/alipayaccountserviceagreement.html> accessed 9 April 2020.

7. ‘Applying EU Law | European Commission’ <https://ec.europa.eu/info/law/law-making-process/applying-eu-law_en> accessed 25 March 2020.

8. ‘BaFin - Virtual Currency’ <https://www.bafin.de/EN/Aufsicht/FinTech/VirtualCurrency/virtual_currency_node_en.html> accessed 16 July 2019.

9. ‘Cases of Money Laundering Linked to Cryptocurrency in Japan up Tenfold in 2018 | The Japan Times’ <https://www.japantimes.co.jp/news/2019/02/28/national/crime-legal/cases-money-laundering-linked-cryptocurrency-japan-tenfold-2018/#.XLBfGdVKjIU> accessed 12 April 2019.

10. ‘Central Bank Group to Assess Potential Cases for Central Bank Digital Currencies | Bank of England’ <https://www.bankofengland.co.uk/news/2020/january/central-banks-group-to-assess-digital-currencies?sf116286084=1> accessed 25 January 2020.

11. ‘Crypto-Activity: A Contribution For A National Regulatory Regime From Consob (Press Release January 2, 2020)’ <http://www.consob.it/web/consob/d ettaglio-news/-/asset_publisher/hZ774IBO5XPe/content/comunicato-stampa-del-2-gennaio-2020-hp/11973> accessed 3 January 2020.

12. ‘China Central Bank Close to Releasing Digital Currency: PBOC Official | CNBC’ <https://www.cnbc.com/2019/08/12/china-central-bank-close-to-releasing-digital-currency-pboc-official.html> accessed 3 March 2020.

13. ‘Consumer Warning on Virtual Currencies | Central Bank of Ireland’ (2018) <https://centralbank.ie/consumer-hub/consumer-notices/consumer-warning-on-virtual-currencies> accessed 30 October 2019.

14. ‘Cryptoassets | FCA’ <https://www.fca.org.uk/consumers/cryptoassets> accessed 13 May 2019.

15. ‘Digital Currencies | Bank of England’ <https://www.bankofenglandco.uk/research/digital-currencies> accessed 13 May 2019.

16. ‘Distributed Ledger Technology and Virtual Currencies - Central Bank of Malta’ <https://www.centralbankmalta.org/en/qqa-dlt-vcs> accessed 30 October 2019.

17. ‘EBA Warning and Opinion on Virtual Currencies | Central Bank of Ireland’ (2014) <https://centralbank.ie/consumer-hub/consumer-notices/eba-opinion-on-virtual-currencies> accessed 30 October 2019.

18. ‘Economic Performance by Country | European Commission’ <https://ec.europa.eu/info/business-economy-euro/economic-performance-and-forecasts/economic-performance-country_en> accessed 25 March 2020.

19. ‘FCA Becomes AML and CTF Supervisor of UK Cryptoasset Activities | FCA’ <https://www.fca.org.uk/news/news-stories/fca-becomes-aml-and-ctf-supervisor-uk-cryptoasset-activities> accessed 25 January 2020.

20. ‘Financial Services – EU Regulatory Framework for Crypto-Assets | European Commission’ <https://ec.europa.eu/info/law/better-regulation/initiatives/crypto-assets-2019/public-consultation_en> accessed 22 January 2020.

21. ‘Financial Services – EU Regulatory Framework for Crypto-Assets | European Commission’ <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12089-Directive-regulation-establishing-a-European-framework-for-markets-in-crypto-assets/public-consultation> accessed 22 January 2020.

22. ‘RegTech | FCA’ (2017) <https://www.fca.org.uk/firms/innovation/regtech> accessed 26 March 2020.

23. ‘Germany: Court Holds That Bitcoin Trading Does Not Require a Banking License | Global Legal Monitor’ <https://www.loc.gov/law/foreign-news/article/germany-court-holds-that-bitcoin-trading-does-not-require-a-banking-license/> accessed 8 December 2019.

24. ‘Global Law Enforcement Action against Vendors and Buyers on the Dark Web | Europol’ <https://www.europol.europa.eu/newsroom/news/global-law-enforcement-action-against-vendors-and-buyers-dark-web> accessed 10 November 2019.

25. ‘Italian CONSOB: Two Registers for Managing Crypto Assets - The Cryptonomist’ <https://en.cryptonomist.ch/2020/01/02/italian-consob-registers-for-crypto-assets/> accessed 3 January 2020.

26. ‘NPA Cryptocurrency Tips Point to 669 Suspected Money-Laundering Cases from April to December | The Japan Times’ <https://www.japantimes.co.jp/news/2018/02/22/business/npa-cryptocurrency-tips-point-669-suspected-money-laundering-cases-april-december/#.XK8r3dVKjIU> accessed 11 April 2019.

27. ‘PACTE, the Action Plan for Business Growth and Transformation in France | Gouvernement.Fr’ <https://www.gouvernement.fr/en/pacte-the-action-plan-for-business-growth-and-transformation> accessed 2 January 2020.

28. ‘Proceeds Of Crime Act 2002 Part 7 - Money Laundering Offences | The Crown Prosecution Service’ <https://www.cps.gov.uk/legal-guidance/proceeds-crime-act-2002-part-7-money-laundering-offences> accessed 3 February 2020.

29. ‘PayPal User Agreement’ (2019) <https://www.paypal.com/uk/webapps/mpp/ua/useragreement-full> accessed 9 April 2020.

30. The Crown Prosecution Service, ‘Cybercrime - Prosecution Guidance’ <https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance>accessed 23 April 2019.

31. ‘Types of EU Law | European Commission’ <https://ec.europa.eu/info/law/law-making-process/types-eu-law_en> accessed 5 November 2019.

32. ‘Virtual Currency Businesses | Department of Financial Services’ <https://www.dfs.ny.gov/apps_and_licensing/virtual_currency_businesses> accessed 21 May 2019

33. ‘What Is China’s Digital Currency Plan? | Financial Times’ <https://www.ft.com/content/e3f9c3c2-0aaf-11ea-bb52-34c8d9dc6d84> accessed 3 March 2020.