Regulation of Cryptocurrencies:

A Reflexive Law Approach

by

Immaculate Dadiso Motsi

BA (Hons), Master of Public Policy (MPP), Master of Laws (LLM)

Supervisors

Prof Dalvinder Singh and Prof Ralf Rogowski

A thesis submitted for the degree of Doctor of Philosophy in Law

University of Warwick, School of Law

March 2020

Table of Contents

Lists of Figures and Tables

Acknowledgements

"I thank thee, and praise thee, O thou God of my fathers, who hast given me wisdom and might, and hast made known unto me now what we desired of thee." Daniel 2:3

I would like to acknowledge Professor Francis Charles Adams (1952 – 2016), who introduced me to Financial Regulation as a Masters Student at the Lee Kuan Yew School of Public Policy, National University of Singapore. Your excellent teaching, support and encouragement gave me the knowledge and confidence I needed to explore and pursue my research interests in this area.

I would also like to thank Professor Dalvinder Singh, who nurtured this interest during my LLM at Warwick Law School and subsequently agreed to supervise my PhD thesis in cryptocurrency regulation. I am grateful for his patience and guidance throughout this process. I am also grateful to Prof Ralf Rogowski, my second PhD supervisor, who explained the esoteric with clarity, and kept me from losing my way throughout my PhD process. I would also like to acknowledge Dr Giuliano Castellano, for supervising my Master's Dissertation on Bitcoin Regulation with compassion and enthusiasm.

I would like to thank the University of Warwick, School of Law, for its 'law in context' orientation that allowed me to benefit from an excellent LLM programme in Corporate Governance and Financial Regulation and for subsequently granting me a Research Scholarship to pursue my PhD.

Finally, I would like to acknowledge Satoshi Nakamoto for his/her/their seminal work, and the global cryptocurrency and blockchain community, for being a constant source of inspiration on social media (#cryptotwitter, #HODL), and at the various formal and informal events I have had the privilege of attending throughout the past six years.

Dedication

I dedicate this thesis to the Three Kings of my life. To my wonderful husband Kingsley Omoijiade (could not have done this without your support and encouragement) and to our beautiful boys, Joshua and Axel (no achievement could ever match the days you were born, and no title before my name could ever compare to that of 'mummy').

Declaration

This thesis is submitted to the University of Warwick in support of my application for the degree of Doctor of Philosophy. It has been composed by me and has not been submitted in any previous application for any degree.

Abstract

This thesis presents a reflexive law approach to the regulation of cryptocurrencies. Cryptocurrencies are a form of digital or virtual currency generated, exchanged and distributed exclusively online. Whilst there are legitimate uses for cryptocurrencies, and there is considerable interest in their innovative potential in the financial sector and beyond, their use in facilitating illegal activities combined with the risks they pose to consumers and investors warrants their regulation. Current cryptocurrency regulation consists of recommendations, warnings, opinions, and statements of international organisations, whose mandates and purview include and intersect with the issues of regulatory concern raised by cryptocurrencies. It also consists of disparate national approaches, which this thesis has classified into jurisdictions with (a) no regulation, (b) restrictive regulations, (c) neutral regulation, and (d) promotive regulations. However, the inherent technical features of cryptocurrencies present specific challenges to this current regulatory framework, in the areas of enforcement and compliance. This thesis argues that a reflexive regulation approach—in which the law acts at a subsystem-specific level to install, correct, and redefine democratic self-regulatory mechanisms—is best suited to contending with the issues of regulatory concern presented by cryptocurrencies, whilst addressing the shortcomings and limitations of current cryptocurrency regulation. This thesis provides strategies for a reflexive regulation approach to cryptocurrencies, developed through the identification of the internal self-regulatory mechanisms of the cryptocurrency system. Identifying these as computer code and consensus-based distributive governance mechanisms respectively, this thesis concludes by providing recommendations aimed at redirecting these internal self-regulatory mechanisms towards achieving regulatory goals. In this way, this thesis draws from the theory of reflexive regulation as presented by Gunther Teubner, in order to provide both a substantive and jurisprudential perspective on the regulation of cryptocurrencies.

List of Abbreviations

AML	Anti-Money Laundering
BOE	Bank of England
BTC	Unit of Bitcoin (also denominated in lower case bitcoin)
CDD	Customer Due Diligence
CFT	Countering the Financing of Terrorism
CFPB	United States Consumer Financial Protection Bureau
CFTC	Commodity Futures Trading Commission
DAO	Decentralised Autonomous Organisation
DLT	Distributed Ledger Technology
EBA	European Banking Authority
ESMA	European Securities and Markets Authority
FATF	Financial Action Task Force
FCA	Financial Conduct Authority (United Kingdom)
FinCen	Financial Crimes Enforcement Network (US Treasury)
Fintech	Financial Technology
FINTRAC	Financial Transactions and Reports Analysis Center of Canada
HMRC	Her Majesty's Revenue and Customs
ICO	Initial Coin Offering
IOSCO	International Organisation of Securities Commissions
KYC	Know Your Customer (requirements)
MAS	Monetary Authority of Singapore
MSB	Money Services Business
NYDFS	New York Department of Financial Services
P2P	Peer-to-Peer
PoW	Proof of Work Consensus Algorithm
Regtech	Regulatory Technology
SAR	Suspicious Activities Reporting
SEC	US Securities and Exchange Commission
Suptech	Supervisory Technology

Introduction

In October 2008, Satoshi Nakamoto published a white paper entitled 'Bitcoin: A Peer-to-Peer Electronic Cash System'.[1] Circulated at the height of the Global Financial Crisis (GFC), where a severe economic crisis was occurring in a climate of extreme distrust and disillusionment with the global banking system, Nakamoto's paper sought to address the inherent weaknesses of the trust-based model for commerce on the internet, which relied exclusively on financial institutions serving as trusted third parties in the processing of electronic payments. Nakamoto's paper proposed an alternative to this system, providing the blueprint for 'an electronic payment system based on cryptographic proof instead of trust'.[2] This, and the accompanying open source software released a year later, was the birth of Bitcoin, the first of what are now known as cryptocurrencies. Cryptocurrencies are a form of digital or virtual currency generated and distributed exclusively online, that 'rely on a cryptographic protocol to regulate the manner in which (and the extent to which) currency can be created and/or exchanged'.[3]

Early academic research into cryptocurrencies immediately identified the duality of cryptocurrencies, which can be seen as both a 'regulatory nightmare' and a 'libertarian dream'.[4] This is because whilst cryptocurrencies present an exciting and innovative alternative to conducting commerce over the internet, providing benefits such as privacy, cost reduction and the ability to 'make non-reversible payments for non-reversible services',[5] cryptocurrencies also present considerable challenges to regulatory and law enforcement agencies. These challenges primarily have to do with the manner in which cryptocurrencies are able to operate beyond the reach of the law, due to technical design features such

[1] S Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (*Bitcoin.org* 2009) <https://bitcoin.org/bitcoin.pdf> Accessed 27 May 2018.
[2] ibid 1.
[3] P De Filippi, 'Bitcoin: A Regulatory Nightmare or a Libertarian Dream' (2014) 3 Internet Policy Review 2.
[4] ibid.
[5] Nakamoto (n 1) 1.

as operating over a global, distributed, peer-to-peer (P2P) network, and the ability to obscure the location and identities of parties to transactions.[6]

This thesis is aimed at considering the regulation of cryptocurrencies, in light of not only the challenges but the also the opportunities presented by the innovative features of cryptocurrencies to regulatory authorities, and to the legal system more broadly. With this in mind, this thesis draws on the theory of reflexive regulation as presented by Gunther Teubner, in order to consider cryptocurrency regulation from both a substantive and jurisprudential perspective. Reflexive regulation envisages a role for the law in which,

> *law must act at the subsystem-specific level to install, correct, and redefine democratic self-regulatory mechanisms. Law's role is to decide about decisions, regulate regulations, and establish structural premises for future decisions in terms of organization, procedure and competences.*[7]

This thesis will show how a reflexive regulation approach is well-suited to both addressing the regulatory challenges, and exploring the regulatory opportunities presented by the advent of cryptocurrencies. This presentation of a reflexive law approach to cryptocurrency regulation will be structured around layered responses to six questions, namely:

1) What are cryptocurrencies and why do they need to be regulated?
2) What is the current approach to cryptocurrency regulation?
3) Why is there a need for an alternative approach to cryptocurrencies?
4) What is reflexive regulation?
5) How can reflexive regulation be applied to cryptocurrencies?
6) What are the strategies for reflexively regulating cryptocurrencies?

[6] Nakamoto (n 1); the definitions of these and other technical terms will be elaborated on in Chapter 1.

[7] G Teubner, 'Substantive and Reflexive Elements in Modern Law (1983) 17 Law & Soc Rev 239, 275.

Structure of Thesis

This thesis will therefore consist of six chapters, each aimed at addressing each of the six questions stated above, as follows:

What are cryptocurrencies and why do they need to be regulated?

Chapter 1 will provide an introduction and overview of cryptocurrencies in order to lay the contextual foundation for the thesis, prior to considering their regulation. Taking an evolutionary perspective to the advent of cryptocurrencies, this chapter will describe the history and development of cryptocurrencies, starting with the emergence of alternative currency and the emergence of Blockchain and Distributed Ledger Technology. The chapter will then highlight the complexity of cryptocurrencies by describing the multiplayer ecosystem in which they operate, including miners, developers and the various cryptocurrency financial intermediaries. This will be followed by a description of the issues of regulatory concern raised by cryptocurrencies, in order to gain an understanding of the motivation and rationale for their regulation. The chapter will then conclude by discussing the key insights from this consideration of what cryptocurrencies are, how they operate, and why they need to be regulated.

What is the current approach to cryptocurrency regulation?

Chapter 2 of this thesis will analyse the current means of regulating cryptocurrencies, prior to an evaluation and analysis of this existing regulatory framework. With this in mind, the chapter will present an overview of international and regional regulatory responses to cryptocurrencies. The organisations to be included in this analysis are the International Monetary Fund (IMF), the G20 and the Financial Stability Board (FSB), the Organisation for Economic Co-Operation and Development (OECD) the Financial Action Task Force (FATF), the Bank of International Settlements (BIS), International Organisation of Securities Commission (IOSCO), and the various organisations within the European Union (EU). This will be followed by an overview of national regulatory responses to cryptocurrencies. This section will categorise regulations as having either no regulation, or restrictive, neutral or promotive jurisdictions. The chapter will then provide some concluding remarks on current cryptocurrency regulation.

Why is there a need for a different approach to regulation?

Chapter 3 will provide some critical insight showing the shortcomings of current cryptocurrency regulation, in order to display why there is a need for an alternative regulatory approach. This will be done firstly by discussing the enforcement challenges regulators face when existing substantive laws are applied to cryptocurrencies. Thereafter, the chapter will discuss the compliance challenges faced by the cryptocurrency industry when seeking to adhere to existing regulations. Chapter 3 will conclude by discussing the need for an alternative approach to cryptocurrency regulation, with an emphasis on what such an approach must be able to address in order to be fit for purpose.

What is reflexive regulation?

The aim of **Chapter 4** is to present the theoretical foundation for an alternative approach to cryptocurrency regulation based on the theory of reflexive regulation. This will be done by first providing an overview of the key components of reflexive regulation theory, as initially presented by Gunther Teubner. This will be followed by a consideration of where reflexive regulation stands in the spectrum of established regulatory theories and strategies with a particular focus on the differences between reflexive regulation and other self-regulation-based theoretical approaches. The chapter will conclude by discussing the rationale and merits of taking a reflexive law approach to the regulation of cryptocurrencies.

How can reflexive regulation be applied to cryptocurrency?

Chapter 5 will present the main mechanisms through which cryptocurrency systems self-regulate and self-govern. This is a necessary pre-cursor to the core component of reflexive regulation, which is the redirection of internal self-regulatory mechanisms towards regulatory goals. With this in mind, the chapter will identify the two main internal governance mechanisms within cryptocurrency system as ‘Code’ and ‘Consensus’. These mechanisms are described and analysed in turn, with a focus on their operational closure (functionality) and cognitive openness (regulability). This will be done with an emphasis on highlighting not only the avenues and means for legal intervention within these internal governance structures, but also identifying the role of law and legal intervention in ameliorating these self-regulatory mechanisms, in order to address the issues of regulatory concern related to cryptocurrencies.

What are the strategies for regulating cryptocurrencies reflexively?

Chapter 6 will conclude the thesis, by providing strategies for the reflexive regulation of cryptocurrencies, based on observations on the structure and self-regulatory mechanisms of the cryptocurrency system made in the preceding chapters. Here, the focus will be on recommendations stemming from the use of code and consensus as internal self-regulatory mechanisms within the cryptocurrency system. Further expanding on previous chapters, these recommendations will be made in light of the identified issues of regulatory concern, in recognition of the highlighted regulatory gaps and fissures present in current cryptocurrency regulation.

In this way, this thesis will present a reflexive law approach to cryptocurrency regulation that begins with assessing current approaches, starting with understanding the nature of cryptocurrencies and what makes them distinctive, and assessing their relevant regulatory concerns.

Chapter One: Overview of Cryptocurrencies

1.1 Introduction

This chapter will provide an introduction and overview of cryptocurrencies in order to lay the contextual foundation for the thesis, prior to considering their regulation. Taking an evolutionary perspective to the advent of cryptocurrencies, the chapter begins by describing their history and development starting with the emergence of alternative currency and the emergence of blockchain and Distributed Ledger Technology (DLT). The chapter will then proceed to highlight the complexity of cryptocurrencies by describing the multi-player ecosystem in which they operate including miners, developers and the various cryptocurrency financial intermediaries. This will be followed by highlighting the issues of regulatory concern raised by cryptocurrencies in order to gain an understanding of the motivation and rationale for their regulation. The chapter will then conclude by discussing the key insights from this consideration of what cryptocurrencies are, how they operate and why they need to be regulated.

1.2 History and Development

1.2.1 Emergence of Alternative Currency

The first step in the evolution of cryptocurrencies was the introduction of the notion of alternative currency. Alternative currencies, which are unconventional 'objects of monetary value',[1] are the earliest conceptual iterations of what have now evolved into cryptocurrencies. Alternative currency can come in the form of global and local community currencies; examples of local community alternative currencies within the United Kingdom (UK) are Transition Town Pounds, Time Banks and Local Exchange Trading Systems (LETS)[2]. These were designed for

[1] Parliamentary Office of Science and Technology, 'Alternative Currencies' (POSTnote Number 475 August 2014) <http://researchbriefings.files.parliament.uk/documents/POST-PN-475/POST-PN-475.pdf> Accessed 7 June 2016.
[2] ibid.

specific purposes, such as the regeneration of local areas, addressing social exclusion and the addition of value to unpaid work. Examples of Transition Town Pounds are the Totnes[3] and Brixton Pounds, which are paper notes with legal status equivalent to a retail voucher, with restrictions to a particular geographical community.[4] However, the majority of alternative currencies are of a more global and universal nature, and include items such as tokens, loyalty schemes, credits, or points earned in games and virtual or online worlds. The latter are early examples of Virtual Currency (VC), which mainly have restricted in-game use as units of value in online or virtual gaming communities. In this way, VC is 'a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community'.[5] Often used synonymously, Digital Currency (DC) is 'a privately issued code or serial number representing value that is circulated online'.[6]

Early VC and DCs had a central managing authority usually in the form of a game developer, who 'directly or through software managed the issuance, storage and redemption of the in-game currency and who may have validated, tracked and recorded transactions'.[7] Examples of these operating in 2012 are Arena Net's Guild Wars 2, Iceland's CCP Games, and Valve Corporation, which aimed to create a shared currency across two virtual environments.[8] Second Life and its Linden Dollar is another example of a closed virtual community with its own VC. Launched in 2013 by Linden Labs, Second Life is an online world that allows real

[3] The Totnes Transition Town Pounds experiment ended in March 2019, citing a decline of use partly due to an increasingly cashless economy. For further details, see <https://www.transitiontowntotnes.org/2019/03/totnes-pound-celebration/>

[4] Parliamentary Office of Science and Technology (n 1).

[5] European Central Bank, 'Virtual Currency Schemes' (*ECB*, 2012) <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> Accessed 7 June 2016.

[6] P Mullan, *The Digital Currency Challenge: Shaping Online Payment Systems through US Financial Regulations* (Palgrave Macmillan 2014) 4.

[7] M Berta and W Noonan, 'The Property-contract Duality of Bitcoin' (*Financier Worldwide Expert Briefing,* June 2015) < https://www.financierworldwide.com/the-property-contract-duality-of-bitcoin#.XeUdyNXgqUk> Accessed 7 June 2016.

[8] P Gross, 'A History of Virtual Currency: Why Bitcoins Shouldn't Surprise You' (*CFA Institute,* 2014) <https://annual.cfainstitute.org/2014/01/10/a-history-of-virtual-currency-why-bitcoins-shouldnt-surprise-you/> Accessed 7 June 2016.

life purchases in the game through Linden Dollars. Although now in decline,[9] Second Life's Linden-based economy was highly liquid, even 'producing its own millionaire, Anshe Chung, who made a very real fortune from buying and selling property that existed only on Second Life servers'.[10] This ability to have bi-directional flows of value between virtual and 'real' worlds led to an extension of the use of VCs, beyond the gaming world into the everyday economy, mostly as a way to launder the proceeds of criminal activity. An example of this is Liberty Reserve, an online bank that converted local currencies to Liberty Reserve Dollars.[11] More recent examples of post-gaming VCs include the now defunct Facebook Credits facility and Amazon Coins,[12] which sought to use their own platform-specific virtual currency to facilitate transactions on their websites.[13] The concept and functionality of digital and virtual currencies was incorporated and augmented by the introduction of cryptocurrencies. Cryptocurrencies are 'digital currencies that rely on a cryptographic protocol to regulate the manner in which (and the extent to which) currency can be created and/or exchanged'.[14] The evolutionary leap that distinguishes cryptocurrency from VC and DC is the use of peer-to-peer networking[15] and cryptography,[16] to maintain the integrity of

[9] According to the New World Notes blog, Second Life has about 60,000 premium subscribers in 2019, up by 3000 from 2017 low point, but still below 2012's peak of 70,000, see <https://nwn.blogs.com/nwn/2019/05/sl-premium-subscriptions-linden-lab-tyche.html > Accessed 2 December 2019.

[10] B Collins, 'Whatever Happened to Second Life?" (*Alphr*, 4 January 2010) <http://www.alphr.com/features/354457/whatever-happened-to-second-life> Accessed 7 June 2016.

[11] Gross (n 8).

[12] R Satran, '6 Virtual Currencies That Went Bust' (*US News*, 13 May 2013) <http://money.usnews.com/money/personal-finance/slideshows/6-virtual-currencies-that-went-bust/9> Accessed 7 June 2016.

[13] These two initiatives preceded Facebook's Libra cryptocurrency initiative and Amazon's blockchain activities. For more details on both projects, see <https://www.ccn.com/facebook-amazon-libra-threat/> Accessed 2 December 2019.

[14] P De Filippi, 'Bitcoin: A Regulatory Nightmare to a Libertarian Dream' (2014) 3(2) Internet Policy Review 1,1.

[15] As explained by techterms, "in a P2P network, the "peers" are computer systems that are connected to each other via the Internet. Files can be shared directly between systems on the network without the need of a central server."<https://techterms.com/definition/p2p> Accessed 2 December 2019.

[16] Cryptography is a "method of protecting information and communications through the use of codes so that only those for whom the information is intended can read and process it". <https://searchsecurity.techtarget.com/definition/cryptography> Accessed 2 December 2019.

a technologically sophisticated system underpinned by blockchain and Distributed Ledger Technology (DLT).

1.2.2 Emergence of Blockchain and DLT

The second significant concept necessary to understand cryptocurrencies, after that of VC and DC, is that of ledgers. Used in bookkeeping and accounting, ledgers have been a part of the earliest banking systems as a means to facilitate payments. For example, when goldsmith banks emerged in the 16th century, 'they kept ledgers of their customers' deposits which enabled payments to be made by making changes in the ledgers rather than physically exchanging the assets'.[17] This ledger-keeping function of banks was made universal by the introduction of central banks to settle interbank obligations and maintain confidence in the convertibility of bank liabilities into cash at par.[18]

Blockchain—the technical backbone of cryptocurrencies—is a secure ledger of transactions shared by all parties in a distributed network. Every transaction on a blockchain is recorded and stored to create an immutable (unchangeable) and auditable log of transactions. This shared log of transactions is partly what enables cryptocurrencies to function without the need of a trusted third party or intermediary, such as a bank, to verify transactions. Whilst the terms 'blockchain' and 'DLT' are often used interchangeably,[19] blockchain is widely viewed as a category or sub-set of DLT.[20] This is because, as shall be further discussed below, blockchain is a form of distributed ledger that has the additional functionality of

[17] R Ali, J Barrdear, R Clews and J Southgate, 'Innovations in Payment Technologies and the Emergence of Digital Currencies' (*Bank of England* 2014) <http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3digitalcurrenciesbitcoin1.pdf> Accessed 20 June 2018.

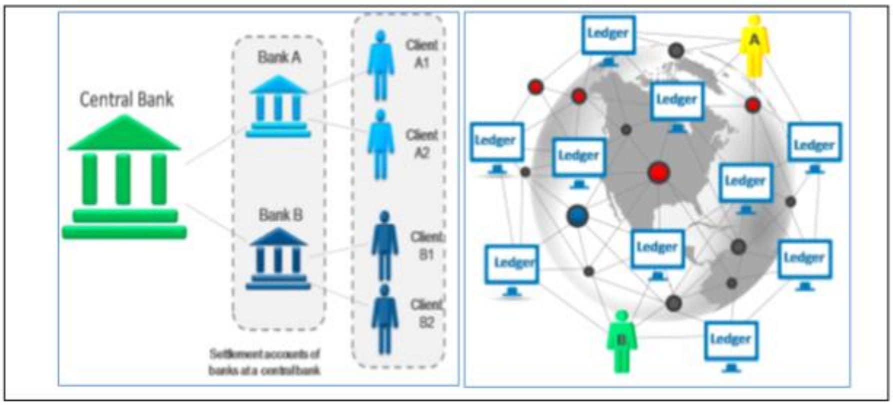
[18] S Dow, 'Central Banking in the Twenty-First Century' (2017) 41 Cambridge Journal of Economics, 1539, 1557.

[19] JP Morgan, 'Decrypting Cryptocurrencies: Technology, Application and Challenges' (*JP Morgan Perspectives,* 9 February 2018) <http://forum.gipsyteam.ru/index.php?act=attach&type=post&id=566108> Accessed 20 June 2018.

[20] World Bank, 'Blockchain and Distributed Ledger Technology' (*World Bank* 2018) <https://www.worldbank.org/en/topic/financialsector/brief/blockchain-dlt> Accessed 20 June 2018.

cryptographically linking data into 'blocks' which form a sequential tamperproof chain. As illustrated in Figure 1 below, the innovation presented by DLT is based on its difference from centralised payments. In a centralised payment system, when client A1 wants to make a payment to client B1, money is deducted from A1's account to bank A, and thereafter the central bank moves money from bank A's settlement account to bank B, which then adds money to client B1's account. Here, the central bank maintains a ledger of interbank transactions, validating transactions and safeguarding against double spending and counterfeit.[21]

Figure 1: Centralised Payment Systems Compared to Distributed Payment Systems



Source: (IMF)[22]

However, with DLT, copies of transaction records (ledgers) are kept in multiple computers on the network, visible to everyone. As shall further be explained below, transactions are settled by a multiple of individual nodes (miners) who solve cryptographic puzzles and are rewarded through cryptocurrency.[23] The illustration of a distributed ledger system (Figure 1) shows how payment from A

[21] M Walport, 'Distributed Ledger Technology: Beyond Blockchain' (*Government Office for Science,* 2016) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf> Accessed 20 June 2018.

[22] A Adriano and H Monroe, 'The Internet of Trust' (*IMF Finance and Development* June 2016) <https://www.imf.org/external/pubs/ft/fandd/2016/06/adriano.htm> Accessed 20 June 2018.

[23] International Monetary Fund, *Virtual Currencies and Beyond: Initial Considerations*. (*IMF Staff Discussion Note*, 16/03) <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf> Accessed 20 June 2018.

to B over a blockchain network is not subject to authorisation and monitoring by a central authority, and not restricted to any geographical location.[24] As explained by Kiviat, the cryptographic technology behind blockchain is the core innovation of cryptocurrencies, because 'for the first time ever, secure electronic transfers of value can occur without the presence of a trusted third party'.[25]

However, it must be noted that the technology behind DLT and blockchain is not entirely new. Peer-to-peer (P2P) networks, Public Key Infrastructure (PKI) and encryption technologies existed prior to the development of cryptocurrencies. More specifically,

> *the P2P network was popularised by Napster in June 1999; PKI, which give the ability to secure transaction between two untrusted parties and provides other key elements like time stamping, has been in use since the 1990s; and finally, the cryptographic hash used in blockchain consensus algorithms became popular for security use in areas like mobile devices since the late 1980s.*[26]

1.2.3 Emergence of Cryptocurrency

In this way, cryptocurrency emerged through combining and building on the notions of digital ledgers and alternative money. This combination of concepts occurred first with Bitcoin, the first and largest of cryptocurrency, and brainchild of Satoshi Nakamoto. In 2008, Nakamoto published a paper aimed at presenting a solution to the problems inherent in the exclusive reliance on financial institutions to process electronic payments and to serve as trusted third parties in the conducting of commerce over the internet. These problems include the cost of intermediation, which increases transactions costs and, in turn, 'limit[s] the minimum practical transaction size and cut[s] off the possibility for small casual

[24] S Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (Unpublished Manuscript 2008) 1,1.
[25] T Kiviat, 'Beyond Bitcoin: Issues in Regulating Blockchain Transactions' (2015) 65 Duke Law Journal 570, 577.
[26] Morgan (n 19).

transactions‘as well as the broader cost in the inability to ‘make non-reversible payments for non-reversible services‘.[27]

Building partly on the work of Adam Back[28] and Wei Dai[29], Nakamoto presented a solution to bypass these and other inherent weaknesses of the trust-based model of commerce over the internet. This was done by developing ‘an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party’.[30] The proposed system would solve the double-spending problem (where the same set of coins are spent in more than one transaction) by ‘using a peer-to-peer distributed timestamp sever to generate computational proof of the chronological order of transactions’.[31]

In this instance, the security of the system is maintained by the collective computational power of dispersed nodes (computers running the Bitcoin software).[32] More specifically, double spending is prevented by publicly announcing all transactions, with a system in place for participants to agree on a single history of the order in which transactions were received, with the earliest transaction being the sole legitimate transaction. This is achieved by each transaction being time-stamped, with each subsequent transaction building on the one before it, to form a chain where ‘each additional timestamp reinforces the ones before it’.[33] An algorithm called ‘proof-of-work’,[34] in which nodes compete to solve mathematical problems in order to verify and add transactions to the blockchain, secures this P2P-distributed time-stamp server. This ensures the irreversibility and immutability of each transaction, and ultimately the security

[27] Nakamoto (n 24) 1.
[28] A Back, ‘Hashback—A Denial of Service Counter-Measure’ (*Hashcash*, 2002) <http://www.hashcash.org/hashcash.pdf> Accessed 20 June 2018.
[29] W Dai, ‘B-Money’ (1998) <http://www.weidai.com/bmoney.txt> Accessed 20 June 2018.
[30] S Nakamoto (n 24) 1.
[31] ibid1.
[32] ibid 3.
[33]ibid 2.
[34] Proof-of-work and other cryptocurrency consensus mechanism will be discussed in detail in Chapter 6.

of the overall system—as an immense amount of Central Processing Unit (CPU) power would be needed to redo the proof-of-work of the block and all blocks after it, and then catch up with and surpass the work of the honest nodes.[35]

An additional feature of this system is a re-conceptualisation of the notion of privacy. In traditional banking, privacy is achieved by restricting access to information by the public about the parties involved in transactions. The identities and transactions are known only to the individuals, the trusted third party (bank), and any other relevant counterparties. However, in the cryptocurrency system, where all transactions are, by design and necessity, publicly announced on a blockchain, 'privacy is maintained by breaking the flow of information in another place: by keeping public keys anonymous'.[36] This means that the public can see that someone is sending X amount to someone else, without knowing who the individuals in each transaction are. This is made possible by the fact that public keys (which can be compared to bank account numbers in traditional systems) are pseudonymous,[37] and can only be accessed by their private key counterpart (which can be compared to a bankcard Personal Identification or PIN number).[38]

Nakamoto concluded his paper by stating that 'the network is robust in its unstructured simplicity'.[39] Others agree with this conclusion, and cryptocurrencies were viewed as being 'an exciting innovation that has the potential to greatly improve human welfare and jump-start other potentially revolutionary developments in global communications and business'.[40] The

[35] S Nakamoto (n 24) 2.
[36] ibid 6.
[37] It must be noted that it is difficult, but not impossible, to link cryptocurrency user identities to their blockchain public keys. Companies such as Elliptic are already doing this in partnership with Interpol <https://www.elliptic.co/> Accessed 2 December 2019. Although there are several means to counteract this (such as using zero knowledge proofs as shall be further discussed) the advent of quantum computing is likely to further enable the de-pseudonymisation of cryptocurrency public keys.
[38] Bitcoin.Org, 'How Are Bitcoin Created?' (2014) <https://bitcoin.org/en/faq#how-are-bitcoins-created> Accessed 20 June 2018.
[39] S Nakamoto (n 21) 8.
[40] P Mullan (n 6) 12.

adoption of cryptocurrencies has been based on benefits including privacy (pseudonymity), security and data protection, payment freedom (from banks and institutional authority); the transparency and neutrality of the public ledger are linked with the ideas of personal financial autonomy, central to understanding Bitcoin's socio-cultural and political roots.[41] These are, in turn, linked to the benefits of financial inclusion[42] due to the lower transaction costs than those in traditional banking systems. [43]

In this way, Nakamoto's Bitcoin became the first form of cryptocurrency, the first commercial business-case for DLT, and the first use of cryptography to generate and secure virtual and digital currency—and, in so doing, Bitcoin provided the technical functionality for these to expand across the virtual into the 'real world'. Indeed, without this ability and possibility to be converted into fiat currency or government issued legal tender, cryptocurrencies would not be commercially viable, as they have no intrinsic value.[44] Since the development of Bitcoin, various other cryptocurrencies have come to the fore. Examples of these include Litecoin, Ethereum, Ripple and Dogecoin, with Bitcoin being by far the most widely used and largest by market capitalisation and volume of transactions.[45] There are, at the time of writing, 4,894 different cryptocurrencies with a market capitalisation of nearly US$200 billion, with Bitcoin forming 67 per cent of the market. [46]

It must be noted that there are new taxonomies that have developed around cryptocurrency, most significantly that adopted by the UK Financial Conduct Authority (FCA) which conceptualises cryptocurrencies as a type of cryptoasset.

[41] For more on this aspect of cryptocurrency see D Golumbia, *The Politics of Bitcoin: Software as Right Wing Extremism* (University of Minnesota Press 2016).
[42] A Patwardhan, 'Financial Inclusion in the Digital Age' in D Chuen and R Deng (eds), *Handbook of Blockchain, Digital Finance, and Inclusion* (Elsevier 2017).
[43] For mini-case studies of developing and emerging markets with active digital currency markets, see <http://nextbillion.net/m/bp.aspx?b=4076> Accessed 2 December 2019.
[44] F Velde, 'Bitcoin: A Primer' (*Chicago Fed Letter No 317* 2013) <https://www.chicagofed.org/publications/chicago-fed-letter/2013/december-317> Accessed 2 December 2019.
[45] For information on these currencies and their market capitalisation, see <http://coinmarketcap.com> Accessed 2 December 2019. The regulatory significance of the differences in cryptocurrencies shall be further discussed in Chapter 4.
[46] Data from Coinmarketcap <https://coinmarketcap.com/> from 5 December 2019.

In this instance, cryptoassets are defined as 'cryptographically secured digital representations of value or contractual rights that use some type of distributed ledger technology (DLT) and can be transferred, stored or traded electronically'. In this taxonomy, cryptocurrencies are conceived of as a type of unregulated payment token, distinct from the FCA-regulated security tokens and e-money tokens.[47] The use of the term 'cryptoassets' instead of cryptocurrency has been adopted by other UK regulators, including the HM Revenue and Customs (HMRC).[48] This taxonomy has been adopted by several research institutes and management consultancy firms,[49] which have followed the FCA's lead in using the term 'cryptoassets'. However, the Bank of England's (BOE) policy guidance uses both terms,[50] most likely due to the fact that cryptocurrency is still the more widely used term in jurisdictions other than the UK.[51] This thesis therefore uses the original concept of cryptocurrencies, which defines them as 'digital currencies that rely on a cryptographic protocol to regulate the manner in which (and the extent to which) currency can be created and/or exchanged'.[52] What follows is a brief description of the key actors in the cryptocurrency ecosystem, in order to highlight the complex nature of their functionality.

1.3 The Cryptocurrency Ecosystem

In order to understand how cryptocurrencies work, it is essential to describe the key participants in the cryptocurrency ecosystem. These are the developers who design cryptocurrencies systems, the nodes that download and run the

[47] Financial Conduct Authority, 'Cryptoassets: Our Work' (*Financial Conduct Authority* 23 January 2019) <https://www.fca.org.uk/firms/cryptoassets> Accessed 3 December 2019.

[48] HMRC, 'Cryptoassets Tax for Individuals' (*HMRC Policy Paper* 1 November 2019) <https://www.gov.uk/government/publications/tax-on-cryptoassets/cryptoassets-for-individuals> Accessed 2 December 2019.

[49] Including Ernst and Young and KPMG, see <https://assets.kpmg/content/dam/kpmg/us/pdf/2018/11/institutionalization-cryptoassets.pdf> Accessed 2 December 2019.

[50] Bank of England, 'What Are Cryptoassets (Cryptocurrencies)?' (*Bank of England* 2019) <https://www.bankofengland.co.uk/knowledgebank/what-are-cryptocurrencies> Accessed 2 December 2019.

[51] See for example, the United States' Federal Reserve <https://www.federalreserve.gov/newsevents/speech/brainard20180515a.htm>

[52] P De Filippi (n 14) 2.

cryptocurrency software, and the miners who generate and validate transactions; the exchanges and wallet providers which store and convert cryptocurrency to fiat; and the cryptocurrency payments service providers, which further facilitate and propagate the use of cryptocurrencies. In sum, the four main ways to acquire cryptocurrencies—by mining, as payment for goods and services, exchanging cryptocurrency with other users and by purchasing cryptocurrency at an exchange [53]—will all be alluded to in this section.

1.3.1 Developers

Cryptocurrency software developers are the programmers who design, implement, maintain and update the computer code of cryptocurrency systems. Bitcoin's software, called Bitcoin Core, is free and open source,[54] meaning that any developer can contribute to the project. Whilst Bitcoin Core has a large number of contributors and developers who contribute in coding, testing, reviewing and commenting on the software, the Bitcoin Core project has software maintainers who have 'commit access',[55] and are responsible for the alignment of the multiple contributions. These software maintainers have been described as performing a 'janitorial role', merging patches that the team agrees should be merged, and acting as a final check to ensure that patches are safe and in line with the project goals.[56]

This decentralised, open source software development process is emblematic of all cryptocurrency platforms that are developed out of the modification of Bitcoin Core's software. A 2019 report by Electric Capital showed that Ethereum had the most developers working on its base protocol, with a monthly average of 99 developers contributing to the project per month, compared to Bitcoin's average

[53] Bitcoin.org (n 38).
[54] Open source software is software with source code that anyone can inspect, modify, and enhance <https://opensource.com/resources/what-open-source> Accessed 2 December 2019.
[55] Commit Access is the right to make changes to the copy of the code that will be used for the project's next official release. For more details on committers and maintainers in a software project, see <https://producingoss.com/en/committers.html> Accessed 2 December 2019.
[56] Bitcoin Core, 'About Us' (*Bitcoin Core* 2019) < https://bitcoincore.org/en/about/> Accessed 2 December 2019.

of 50 developers per month[57]. Other cryptocurrency platforms (including EoS, Tron, and Cardano) averaged 25 developers contributing per month. In total, Electric Capital's global data revealed that over 4000 developers per month contribute code to over 2800 cryptocurrencies.[58] Similar to Bitcoin, Ethereum has core developers, including its founder Vitalik Buterin, who make the most contributions to the development of the platform.[59] In this way, it can be seen that cryptocurrency development takes place in a decentralised and crowd-sourced manner, albeit with a smaller team of software developers responsible for committing, moderating and amalgamating proposed improvements to the cryptocurrency platform.[60]

1.3.2 Nodes and Miners

The term 'node' in cryptocurrency refers to a computer that downloads and runs the cryptocurrency software. There are various kinds of nodes, with a full node being one that has downloaded the entire blockchain from the genesis block or first transaction,[61] and light nodes being those that have downloaded only part of blockchain.[62] Every type of node contributes to the security of the cryptocurrency blockchain. The more nodes there are, the larger the distributed network and the more difficult it is to hack. The distributed P2P nature of cryptocurrency means that there is no single point of attack or failure. Indeed, it would require large amounts of computing power to access every node and alter

[57] Electric Capital, 'Electric Capital Developer Report H1 2019' (*Medium*, 12 August 2019) <https://medium.com/@ElectricCapital/electric-capital-developer-report-h1-2019-7d836d68fecb> Accessed 2 December 2019.

[58] ibid.

[59] For an informal list of Ethereum Core Developers, see <https://medium.com/ethex-market/who-are-the-core-devs-of-ethereum-part-i-beb342aaaff0> Accessed 2 December 2019.

[60] The role of developers and the process through which changes are made to cryptocurrency platforms will be re-visited and further discussed in relevant sections of subsequent chapters of the thesis.

[61] According to Bitcoin.org, running a full node requires a minimum of 200 gigabytes of free disk space, 2 gigabytes of memory (RAM), a broadband internet connection with speeds of at least 400 kilobits per second, and a minimum of 6 hours per day in which the system is left running. See <https://bitcoin.org/en/full-node#minimum-requirements> Accessed 2 December 2019.

[62] R Sharma, 'Running a Full Bitcoin Node for Investors' (*Investopedia* 25 June 2019) <https://www.investopedia.com/news/running-full-bitcoin-node-investors/> Accessed 2 December 2019.

them all at the same time.[63] This would take what is known as a '51% attack', a taxing computational feat, as it entails one node capturing and controlling a majority of network hash rate, to revise transaction history and prevent new transactions from confirming. [64]

Miners are a type of full node that play the key role of verifying transactions and, in so doing generating new cryptocurrency. Miners generate new cryptocurrency through the use of powerful software designed to solve complex mathematical problems.[65] Here, miners earn cryptocurrency each time a correct response is generated by their software, which provides financial incentives for participating in and maintaining the network. In general, cryptocurrency software is designed to transform blocks of transactions on the blockchain into a 'hash', which is a shorter string of numbers and letters verifying each transaction based on the transaction preceding it. As explained by Coindesk, 'because each block's hash is produced using the hash of the block before it, it becomes a digital version of a wax seal. It confirms that this block—and every block after it—is legitimate, because if you tampered with it, everyone would know'.[66] This aspect of cryptography ensures that it is nearly impossible to fake cryptocurrency transactions. Miners play a vital role, because it is only after the competitive mining process verifies the transactions that the cryptocurrency relating to that transaction are generated and issued to the recipient, along with the miners' own cryptocurrency 'payment'.[67] In sum, unlike fiat currency that is created when central banks print money, cryptocurrency is created at the point of verification on the blockchain through cryptographic hash functions.

[63] C Miles, 'Blockchain Security: What Keeps Your Transaction Data Safe?' (*IBM* 12 December 2017) <https://www.ibm.com/blogs/blockchain/2017/12/blockchain-security-what-keeps-your-transaction-data-safe/> Accessed 2 December 2019.

[64] Nakamoto (n 24).

[65] ibid.

[66] Coindesk, 'How Bitcoin Mining Works' (*Coindesk* 20 August 2013) <http://www.coindesk.com/information/how-bitcoin-mining-works/> Accessed 2 December 2019.

[67] Miners most commonly create 'mining pools' to combine resources and share their processing power over a network. For more detail on mining pools see <https://www.buybitcoinworldwide.com/mining/pools/> Accessed 2 December 2019.

1.3.3 Exchanges

In cryptocurrency markets, the simplest form of transactions take place using DLT on the blockchain. However, the movement of cryptocurrencies off the blockchain requires intermediation. Here, intermediaries 'act as custodians of cryptocurrency or cryptocurrency credentials originally belonging to their clients and may facilitate and clear transactions for clients without updating the public ledger'.[68] More generally, as adapted from the New York Department of Financial Services (NYDFS), intermediaries in cryptocurrency markets are mainly entities involved in (a) receiving cryptocurrency for transmission or transmitting it, (b) holding cryptocurrency for others, (c) buying and selling cryptocurrency, and (d) exchange services involved in the conversion or exchange of fiat currency or other value into cryptocurrency.[69] In this way, exchanges are the link between the virtual cryptocurrencies and the everyday economy.

Exchanges are a pivotal component of the cryptocurrency ecosystem, as they play the primary role of converting cryptocurrencies to fiat currency. Some exchanges are large exchanges for institutional traders, whilst others are simpler wallet services with more limited buying and selling capabilities.[70] In addition to this, exchanges are also the primary facilitators of cryptocurrency trading activity (including derivatives), as well the main means for storing investments. This can occur either online, or in 'cold storage' services that secure cryptocurrency offline using additional security measures such as multi-signature (multisig)

[68] S Hughes and S Middlebrook, 'Advancing a Framework for Regulating Cryptocurrency Payments Intermediaries' (2015) 32 Yale J on Reg 495, 497.

[69] New York Department of Financial Services (*NYDFS* 2015) 'BitLicense Regulatory Framework' <https://dfs.ny.gov/legal/regulations/bitlicense_reg_framework.htm> Accessed 2 December 2019.

[70] Coindesk, 'How Can I Buy Bitcoins? (*Coindesk* 2015) <http://www.coindesk.com/information/how-can-i-buy-bitcoins/> Accessed 2 December 2019.

wallets, that use a number of keys to protect the account.[71] With these functions in mind, cryptocurrency exchanges can be classified as being custodial, non-custodial, P2P, and decentralised exchanges (DEX).[72] The distinction between custodial and non-custodial exchanges lies in whether or not they hold the user's private keys.[73] Custodial exchanges have access to user's private keys and cryptocurrency in order to execute trades faster offline (off-chain), without waiting for the more time-consuming transaction verification on the blockchain (on-chain).[74] Both P2P and DEX are non-custodial exchanges. P2P exchanges 'provide a flexible user matching platform where users can decide whether to store funds at the exchange and perform the actual trade outside of the platform'.[75] On the other hand, DEXs 'uses a public blockchain for both order matching as well as clearing and settlement while allowing users to maintain control of their funds for the entirety of the trading process',[76] which, like P2P exchanges, is a completely decentralised online means of transacting. Finally, similarly facilitating the exchange of cryptocurrency to fiat are cryptocurrency Automated Teller Machines (ATMs). Records show that there are now over 5,000 cryptocurrency ATMs around the world, with 70 per cent of these being in the United States and Canada.[77] Cryptocurrency ATMs can be used in the following ways: to use fiat to purchase cryptocurrencies, use cryptocurrencies to purchase

[71] ibid.

[72] M Rauchs and others, '2nd Global Cryptoasset Benchmarking Study' (*Cambridge Centre for Alternative Finance* December 2018) <https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2019-09-ccaf-2nd-global-cryptoasset-benchmarking.pdf> Accessed 2 December 2019.

[73] J Wood, 'Crypto Exchanges: Custodial vs Non-Custodial vs Decentralized' (*Medium* 18 March 2018) <https://medium.com/@jacobrobertwoods/crypto-exchanges-custodial-vs-non-custodial-vs-decentralized-3d1d04cf205> Accessed 2 December 2019.

[74] The fastest cryptocurrency transaction time in September 2019 was Dash (2 mins 39 seconds), Bitcoin averages 10 minutes per transactions. (The difference between Bitcoin BTC and Bitcoin Cash BCH will be discussed further, in Chapter 6). Cryptocurrency transaction speeds vary based on nodes, consensus mechanisms in use, network volumes and congestion. For further details, see Coinsutra <https://coinsutra.com/transaction-speeds/> Accessed 2 December 2019.

[75] M Rauchs (n 72) 12.

[76] ibid.

[77] M Beedham, 'There Are Now Over 5,000 Cryptocurrency ATMs Around The World' (*The Next Web* 26 June 2019) <https://thenextweb.com/hardfork/2019/06/26/5000-bitcoin-cryptocurrency-atms-coinatmradar/> Accessed 2 December 2019.

other cryptocurrencies, or to cash-out virtual cryptocurrency for fiat currency by withdrawing the fiat currency in exchange for cryptocurrency at the ATM.[78]

1.3.4 Wallet Providers

Electronic Wallet Providers are exclusively concerned with the storage of cryptocurrency.[79] This distinction is not always clear, as some wallets provide currency exchange services within the wallet interface.[80] In the simplest of terms, wallets are used for storing cryptocurrency, whereas exchanges are mainly for buying and selling cryptocurrencies from and into other cryptocurrencies or fiat. Wallet services are either accessed through mobile applications, web interfaces, desktop clients (which requires the downloading of software), or a combination of the three. Wallet services offer storage facilities either online or offline, with most offline storage services being offered at a fee, and online storage often taking place at no direct cost to customers. In addition to this, some wallets are independent (cannot be controlled or accessed by the service providers) whilst others are not.[81] An example of the former is Coinbase's Vault service, which denies the company access to consumer funds, and examples of the latter are MyCelim and Exodus Blockchain Assets, a wallet service that also allows for the trading of cryptocurrency within wallets.[82] Additionally, there is the option to use a cryptocurrency hardware wallet, which stores private keys on a secure hardware device such as Trezor,[83] offering the extra security of being immune to software viruses and hacking by virtue of being offline. Similar advantages are

[78] Financial Action Task Force, 'Guidance for a Risk-Based Approach: Virtual Currencies' (*FATF* June 2015) <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf> Accessed 2 December 2019.

[79] G Hileman and M Rauchs, 'Global cryptocurrency benchmarking study' (Centre for Alternative Finance, 2017) <https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf> Accessed 2 December 2019.

[80] ibid.

[81] There is also the option for cryptocurrency owners to purchase hardware wallets in which to store their cryptocurrency. These are the most secure option, as they are offline and so cannot be hacked. An example of a hardware wallet is Trezor. <https://trezor.io/> 3 December 2019.

[82] O Beigel, 'Bitcoin Wallet Guide, Reviews and Comparison' (*99bitcoins* 12 November 2019) <https://99bitcoins.com/bitcoin-wallet/> Accessed 2 December 2019.

[83] For more on Trezor's hardware wallet, see <https://trezor.io/> Accessed 3 December 2019.

offered by wallets providing 'cold storage'[84] options for cryptocurrency users to store their private keys in an offline environment, away from the internet.

1.3.5 Payment Providers

Cryptocurrency payment providers are those that use cryptocurrency primarily as a 'payment rail' for fast and cost-efficient payments, and those that facilitate the use of cryptocurrencies.[85] Of focus here will be cryptocurrency lending platforms, remittance services and merchant services.

1.3.5.1 Lending Platforms

Based on crowdfunding models,[86] cryptocurrency lending platforms are aimed at facilitating global P2P financing, including micro-financing using cryptocurrency. These platforms offer several innovations, such as relationship lending and the replacement of traditional credit scoring with algorithms based on Big Data mining, in order to assess creditworthiness and trustworthiness through analysis of variables such as buying habits, lifestyle choices and memberships.[87] Cryptocurrency lending platforms not only connect potential lenders to borrowers, they provide a space in which borrowers can 'pitch' their business plans to lenders directly and, in so doing, reducing the information asymmetries evident in traditional banking, all without geographical barriers. In addition to this, cryptocurrency lending platforms facilitate transactions by transmitting and exchanging cryptocurrency, and remitting interest repayments in the lender's

[84] Coinsutra, 'What is Cold Storage in Cryptocurrency?' (*Coinsutra* 12 August 2019) <https://coinsutra.com/cold-storage-cryptocurrency/> Accessed 2 December 2019.
[85] Hileman and Rauchs (n 79).
[86] Crowdfunding is a way of raising finance by asking a large number of people each for a small amount of money. For more details, see <https://www.ukcfa.org.uk/what-is-crowdfunding/> Accessed 2 December 2019.
[87] Panorama Crypto, '8 Cryptocurrency Lending Platforms' (*Panorama Crypto* 3 October 2019) <https://panoramacrypto.com/8-cryptocurrency-lending-platforms/> Accessed 2 December 2019.

cryptocurrency of choice. Examples of cryptocurrency lending platforms include YouHodler, Celsius Network and Coinloan.[88]

1.3.5.2 Remittance Services

Similarly, there are a plethora of Financial Technology (fintech) start-ups leveraging cryptocurrency and DLT to provide remittance services. These services exploit the technology's ability to transfer and exchange value in near real time, to and from anywhere in the world, and the exchangeability of any cryptocurrency into any fiat currency across the world.[89] Often with a geographical focus on the developing world, these cryptocurrency remittance services connect remitters to receivers using bespoke ATMs, mobile and smart phones, and local exchangers. Examples of these forms of service providers include BitPesa (Sub-Saharan Africa), BitSpark (APAC region), and Coin.ph (South-East Asia).[90]

1.3.5.3 Merchant Services

Cryptocurrency merchant services process payments on behalf of sellers accepting cryptocurrency payments. Some of these merchant service providers feature a 'fuller-featured platform that lets users buy, store and transfer cryptocurrency, often providing additional services such as insured accounts and bill payment services'.[91] Typically, cryptocurrency payment processors provide software applications or embeddable code that allow the merchant or other business to accept cryptocurrency payment on its website or at its brick-and-mortar location. They then either electronically transmit the cryptocurrency to the merchant's wallet (hosted by the processor or another wallet provider, or held directly by the merchant), or convert some or all of the cryptocurrency into

[88] S Khatwani, '2019's Best Cryptocurrency Lending (Crypto Loans) Platforms To Use' (*The Money Mongers* 22 October 2019) Accessed 2 December 2019.
[89] M Rauchs (n 72).
[90] M Di Salvo, 'Report: Use of Cryptocurrencies for Remittances is Growing in Popularity' (*Bitcoin.com* 25 December 2018) <https://news.bitcoin.com/report-use-of-cryptocurrencies-for-remittance-is-growing-in-popularity/> Accessed 2 December 2019.
[91] Hileman and Rauchs (n 79) 72.

fiat currency and transmit payments to the merchant's account, as directed. [92] Examples of cryptocurrency merchant service providers include CoinPayments, BitPay and Coinbase Merchant Service.[93]

1.4 Issues of Regulatory Concern

Following on from this overview of the cryptocurrency ecosystem is a consideration of why cryptocurrencies are in need of regulation. There are several issues of concern to regulators that highlight why cryptocurrencies are subject to legal and regulatory oversight. These include the use of cryptocurrency in cybercrime activities; money laundering, terrorist financing and tax evasion; consumer protection; investor protection; and prudential and systemic risk. Each of these shall be discussed in turn.

1.4.1 Cyber Crime

Cryptocurrencies are being used in the perpetuating of both cyber-dependant and cyber-enabled crime. As per the definitions of the UK National Cyber Security Strategy, cyber-dependent crimes are 'crimes that can be committed only through the use of Information and Communications Technology ('ICT') devices, where the devices are both the tool for committing the crime, and the target of the crime', whereas cyber-enabled crimes are 'traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of ICT'.[94]

[92] Financial Action Task Force (n 78).
[93] H Agrawal, '7 Best Bitcoin Payment Gateways for Merchant Account & Services' (*Coinsutra* 15 November 2019) <https://coinsutra.com/bitcoin-payment-gateways-merchants/> Accessed 2 December 2019.
[94] HM Government, *National Cybersecurity Strategy 2016 to 2021* (Policy Paper 1 November 2016) 17 <https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021> Accessed 2 December 2019.

1.4.2 Cyber-Dependent Crimes

Cyber-dependent crimes include the illicit intrusions into computer networks, including hacking, and the disruption or downgrading of computer functionality, including malware and Denial of Service (DOS) or Distributed Denial of Service (DDOS) attacks.[95] Hacking is a frequent feature in cryptocurrency activity in three ways. Firstly, cryptocurrency exchanges and wallet providers are often the victims of hacking themselves, resulting in the theft or loss of cryptocurrency. This shall be further discussed below. Secondly, the use of cryptocurrency mining malware, also known as 'cryptojacking', involves the use of malicious software to use a device's CPU power to mine cryptocurrency without authorisation. This could potentially render a device unresponsive or unavailable for legitimate processes, making it appear as if the device is simply running slower than usual. Cryptocurrency mining uses a large amount of computing power. An increase in available CPU power therefore results in an increased probability of solving the complex equations required to validate transactions and earn cryptocurrency. Finally, cryptocurrencies are fuelling the use of ransomware attacks. Ransomware, such as Ryuk, 'encrypts the targets' hard drives, locking data until victims contact the hackers and pay a Bitcoin ransom to have their data restored'.[96] These activities have proved profitable to cybercriminals with ransomware such as CryptoLocker and CryptoWall having received 133,045.9961 BTC and 87,897.8510 BTC respectively, and Jenkins-Miner (cryptojacking software) earning its operator over US$3,000,000 worth of the cryptocurrency Monero.[97]

[95] DOS is a type of cyber-attack designed to render a service inaccessible. DDOS is a DOS attack that originates from multiple computers instead of one. For further information on these and other types of cyber-attacks, see <https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection> Accessed 2 December 2019.

[96] M Beedham, 'Report: Cryptocurrency Ransomware Payments up 90%, Thanks to Ryuk' (*The Next Web*, 18 April 2019) <https://thenextweb.com/hardfork/2019/04/18/cryptocurrency-ransom-increase-ryuk/> Accessed 2 December 2019.

[97] G Tziakouris, 'Cryptocurrencies—A Forensic Challenge or Opportunity for Law Enforcement? An Interpol Perspective' [2018] IEEE Security and Privacy 13(4).

1.4.3 Cyber-Enabled Crimes

Reported incidents of cyber-enabled crimes involving cryptocurrencies include economic-related cybercrime such as fraud and online marketplaces for illegal goods and services. Instances of fraud will be further discussed in the section on consumer and investor protection below. The most prominent use of cryptocurrency in cyber-enabled crimes has been their use for the buying and selling of illegal goods and services on darknet[98] markets such as Silk Road.

Silk Road was an online marketplace used for the sale and purchase of mainly illicit drugs, as well as 'stolen credit and debit card numbers, fake IDs, counterfeit currencies, hacking tools and login credentials for hacked accounts'.[99] Its founder, Ross Ulbricht, was sentenced to life imprisonment after being convicted of on seven charges related to narcotics distribution, computer hacking and conspiracy.[100] The Silk Road case highlights how Bitcoin and other cryptocurrencies can be used for money laundering and financial crime, as all purchases on the website could only be made through bitcoins. Following up from Silk Road are other dark marketplaces focused on selling drugs, such as Atlantis and Silkroad 2.0 and 3.0. As such, the risk of cryptocurrency use for nefarious purposes is still ongoing, despite the advances in enforcement that led to the conviction of Ross Ulbricht. [101] Other cases related to Silkroad include *R v Assaf and others*,[102] where four University of Manchester students were charged with fourteen drug-related counts, and sentenced in March 2018 to 12, 11, 15 and seven years respectively, for buying and selling of illicit drugs using Silkroad.

[98] The darknet or darkweb is a part of the internet that uses custom software and hidden networks in order to create an encrypted network of secret websites with internet content that is not accessible via traditional search engines. Description adapted from Investopedia <https://www.investopedia.com/insights/what-dark-net/> Accessed 2 December 2019.
[99] K Zetter, 'How the Feds Took Down the Silk Road Drug Wonderland' (*Wired.Com* 18 November 2013*)* <http://www.wired.com/2013/11/silk-road/> Accessed 2 December 2019.
[100] S Higgins, 'Silk Road Operator Ross Ulbricht Sentenced to in Life in Prison' (*Coindesk ,* 29 May 2015) <http://www.coindesk.com/ross-ulbricht-sentenced/> Accessed 2 December 2019.
[101] These advances in enforcement shall be further discussed in more detail, in Chapter 5 of this thesis.
[102] *R v Assaf and others* [2019] EWCA Crim 1057 Court of Appeal, Criminal Division.

1.4.4 Money Laundering, Terrorist Financing and Tax Evasion

Beyond their use in illicit markets, cryptocurrencies are also of concern to regulators due to their potential use in evading taxes and circumventing Anti-Money Laundering (AML) and Counter Terrorism Financing (CTF) regulations. As highlighted by the European Banking Authority (EBA), money laundering and terrorist financing through cryptocurrency is made possible by the fact that criminals are able to deposit and transfer VCs anonymously, as well as transfer these funds 'globally, rapidly and irrevocably'.[103] Similarly, because of pseudonymity, terrorists can use cryptocurrency remittance systems and accounts for financing purposes, whilst 'undermining the ability of enforcers to obtain evidence and recover criminal assets'.[104] Examples of cryptocurrency-related money laundering cases include that of the Bitcoin exchange OKCoin, where hundreds of thousands of US dollars were laundered,[105] as well as the case of BitInstant, in which an estimated sum of more than US$1,000,000 was laundered for Silk Road market customers.[106]

In addition to the potential threat of money laundering, it is important to note the potential use of cryptocurrencies by extremist groups to facilitate the trade of illicit products (for instance, stolen antiquities, drugs, and firearms), remit money to areas that are under high financial scrutiny or embargo, and publicly crowdfund their operations.[107] However, despite the public reporting of the use of cryptocurrencies by terrorist organisations such as Islamic State as a means of moving and raising funds, these organisations are also very focused on the traditional means of moving funds.[108] Finally, cryptocurrency tax evasion occurs

[103] European Banking Authority, 'Opinion on 'Virtual Currencies' (*EBA* 2014) <http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf> Accessed 2 December 2019.

[104] ibid.

[105] Gautham, 'Bitcoin Exchange OKCoin Fined in Money Laundering Case' (*Newsbtc,* 15 August 2016) <https://www.newsbtc.com/2016/08/15/china-okcoin-exchange-fined> Accessed 15 January 2020.

[106] Ibid.

[107] G Tziakouris (n 97).

[108] I McKendry, 'ISIL May Be Using Bitcoin, Fincen's Calvery Says', (*American Banker* 16 November 2015) <https://www.americanbanker.com/news/isil-may-be-using-bitcoin-fincens-calvery-says> Accessed 15 January 2020.

where holders of cryptocurrency fail to report income and pay taxes from cryptocurrency transactions in line with the relevant regulatory requirements. In the US, the Internal Revenue Service (IRS)'s criminal chief Don Fort described cryptocurrencies as a 'significant threat' to tax collection,[109] announcing criminal tax evasion cases involving them, based on data on cryptocurrency holders compelled from cryptocurrency exchanges.

1.4.5 Consumer and Investor Protection

Cryptocurrencies additionally pose various types of risks to consumers and investors, who may buy unsuitable products, face large losses, be exposed to fraudulent activity, struggle to access market services, or be exposed to the failings of service providers.[110] These risks are highest when cryptocurrencies are used as a means of payment, particularly with fraudulent exchanges, exchanges being hacked, and a numerous range of personal e-wallet security concerns.[111]

Buying or selling cryptocurrency through an exchange entails the depositing of cryptocurrency into a wallet provided by the exchange service provider. In order to ensure constant and adequate liquidity to execute transactions in near real-time, exchanges have access to the private keys assigned to each customer, enabling them to partake in a form of fractional reserve banking, a fact that sometimes pushes them to act 'more like a margin-taking balance-sheet deploying broker-dealers'[112] instead of a simple exchange service—an activity

[109] L Browning and L Davison, 'Crypto Tax Avoiders Face IRS Roulette: Fess Up or Try Hiding' (*Bloomberg*, 1 August 2019) < https://www.bloomberg.com/news/articles/2019-08-01/crypto-tax-avoiders-face-irs-roulette-fess-up-or-try-to-hide> Accessed 15 January 2020.

[110] HM Treasury, 'Cryptoassets Taskforce: Final Report' (*HM Treasury Policy Paper,* 30 July 2018) < https://www.gov.uk/government/publications/cryptoassets-taskforce> Accessed15 January 2020.

[111] European Banking Authority (n 103).

[112] I Kaminska, 'Time to Re-Evaluate Blockhain Hype' (*FTAphaville* 3 August 2016) <http://ftalphaville.ft.com/2016/08/03/2171799/time-to-reevaluate-blockchain-hype/> Accessed 2 December 2019.

for which Bitfinex was sanctioned by US regulators in 2016.[113] The act of depositing Bitcoin in an exchange and ceding exclusive use of a private key to a third party invokes fiduciary duties, and the need for trust between the exchange and the customer. In addition to this, the exchange requests and has access to customer's bank details and other identity markers, again invoking a duty of trust in the protection of customer data. Similarly, the removal of the safety found in the immutable digital seal of transactions on the blockchain, as a result of transactions between customers being recorded only on exchanges' trade history with only the exchanges' wallet transactions being recorded on the blockchain,[114] further adds to the risks faced by consumers. Where exchange services are provided by brokerages or facilitated by P2P platforms, further risk arises from the need for customers to verify for themselves the legitimacy of a trading partner, as well as the risk of delivery of funds either via bank transfer or in person.

However, the most frequent manifestation of risk in exchange services has to do with the loss of funds held in escrow by hacking. In 2019 alone, 12 major hacks occurred of cryptocurrency exchanges, in which over US$292 million worth of cryptocurrency and 510,000 user logins were stolen.[115] More historically, Moore and Christin found that 18 out of 40 Bitcoin exchanges tracked between 2010 and 2013 had closed down after being breached, showing the failure rate of Bitcoin exchanges to be 45 per cent, with a median lifetime of only 381 days.[116] Interestingly, their study found that high-volume exchanges are less likely to close, but more likely to experience a breach, meaning that exchanges face a paradoxical challenge whereby 'the continued operation of an exchange depends

[113] S Higgins, 'CFTC Fines Bitcoin Exchange Bitfinex $75,000 Over Trading Violations' (*Coindesk* 3 June 2016) < https://www.coindesk.com/cftc-bitcoin-exchange-bitfinex-trading-violations> Accessed 2 December 2019.

[114] N Bhaskar and D Lee, 'Bitcoin Exchanges' in D Lee, and C Kuo (eds), *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data* (Elsevier 2015).

[115] P Thomson, 'Most Significant Hacks of 2019—New Record of Twelve in One Year' (*Cointelegraph* 20 January 2020) <https://cointelegraph.com/news/most-significant-hacks-of-2019-new-record-of-twelve-in-one-year> Accessed 15 January 2020.

[116] T Moore and N Christin, 'Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk' *International Conference on Financial Cryptography and Data Security* (2016) 25-33 Springer Berlin Heidelberg.

on running a high transaction volume, which makes the exchange a more valuable target to thieves'.[117] An additional risk factor of exchanges lies in the irrevocability of transactions, where, in this case, 'irrevocability makes any Bitcoin transaction involving one or more intermediaries' subject to added risk, such as if the intermediary becomes insolvent or absconds with customer deposits'.[118] This risk came most prominently to the fore with the collapse of Mt Gox, the world's largest cryptocurrency exchange at the time, whose bankruptcy in 2014 led to the loss of over US$473 million worth of Bitcoin.[119] This has been the largest recorded theft of Bitcoin in history. More recent loss of funds include that of the Canadian cryptocurrency exchange QuadrigaCX in 2019, which led to customers losing US$190 million in both cryptocurrency and fiat.[120] The QuadrigaCX case highlights another key point of vulnerability of cryptocurrency exchanges. In this instance, the loss of customer funds occurred after the passing QuadrigaCX's CEO, Gerald Cotten, as no one else either in or outside of the company knew how to access the exchange's cryptocurrency reserves—or indeed, where they might even be located.[121] Similar loss of customer funds without the possibility of recourse or refund can occur in instances where the customer themselves loses their own private keys.[122]

In addition to concerns around the hacking of platforms and consumer loss of access to funds, cryptocurrency trading platforms may fail to act in the best interest of investors. A case in point is *Ang v Reliantco Investments Ltd*, where the claimant, Ms Ang, who invested in Bitcoin futures, claimed that Reliantco, a financial products and services online trading platform, wrongfully blocked and

[117] ibid 7.

[118] ibid 2.

[119] R McMillan, 'The Inside Story of Mt Gox, Bitcoins $460million Disaster' (*Wired.com* 3 March 2014) <http://www.wired.com/2014/03/bitcoin-exchange/> Accessed 2 December 2019.

[120] N De, 'Quadriga Creditor Protection Filing' (*Coindesk* 1 February 2019) <https://www.coindesk.com/quadriga-creditor-protection-filing> Accessed 2 December 2019.

[121] N De and A Baydakova, 'The Collapse of QuadrigaCX: What We Know (And What We Don't)' (*Coindesk,* 6 February 2019*)* <https://www.coindesk.com/quadrigacx-explainer> Accessed 2 December 2019.

[122] M Frauenfreder, 'I Forgot My PIN': An Epic Tale of Losing $30,000 in Bitcoin' (*Wired* 29 October 2017) <https://www.wired.com/story/i-forgot-my-pin-an-epic-tale-of-losing-dollar30000-in-bitcoin/> Accessed 2 December 2019.

terminated her platform account and breached data protection obligations in connection with her account.[123]

The trading of crypto-securities and cryptocurrency-based derivatives has become popular—an example of this is Cryptofacilities,[124] which allows customers to trade a forward contract on the BTC price to hedge against fluctuation. However, these offerings may be fraudulent as seen by the findings of the Wall Street Journal, which, in a review of documents produced for 1,450 digital coin offerings, found 271 with red flags, including 'plagiarized investor documents, promises of guaranteed returns and missing or fake executive teams'.[125] In this way, cryptocurrency investors are vulnerable to fraudulent activities including scams and Ponzi schemes, particularly related to Initial Coin Offering (ICO)s.[126] Exit scams related to ICOs occur in instances where criminals persuade their victims to buy large numbers of fake coins, subsequently disappearing with millions of dollars.[127] For example, a 2018 report by ABC News stated that more than 1,200 Australians experienced losses totalling more than AU$1.2 million as a result of cryptocurrency scams.[128] These and numerous other instances around the world have led to warnings by the International Organisation of Securities Commissions (IOSCO), stating that 'these offerings are not standardised, and their legal and regulatory status is likely to depend on the

[123] *Ang v Reliantco Investments Ltd* [2019] Queen's Bench Division (Commercial Court) EWHC 879 (Comm).

[124] See <https://www.cryptofacilities.com> Accessed 2 December 2019.

[125] S Shifflett and C Jones, 'Buyer Beware: Hundreds of Bitcoin Wannabes Show Hallmarks of Fraud' (*Wall Street Journal* 17 May 2018) <https://www.wsj.com/articles/buyer-beware-hundreds-of-bitcoin-wannabes-show-hallmarks-of-fraud-1526573115> Accessed 2 December 2019.

[126] 'An Initial Coin Offering (ICO) is the cryptocurrency industry's equivalent to an Initial Public Offering (IPO). ICOs act as a way to raise funds, where a company looking to raise money to create a new coin, app, or service launches an ICO. Interested investors can buy into the offering and receive a new cryptocurrency token issued by the company'. Definition from Investopedia <https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp> Accessed 2 December 2019.

[127] G Tziakouris (n 97).

[128] L Hobday, 'More Than 1,200 People Complain to ACCC about Bitcoin Scams' (*ABC News* 19 February 2018) <http://www.abc.net.au/news/2018-02-19/more-than-1200-people-complain-to-accc-about-bitcoin-scams/9462240> Accessed 2 December 2019.

circumstances of the individual ICO'.[129] The regulation of ICO's and IOSCO's stance will be discussed in the following chapter. Of relevance in this section is the need for investor protection regarding cryptocurrency, where their speculative nature, complexity and insufficient information result in the risk of loss and fraud.[130]

1.4.6 Prudential and Systemic Risk

The final issue of regulatory concern brought about by cryptocurrencies has to do with their potential implications for financial stability, prudential and systemic risk, which may arise if the market grows and cryptocurrencies are more widely used. The BIS's view on the systemic implications of cryptocurrency is similar to that of the IMF, which is that they do not yet pose systemic risk due to currently relatively low volume of transactions.[131] However, the BIS includes the warning that 'if authorities do not act pre-emptively, cryptocurrencies could become more interconnected with the main financial system and become a threat to financial stability'.[132] Similarly, in the UK, the BOE's Financial Policy Committee (FPC) concluded that:

> *existing crypto-assets do not currently pose a material risk to UK financial stability, and the FPC 'will act to ensure the core of the UK financial system*

[129] IOSCO, 'IOSCO Board Communication on Concerns Related to Initial Coin Offerings (ICOs)' (*IOSCO/MR/01/2018* 18 January 2018) <http://www.iosco.org/news/pdf/IOSCONEWS485.pdf> Accessed 2 December 2019.

[130] BaFin, 'Initial Coin Offerings: High Risk for Consumers' (*BaFin* 15 November 2017) <https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2017/fa_bj_1711_ICO_en.html;jsessionid=F880FC5388DF54C0EE1A65D0AC63407A.1_cid290> Accessed 2 December 2019.

[131] Cryptocurrencies account for only 0.5% of the total value of all narrow money. For further analysis see N Reiff 'How Much of the World's Money is in Bitcoin?' (*Investopedia* 16 January 2020) < https://www.investopedia.com/tech/how-much-worlds-money-bitcoin/> Accessed 20 January 2020.

[132] A Carstens, 'Money in the Digital Age: What Role for Central Banks?' (*Bank of International Settlements* 6 February 2018) <https://www.bis.org/speeches/sp180206.pdf> Accessed 2 December 2019.

> *remains resilient if linkages between crypto-assets and systemically important financial institutions or markets were to grow significantly.*[133]

However, there are areas in which cryptocurrencies are starting to become more interconnected with the main financial system, particularly with hybrid exchanges that combine blockchain-based service provision with existing traditional banking and finance institutions. An example of this is Circle Pay. Having acquired an e-money license in the UK, and being fully registered as a MSB across all US states, including being one of the few to acquire a NYC Bitlicense, Circle Pay's operations in the UK are based on a partnership with Barclays Bank that allows them to hold pounds sterling on behalf of their customers. Circle Pay operates on the Bitcoin blockchain, in order to facilitate near instantaneous transactions, however it does not participate in trading activities so it cannot be fully classified as an exchange. It does, however, provide limited wallet services and high frequency, low-volume remittances.[134][135] This hybrid model follows on for the 2013 partnerships between the German bank Fidor Bank AG and Bitcoin.de (providing liability for Bitcoin.de's parent company, Bitcoin Germany GmbH), and the exchange Kraken, in the first cooperation between the banking sector and the cryptocurrency industry.[136] This fiat-focused, over-the-blockchain model that also allows for cryptocurrency transactions in partnership with the traditional banking industry, is potentially a signpost for the future of intermediation of cryptocurrencies and the blockchain.

Further discussion of hypothetical scenarios regarding the potential impact of cryptocurrencies on prudential regulation, monetary and fiscal policy are being conducted within the context of research into the development of Central Bank

[133] Financial Policy Committee, 'Financial Policy Committee statement from its meeting - 12 March 2018' (*Bank of England* 16 March 2018) <https://www.bankofengland.co.uk/statement/fpc/2018/financial-policy-committee-statement-march-2018> Accessed 2 December 2019.

[134] I Allison, 'Bitcoin Graduate Circle Launches Free Social Payment App in UK with Barclays', (*International Business Times* 6 April 2016) <http://www.ibtimes.co.uk/bitcoin-graduate-circle-launches-free-social-payment-app-uk-barclays-1553353> Accessed 2 December 2019.

[135] Circle.com, 'About' (*Circle* 2016) <https://www.circle.com/en-gb/about> Accessed 2 December 2019.

[136] P Mullan, '*The Digital Currency Challenge*' (2014 Palgrave McMillan) 58.

Digital Currencies (CBDC).[137] In this way, the assessment of the potential prudential and systemic risks associated with cryptocurrencies might warrant further discussion in the future, subject to the development and adoption of cryptocurrencies by both private and the public sector.

1.5 Conclusion

With an analysis of the regulation of cryptocurrency in mind, this chapter has sought to answer two fundamental preliminary questions, namely: 'what are cryptocurrencies and how do cryptocurrencies work?', and 'why do cryptocurrencies need to be regulated?' Taking an evolutionary perspective on the advent of cryptocurrencies, this chapter has described how cryptocurrencies developed from the DC and VC combined with traditional notions of ledgers, incorporating blockchain and DLT to create a unique means of generating, storing and transmitting value.[138] This description highlighted the use of DLT and blockchain, cryptographic protocols and P2P networking as the features that make cryptocurrencies distinct. In other words, the technical components and functionality of cryptocurrencies are their primary defining features. The description of the multi-player cryptocurrency ecosystem, consisting of developers, nodes and miners, exchanges, and wallet and payment providers highlighted both the complexity and system-like features of cryptocurrencies, which are fundamental to understanding how cryptocurrencies work. This understanding of the fundamental role of the underlying technology to the conceptualising of cryptocurrency, and the complex and system-like functioning

[137] Bank of England, 'Central Bank Group To Assess Potential Cases For Central Bank Digital Currencies' (*Bank of England* News Release 21 January 2020) <https://www.bankofengland.co.uk/-/media/boe/files/news/2020/january/central-bank-group-to-assess-potential-cases-for-central-bank-digital-currencies.pdf?la=en&hash=F0F25B3FC0CB1F7A64B08797C3D124C171C0BF27> Accessed 15 January 2020.

[138] Discussions on whether or not cryptocurrencies qualify as 'money' are peripheral to and beyond the scope of this thesis. For further discussions on this topic see O Bjerg, 'How is Bitcoin Money?' [2016] 33 Theory, Culture & Society, 53; European Parliament, 'Virtual Money: How Much Do Cryptocurrencies Alter the Fundamental Functions of Money? (*European Parliament* Monetary Dialogue Papers, December 2019) <https://www.europarl.europa.eu/cmsdata/189495/LSE-original.pdf> Accessed 8 December 2019.

of cryptocurrencies form the contextual and conceptual foundation for this thesis.

The second half of this chapter identified the issues of regulatory concern presented by cryptocurrencies, in order to consider why cryptocurrencies are in need of regulation. These concerns have to do with the potential use of cryptocurrencies for the purposes of cybercrime, money laundering, financing of terrorism and tax evasion, consumer and investor protection and finally, prudential and systemic risk. This analysis has shown that whilst there are legitimate uses for cryptocurrencies, and there is considerable interest in their innovative potential in the financial sector and beyond, the proliferation of the Silk Road darkweb site and the legal challenges brought about by the collapse of Mt Gox sparked equally legitimate regulatory attention directed at this market.

However, it must be noted that there is a growing concern that 'public discussion surrounding cryptocurrency crime trends is often anecdotal, sensationalised, and of little practical use to compliance officers at cryptocurrency businesses'[139] especially when data and evidence is sought to support concerns around the potential use of cryptocurrencies for nefarious purposes. For example, data from leading cryptoasset management firm Elliptic shows how 'the overall impact of Bitcoin and other cryptocurrencies on money laundering and other crimes is sparse in comparison to cash transactions', and that, as of 2019, only US$829 million in Bitcoin has been spent on the darkweb (a mere 0.5 per cent of all Bitcoin transactions); illicit transactions still make up a small share of all cryptocurrency activity at just 1.1 per cent.[140] [141]

[139] Elliptic, 'Cryptocurrencies: Money Laundering & Terrorist Financing Trends [Infographic]' (*Elliptic* 29 March 2019) <https://www.elliptic.co/our-thinking/cryptocurrencies-money-laundering-terrorist-financing-trends-infographic> Accessed 8 December 2019.

[140] Elliptic, 'Bitcoin Money Laundering: How Criminals Use Crypto (And How MSBs Can Clean Up Their Act)' (*Elliptic,* 18 September 2019) < https://www.elliptic.co/our-thinking/bitcoin-money-laundering> Accessed 8 December 2019.

[141] Further discussions include comparisons in volumes laundered via the traditional banking system in relation to those via cryptocurrency which are negligible by comparison. For details see <https://breakermag.com/crypto-money-laundering-is-nothing-compared-to-what-banks-do/> Accessed 15 January 2020.

Similarly, a report by the Rand Corporation on cryptocurrency use for terrorist financing concluded that 'current concerns about cryptocurrency as a significant enabler of terrorist groups are almost certainly overblown, but coming improvements in cryptocurrency technologies will likely have a significant long-term effect on CTF'.[142] Further to this observation is the assertion that compared to cash, cryptocurrencies are a lot more transparent, as every transaction is recorded in a publicly visible ledger.[143] This enables companies such as Chainanalysis—equipped with the right tools—to:

> *see how much of all cryptocurrency activity is associated with crime, hone in on the types of crime that dominate the ecosystem, and share insights with law enforcement and the industry to curb its impact and stop bad actors from abusing the system and, in many cases, taking advantage of vulnerable people.*[144]

This observation further highlights the technical nature of the differences between cryptocurrency and fiat currency, and points at the innovative potential that cryptocurrencies present—not just to global commerce, but to law enforcement. This shall be a central theme of this thesis, which supports the view that in addressing the above-mentioned issues of regulatory concern one must balance both the mitigation of risk and the promotion of growth in innovation, both for the benefit of the public good. What follows is an overview of current cryptocurrency regulation, in both the global and national spheres.

[142] C Dion-Schwarz, D Manheim and P Johnston, 'Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats' (*Rand Corporation,* 2019) <https://www.rand.org/pubs/research_reports/RR3026.html> Accessed 15 January 2020.

[143] Chainanalysis, 'The Chainanalysis 2020 Crypto Crime Report' (*Chainanalysis*, January 2020) < https://go.chainalysis.com/2020-Crypto-Crime-Report-Demo.html?aliId=eyJpIjoiQkxPMEcwRk1uXC9zSGRrbTAiLCJ0IjoiN3JUcUNtNWxaUlc2QnhOc2JJOXhqdz09In0%253D> Accessed 15 January 2020.

[144] ibid.

Chapter Two: Current Cryptocurrency Regulation

2.1 Introduction

This chapter is aimed at describing the current means of regulating cryptocurrencies, prior to an evaluation and analysis of the existing regulatory framework. With this in mind, the chapter will present an overview of international and regional regulatory responses. The organisations to be included in this analysis are the International Monetary Fund (IMF), the G20 and the Financial Stability Board (FSB), the Organisation for Economic Co-Operation and Development (OECD) the Financial Action Task Force (FATF), the Bank of International Settlements (BIS), International Organisation of Securities Commission (IOSCO), and the various organisations within the European Union (EU). This will be followed by an overview of national regulatory responses to cryptocurrencies. This section will categorise regulations as having either no regulation, or restrictive, neutral or promotive jurisdictions. The chapter will then provide some concluding remarks on current cryptocurrency regulation.

2.2 International and Regional Regulatory Responses

At the international level, the regulatory responses to cryptocurrency have comprised of the issuance of reports, guidance and manuals based on the specific remit areas of relevant international organisations. These shall be examined in turn, starting with the International Monetary Fund (IMF).

2.2.1 International Monetary Fund (IMF)

The primary role of the IMF is to ensure the stability of the international monetary and financial system, including exchange rates, international payments and macroeconomic policy.[1] With this in mind, the IMF has a view on harnessing

[1] International Monetary Fund, 'About' (*IMF* 2018) <https://www.imf.org/en/About> Accessed 19 June 2018.

the innovative potential cryptocurrencies and their underlying blockchain technology, highlighting the different ways in which they can benefit the global economy.[2] However, this optimism is tempered by an awareness of the regulatory challenges posed by cryptocurrencies. Whilst initially stating that cryptocurrencies pose no systemic risk,[3] the IMF has expressed concern about issues such as money laundering and terrorist financing, with a cautionary note to central banks on the competitive pressure cryptocurrencies are likely to exert on demand for fiat currency in the future being issued in 2018.[4] Rather than advocating a prohibitive stance, these warnings are expressed as a call to adopt and adapt to new technology, including exploring the development of central bank-issued digital currency,[5] supported by a suitable regulatory response. In this regard, IMF's former Managing Director, Christine Lagarde, described cryptocurrency regulation as inevitable, calling for an international approach to regulation and 'proper supervision'.[6] Elaborating on this proposed proper supervision, Lagarde opined that this should focus less on entities and instead be more activity-based, focusing on 'who is doing what, and whether they're properly licensed and supervised';[7] she further stated that cryptocurrency's own blockchain technology might provide the most suitable approach to their regulation.[8] The approach advocated by the IMF can therefore be summarised as

[2] E Shulze, ''We Are about to See Massive Disruptions': IMF's Lagarde Says it's Time to Get Serious about Digital Currency' <*CNBC* 13 October 2017) <https://www.cnbc.com/2017/10/13/bitcoin-get-serious-about-digital-currency-imf-christine-lagarde-says.html> Accessed 19 June 2018.

[3] International Monetary Fund, 'Virtual Currencies and Beyond: Initial Considerations' IMF Staff Discussion Note 3 2016) <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf> Accessed 19 June 2018

[4] D He, 'Monetary Policy in the Digital Age' (2018) *Finance and Development* Vol 55.2 <http://www.imf.org/external/pubs/ft/fandd/2018/06/central-bank-monetary-policy-and-cryptocurrencies/he.pdf> Accessed 3 July 2018.

[5] C Lagarde, 'Winds of Change: The Case for New Digital Currency' (2018) Singapore Fintech Festival Speech <https://www.imf.org/en/News/Articles/2018/11/13/sp111418-winds-of-change-the-case-for-new-digital-currency> Accessed 14 January 2020.

[6] Z Alkhalisi, 'IMF Chief: Cryptocurrency Regulation is inevitable' (*CNNMoney* 11 February 2018) <http://money.cnn.com/2018/02/11/investing/lagarde-bitcoin-regulation/index.html> Accessed 19 June 2018

[7] ibid.

[8] C Lagarde, 'Addressing the Dark Side of the Cryptoworld' (*IMF Blog,* 13 March 2018) <https://blogs.imf.org/2018/03/13/addressing-the-dark-side-of-the-crypto-world/> Accessed 3 July 2018.

the promotion of an 'even-handed regulatory agenda' that 'protects against risks without discouraging innovation'.[9]

In addition to a balanced approach aimed at harnessing and leveraging the technology behind cryptocurrencies for the public good, whilst addressing their risks, the IMF has called for a unified global response to cryptocurrency regulation, and stated that greater international discussion and cooperation is needed in order to address the regulatory challenges posed by cryptocurrencies.[10] This echoes concerns raised in the IMF's initial considerations report around cryptocurrencies, where the challenges of asserting jurisdiction in light of the cross-border reach of the technology were noted.[11]

2.2.2 G20 and Financial Stability Board (FSB)

Similar calls for a concerted international approach to cryptocurrency-related regulation were raised by countries during the 2018 G20 group and nations meeting in Argentina,[12] and the 2018 World Economic Forum in Davos—where, in particular, French president Emmanuel Macron called for the establishment of a 'global contract for global investment' aimed at arriving at an international approach to cryptocurrency regulation. [13]

[9] C Lagarde, 'An Even-Handed Approach to Cryptoassets' (*IMF Blog*, 16 April 2018) <https://blogs.imf.org/2018/04/16/an-even-handed-approach-to-crypto-assets/> Accessed 3 July 2018.

[10] S Hagan and A Mayeda, 'IMF Calls for Global Talks on Cryptocurrencies' (*Bloomberg* 18 January 2018) <https://www.bloomberg.com/news/articles/2018-01-18/imf-calls-for-global-talks-on-digital-fx-as-bitcoin-whipsaws> Accessed 19 June 2018.

[11] International Monetary Fund (n 3). <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf> Accessed 27 May 2016.

[12] G20, 'Communiqué of the First G20 Meeting of Finance Ministers and Central Bank Governors of 2018' (*G20* 20 March 2018) <https://back-g20.argentina.gob.ar/sites/default/files/media/communique_g20.pdf> Accessed 19 June 2018.

[13] N De, 'World Leaders are Talking Crypto at Davos' (*Coindesk* 25 January 2018) <https://www.coindesk.com/may-lagarde-mnuching-davos-bitcoin-roundup/> Accessed 20 June 2018.

During the summit, the members of the G20 set a deadline for taking the first steps toward unified regulations for cryptocurrencies. [14] In addition to this, they stated their commitment to implementing the FATF's anti-money laundering (AML) and counter-terrorist financing (CTF) standards, as well as their commitment to abide by OECD's Base Erosion and Profit Shifting framework, aimed at developing new profit allocation concepts for taxing the digital economy by 2020.[15] This proactive stance differs slightly from that of the FSB, which coordinates financial regulation for the G20 Economies. The FSB has resisted calls from some G20 members to regulate cryptocurrencies. Instead, under the chairmanship of the Bank of England (BOE)'s Mark Carney, the FSB's initial assessment has been that, due to the fact that cryptocurrencies do not pose risks to global financial stability at this time, attention should be focused away from regulation and redirected towards international coordination aimed at 'plug[ing] data gaps in monitoring the rapidly evolving cryptocurrency space'.[16] It remains to be seen whether or not the commitments and assertions made during the 2018 G20 summit will result in more concrete and coordinated responses to the regulation of cryptocurrencies. However, the statement does provide some indication of the rising awareness of the jurisdictional challenges presented by cryptocurrencies.

2.2.3 Organisation for Economic Co-operation and Development (OECD)

The OECD, which was formed to be 'a forum in which governments can work together to share experiences and seek solutions to common problems',[17] has sought to position itself as the best-placed forum to harmonise global cryptocurrency regulation. Citing current ongoing initiatives, such as the OECD Responsible Business Conduct Committee and the joint OECD/G20 Taskforce on

[14] G20 (n 12).

[15] ibid.

[16] H Jones, 'G20 Watchdog Focuses on Rules Review, Hold Fire on Cryptocurrencies' (*Reuters* 18 March 2018) <https://www.reuters.com/article/us-g20-regulations-carney/g20-watchdog-focuses-on-rules-review-holds-fire-on-cryptocurrencies-idUSKBN1GU0SF> Accessed 19 June 2018.

[17] OECD, 'Our Mission' (*OECD* 2018) <http://www.oecd.org/about/> Accessed 19 June 2018.

Financial Consumer Protection, the OECD has expressed its intention to play a coordinating role in the global regulation of cryptocurrencies.[18]

The OECD's three recommendations on policy responses to cryptocurrencies were highlighted in a March 2018 presentation. Firstly, it was recommended that regulators be proactive and forward-looking, in order to avoid knee-jerk reactions resulting in regulators intervening before fully understanding the technology. Secondly, that regulators need to keep up to date with the rapid developments and new DLT applications, and build their capacity to deal with and understand these developments. Finally, the recommendations state that there must be coordination on two fronts: collaboration amongst key stakeholders including industry, academic and consumer groups, and international coordination in light of the fact that 'the global nature and inter-connectedness of markets call for international co-operation to avoid regulatory fragmentation, curb incentives for regulatory arbitrage, and spread best practice'.[19] In both recommended approaches, emphasis was placed on the use of global industry standards, where the OECD hopes to play a key role 'due to its ability to provide a forum for exchange of views across a wide range of policy areas, develop relevant international standards and guidance and provide capacity building to both members and partners'.[20]

The intention to help shape the future direction of global cryptocurrency regulation is well founded, given the OECD's past influence on regulation. In 2014, the OECD published its initial assessment of cryptocurrency in a working paper entitled, 'The Bitcoin Question: Currency versus Trust-less Transfer Technology'.[21] In addition to highlighting the consumer protection risks

[18] G Medcraft, 'The OECD and the Blockchain Revolution' (*OECD*, Presentation at the OECD Friends of Going Digital Meeting, Paris 29 March 2018) <http://www.oecd.org/parliamentarians/meetings/meeting-on-the-road-london-april-2018/The-OECD-and-the-Blockchain-Revolution-Presentation-by-Greg-Medcraft-delivered-on-29-March-2018.pdf> Accessed 30 June 2018.

[19] ibid.

[20] ibid.

[21] A Blundell-Wignall, 'The Bitcoin Question: Currency versus Trust-less Transfer Technology' (2014), *OECD Working* Papers *on Finance, Insurance and Private Pensions*, No 37.

associated with cryptocurrencies, and the potential benefits found in the separation of cryptocurrency from its underlying technology, the paper concluded with several policy recommendations including:

- A general ban on any form of use of cryptocurrencies in the clearing system between banks and the central bank, to ensure that the monetary system is not undermined;
- Some form of agreement for best practice registration that permits consumer protection, tax and anti-laundering authorities to verify the owner's identity;
- Balance-sheet reporting and income statements for all networks, and other appropriate regulations to ensure a level playing field;
- Some amount of capital should be held by exchanges on the balance sheet for fraud and technological failures;
- The use of government plenary powers to close down all non-complying networks. [22]

As one of the first official statements on cryptocurrency, the report paved the way for the separation between cryptocurrency and the underlying blockchain and DLT; it reiterated consumer protection, money laundering and tax evasion threats posed by cryptocurrency, and informed regulatory policy such as capital adequacy requirements and reporting requirements targeted at cryptocurrency exchanges and wallet providers. In addition to offering a platform to coordinate a global approach to cryptocurrency regulation, the OECD—like the IMF—has recognised the use of blockchain and DLT to tackle international policy issues, including facilitating the automatic trade of information between tax authorities and anti-money laundering[23] and seeks to use these in order to develop practical tools aimed at addressing regulatory challenges posed by cryptocurrencies.[24]

[22] ibid.

[23] Medcraft (n 18).

[24] OECD, 'OECD Secretary General Report to G20 Financial Ministers and Central Bank Governors' (*OECD,* Argentina March 2018) <https://www.oecd.org/tax/OECD-Secretary-General-tax-report-G20-Finance-Ministers-Argentina-March-2018.pdf> Accessed 2 July 2018.

2.2.4 Financial Action Task Force (FATF)

In addition to the OECD, the FATF—whose objective is to set standards relating to combating money laundering, terrorist financing and other related threats[25]—was also one of the first organisations to present a regulatory opinion on cryptocurrencies. In 2015, the FATF issued a report providing guidance on a risk-based approach to virtual currencies. This guidance was aimed at explaining the application of a risk-based strategy to AML and CFT measures in the cryptocurrency context; identifying the entities involved in what they called 'Virtual Currency (VC) payment products and services'; and clarifying the application of the relevant FATF recommendations to convertible virtual currency exchangers.[26] In these guidelines, the FATF's recommendations were to focus on institutions and intermediaries that provide gateways and points of intersection with the regulated financial system, including exchanges, and applying relevant AML and CFT requirements to these institutions.[27] In this way, this guidance, along with that of the OECD, shaped the way for national regulatory approaches based almost exclusively on targeting cryptocurrency exchanges and wallet providers for AML/CFT purposes.

Coordinating its efforts with organisations such as the G20, the FATF (as well as other regulatory bodies) has expressed concern about 'the current patchwork regulatory framework across different countries [which] can be exploited by criminals, stifle innovation and create uncertainty'.[28] As such, the FATF is advancing the development of a global approach through its standardisation mandate, specific to AML and CFT. Beyond advocating for an institution-centric risk-based approach to addressing the AML and CFT risks poses by cryptocurrencies, the FATF has also started considering the use of similar

[25] FATF, 'Who We Are' (*FATF* 2018) <http://www.fatf-gafi.org/about/> Accessed 2 July 2018.
[26] FATF, 'Guidance for a Risk-Based Approach: Virtual Currencies' (FATF June 2015) <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf> Accessed 19 June 2018.
[27] ibid.
[28] FATF, 'FATF Report to the G20 Finance Ministers and Central Bank Governors' (*FATF* March 2018) <http://www.fatf-gafi.org/media/fatf/documents/FATF-G20-FM-CBG-March-2018.pdf> Accessed 19 June 2018.

technology in order to operationalise regulatory objectives. In this case, the FATF is 'considering if further action is necessary to fully exploit the opportunities presented for digital ID to improve the efficiency and effectiveness of customer due diligence measures',[29] displaying a growing trend in line with the IMF and the OECD towards technology-enhanced regulation.

2.2.5 Bank of International Settlements (BIS)

The BIS's mandate is to 'serve central banks in their pursuit of monetary and financial stability, to foster international cooperation in those areas and to act as a bank for central banks'.[30] Their position on cryptocurrencies was presented by Managing Director, Agustín Carstens, in a February 2018 speech in which he highlighted the potential role of central banks in the digital age.[31] Highlighting the case for policy intervention and regulation—due to concerns about consumer and investor protection, tax evasion, money laundering and criminal financing—the BIS's view on the systemic implications of cryptocurrency is similar to that of the IMF: that cryptocurrencies do not yet pose systemic risk. However, the BIS includes the warning that 'if authorities do not act pre-emptively, cryptocurrencies could become more interconnected with the main financial system and become a threat to financial stability'.[32] Further warnings have been provided for central banks to safeguard payment systems in light of cryptocurrency's linkages to and reliance on existing institutional infrastructure such as bank accounts. With this in mind, the BIS advised that authorities apply the principles of the Basel Process, in order to ensure that 'the same high standards that money transfer and payment service providers have to meet are also met by Bitcoin-type exchanges' so that 'legitimate banking and payment

[29] ibid.

[30] Bank for International Settlements, 'About BIS' (*Bank for International Settlements* 2018) <https://www.bis.org/about/index.htm?m=1%7C1> Accessed 3 July 2018.

[31] A Carstens, 'Money in the Digital Age: What Role for Central Banks?' (*Bank of International Settlements* 6 February 2018) <https://www.bis.org/speeches/sp180206.pdf> Accessed 3 July 2018. 9.

[32] ibid.

services are only offered to those exchanges and products that meet these high standards'.[33]

In this way, the BIS's recommendations and observations are consistent with the pervasive institution-centric approach to cryptocurrency regulation targeted at exchanges and wallet providers (conceptualised here as non-bank financial institutions) that need to be regulated in a like-for-like manner, with the same regulation for the same risk without exceptions. More specific guidance on cryptocurrency regulation beyond the application of the above-mentioned application of the Basel Committee on Banking Supervision[34] principles were presented in the context of overall considerations of the effects of financial technology (fintech) on banks and bank supervision. Here, the increased need for cooperation, internal capacity of bank supervisors, the opportunities of supervisory technology (suptech), the examination of existing regulatory frameworks and the facilitation of innovation were all presented.[35] Regarding the need for cooperation, the BIS has recommended that 'supervisors should coordinate supervisory activities for cross-border fintech operations, where appropriate' and that 'supervisors should learn from each other's approaches and practices and consider whether it would be appropriate to implement similar approaches or practices'.[36]

Also falling under the purview of the BIS is the Committee on Payments and Market Infrastructure (CPMI) which 'promotes the safety and efficiency of payment, clearing, settlement and related arrangements, thereby supporting financial stability and the wider economy'.[37] In 2015, the CPMI launched a sub-

[33] ibid.

[34] The Basel Committee on Banking Supervision (BCBS) is the primary global standard setter for the prudential regulation of banks and provides a forum for regular cooperation on banking supervisory matters. See <https://www.bis.org/bcbs/> Accessed 3 July 2018.

[35] Basel Committee on Banking Supervision, 'Sound Practices: Implications of Fintech Developments for Banks and Bank Supervisors' (*Bank of International Settlements* August 2017) <https://www.bis.org/bcbs/publ/d415.pdf> Accessed 3 July 2018.

[36] ibid 7.

[37] Bank for International Settlements (BIS) 'CPMI—Overview' (*Bank for International Settlements* 2018) <https://www.bis.org/cpmi/about/overview.htm?m=3%7C16%7C691> Accessed 6 August 2018.

group on digital currencies within its working group on retail payments aimed at identifying their key features and implications for central banks. The key contribution by the CPMI was the conceptualisation of cryptocurrencies as payment systems which enabled the identification of risk categories associated with traditional retail payment systems and payment instruments, including operational risks. More specifically, the CPMI opined that 'many of the risks that are relevant to e-money and other electronic payment instruments are also relevant to digital currencies', and secondly, identified that 'the development of distributed ledger technology is an innovation with potentially broad applications… extending beyond payments'[38]. As such, CPMI recommended that central banks continue monitoring and analysis the implications of both digital currencies and DLT.[39] In this way, the CPMI's opinion has informed national regulatory approaches that fall under the neutral category of this study, as shall be discussed below, including like-for-like regulation and the wait-and-see approach.

2.2.6 International Organisation of Securities Commissions (IOSCO)

IOSCO—the global standard-setter for securities regulation[40]—issued a statement to its members regarding the risks of cryptocurrencies and initial coin offerings (ICOs).[41] Prior warnings on the risks posed by cryptocurrencies to investors were issued in its Global Securities Risk Outlook, where increased complexity, legal ambiguity and misunderstanding of risk designed were cited amongst potential risks to investors. [42] In addition to highlighting risks and collating national approaches, IOSCO's board has also established a Consultation

[38] Committee on Payments and Market Infrastructures (CPMI) 'Digital Currencies' (*Bank for International Settlements,* November 2015) <https://www.bis.org/cpmi/publ/d137.pdf> Accessed 6 August 2018. 1.

[39] ibid.

[40] IOSCO, 'About IOSCO' (*IOSCO* 2018) <https://www.iosco.org/about/?subsection=about_iosco> Accessed 19 June 2018.

[41] IOSCO, 'IOSCO Board Communication on Concerns Related to Initial Coin Offerings (ICOs) (*IOSCO*/MR/01/2018 18 January 2018) <http://www.iosco.org/news/pdf/IOSCONEWS485.pdf> Accessed 19 June 2018.

[42]IOSCO, 'Securities Markets Risk Outlook' (*IOSCO*2016) <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD527.pdf> Accessed 19 June 2018.

Network, through which ‘members can discuss their experiences and bring their concerns, including any cross-border issues, to the attention of fellow regulators’.[43] This initiative will be supported by the development of ‘a Support Framework to assist members as they consider how to address the domestic and cross-border issues stemming from coin offerings that could impact investor or consumer protection’ and a FinTech Network ‘to help the sharing of information, knowledge, and experiences related to FinTech among its members.[44]

In this way, IOSCO’s approach regarding cryptocurrency regulation differs from that of other international regulatory bodies, in that it does not provide substantive guidance and recommendations on regulatory responses, but rather focuses on providing a platform for the sharing of best practice by global regulators, and ensuring the dissemination of information about the risk profile of cryptocurrencies.

2.2.7 European Union (EU)

The European Commission is still reviewing its regulatory framework for cryptocurrencies. In this regard, the Joint Committee of the European Supervisory Authorities for securities (ESMA), banking (EBA), and insurance and pensions (EIOPA) issued a blanket warning to consumers regarding the risks of cryptocurrencies. [45] More comprehensively, in 2004, the EBA published a list of 70 risks connected with investing in digital currencies, and has advised that consumers should only buy virtual currencies if they are aware of the risks.[46]

[43] IOSCO (n 41) 1.
[44] IOSCO, ‘IOSCO Annual Conference Focuses on Key Challenges Facing Securities Regulators’ (*IOSCO*/MR/13/2018 10 May 2018) <https://www.iosco.org/news/pdf/IOSCONEWS497.pdf> Accessed 19 June 2018. 2.
[45] ESMA, ESAs Warn Consumers of Risks in Buying Virtual Currencies’ (*ESMA* February 12, 2018) <https://www.esma.europa.eu/press-news/esma-news/esas-warn-consumers-risks-in-buying-virtual-currencies> Accessed 3 July 2018.
[46] EBA, ‘Opinion on ‘Virtual Currencies’ (*EBA* 2014) <http://www.eba.europa.eu/documents/10180/657547/EBA-Op-201408+Opinion+on+Virtual+Currencies.pdf> Accessed 19 June 2018.

More specific regulations have been put in place by ESMA, which has proposed restrictions on derivatives tied to virtual currencies for retail investors, including rules on leverage ratios specific to cryptocurrency Contracts for Differences (CFDs), [47] and is also assessing how the EU's new MiFID II rules are relevant to cryptocurrencies.[48] In addition to this, in 2016, the EBA proposed establishing a separate regulatory regime specific for cryptocurrency to support anti-money laundering efforts.[49] This proposed regime was put in place to consider 'proposals to bring custodian wallet providers (CWPs) and virtual currency exchange platforms (VCEPs) within the scope of the Directive (4AMLD) as obliged entities'.[50] If adopted, this would require cryptocurrency wallet providers and exchange platforms to have in place policies to prevent and report money laundering and terrorist financing, and to adhere to fit and proper testing under registration and licensing requirements.[51] This approach—focusing on wallet providers and exchange platforms for AML and CFT purposes, combined with licensing requirements based on function—is consistent with that of the BIS, FATF and the OECD.

With regards to the ECB, the initial stance taken in 2012 was that the cryptocurrency industry was too immature to regulate.[52] The ECB has recently reiterated its view that regulation currently falls outside the scope of the Bank's

[47] ESMA, 'Additional Information on the Agreed Product Intervention Measures Relating to Contracts for Differences and Binary Options' (*ESMA* 35-43-1000 27 March 2018) <https://www.esma.europa.eu/sites/default/files/library/esma35-43 1000_additional_information_on_the_agreed_product_intervention_measures_relating_to_contracts_for_differences_and_binary_options.pdf> Accessed 3 July 2018.

[48] The Markets in Financial Instruments Directive is the EU legislation that regulates firms who provide services to clients linked to 'financial instruments' (shares, bonds, units in collective investment schemes and derivatives), and the venues where those instruments are trade. See <https://www.esma.europa.eu/policy-rules/mifid-ii-and-mifir> Accessed 3 July 2018.

[49]EBA, 'Opinion of the European Banking Authority on the EU Commission's proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849 (4AMLD)' (*EBA* -Op-2016-07 11 August 2016) <https://www.eba.europa.eu/documents/10180/1547217/EBA+Opinion+on+the+Commission%E2%80%99s+proposal+to+bring+virtual+currency+entities+into+the+scope+of+4AMLD> Accessed 3 July 2018.

[50] ibid 2.

[51] ibid.

[52] European Central Bank (ECB), 'Virtual Currency Schemes' (ECB 2012) <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> Accessed 19 June 2018.

powers, stating that 'with regard to its own tasks in the field of payment systems, price stability and financial stability, the ECB does not see a need to amend or expand the current EU legal framework related to these tasks'.[53] Since then, there has been a call to review whether the regulatory and oversight tools in the field of trading, clearing and settlement require updating, in light of risks to financial market infrastructure, should a major incident involving cryptocurrency lead to contagion.[54] However, the prevailing view remains that cryptocurrency pose no systemic risk.

Finally, the EU has announced the creation of an international consortium that seeks to diminish the use of cryptocurrencies and the dark web by criminals. This support has led to the establishment of a new project called TITANIUM (Tools for the Investigation of Transactions in Underground Markets). Spearheaded by an association consisting of fifteen members, seven of who are from European countries, TITANIUM's goal is to curtail criminals and attackers from using blockchain technology to avoid law detection, while at the same time respecting the privacy rights of legitimate users.[55] This initiative—to prevent criminal use of the dark web and virtual currencies—is the first global attempt (outside of Interpol[56] and initiatives by the UNDOC[57]) to address the use of cryptocurrency to fuel criminal activity on the dark web in a collaborative and multi-jurisdictional manner.

[53] European Central Bank (ECB), 'Virtual Currency Schemes—a further analysis' (*ECB* February 2015) <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> Accessed 3 July 2018. 32.

[54] Y Mersch, 'Virtual or Virtueless? The Evolution of Money in the Digital Age' (*ECB* 8 February 2018) <https://www.ecb.europa.eu/press/key/date/2018/html/ecb.sp180208.en.html> Accessed 3 July 2018.

[55] European Commission, 'Project to Prevent Criminal Use of the Dark Web and Virtual Currencies launched by International Consortium' (*European Commission* 1 June 2017) <https://cordis.europa.eu/news/rcn/141335_en.html> Accessed 3 July 2018.

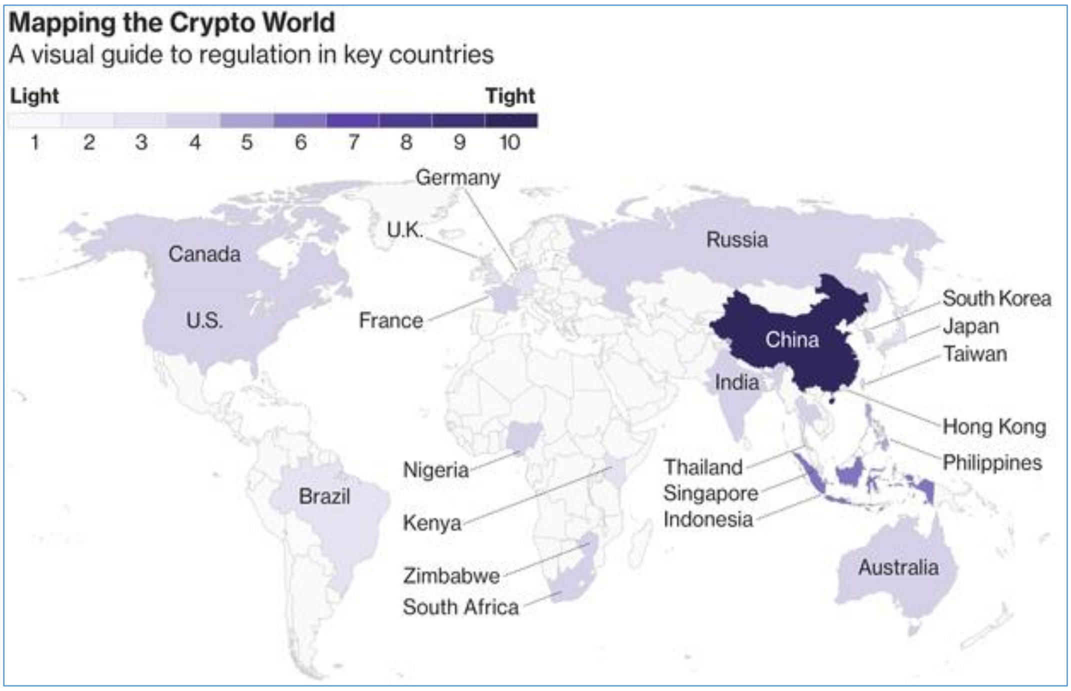
[56] Interpol, 'Interpol Holds First DarkNet and Cryptocurrencies Working Group' (*Interpol* 3 April 2018) <https://www.interpol.int/News-and-media/News/2018/N2018-022> Accessed 3 July 2018.

[57] UNDOC, 'UNDOC Delivers the First Cryptocurrency Investigation Training Course in Latin America' (*UNDOC* 19 January 2018) <https://www.undoc.org/unodc/en/drug-trafficking/crimjust/news/unodc-delivers-the-first-cryptocurrency-investigation-training-course-in-latin-america.html> Accessed 3 July 2018.

2.3 National Regulatory Responses

Drawing, in part, from the guidance of international regulatory bodies, national regulation of cryptocurrencies differs from country to country. An overview of these approaches reveals that there is a spectrum along which each jurisdiction can be classified, ranging from no regulation and light regulation, to tight and restrictive regulation. This spectrum has been investigated by Bloomberg, amongst others, which developed a visual guide to cryptocurrency regulation in key countries, as illustrated in Figure 2 below. This guidance is based on research around the legal status of cryptocurrency exchanges, cryptocurrency payments, ICOs, conversions from cryptocurrency to fiat, currency bans, planned legislation to control cryptocurrencies and warnings issued about cryptocurrencies.[58]

Figure 2: Cryptocurrency Regulation Spectrum



Source: Bloomberg[59]

[58] Bloomberg, 'What the World's Governments are saying about Cryptocurrencies' (*Bloomberg News* March 26, 2018) <https://www.bloomberg.com/news/articles/2018-03-26/what-the-world-s-governments-are-saying-about-cryptocurrencies> Accessed 3 July 2018.
[59] ibid.

Responses to these questions were used to rate key jurisdictions' regulatory approach on a scale of one to ten, from light regulation in countries such as the UK, Brazil and Kenya, to China and Indonesia displaying the tightest regulations of jurisdictions examined. Further attempts to categorise cryptocurrency regulation by jurisdiction along a spectrum has been conducted by Bitlegal,[60] using the broad categories of 'permissive', 'contentious' and 'hostile', by considering how cryptocurrency is regulated, where cryptocurrency is legal, how cryptocurrency is taxed, and how cryptocurrency intermediaries are regulated.

While the categories given by Bloomberg, Bitlegal and other organisations are instructive, what follows is a broader overview of national regulatory responses, providing examples under the categories of jurisdictions with no regulation, restrictive regulation, neutral regulation and promotive regulation. This categorisation will allow for a more nuanced overview of national cryptocurrency regulation in particular, by highlighting the implications of the differences between countries that are actively promoting and attracting or, inversely, actively suppressing the use of cryptocurrencies, and those jurisdictions which are taking a technologically neutral/agnostic approach to cryptocurrency regulation. These shall be discussed in turn below.

2.3.1 Jurisdictions with No Regulation

This category consists of jurisdictions which have made no regulatory announcements on cryptocurrencies, and those whose announcements consist exclusively of issuing warnings over the use of cryptocurrency. It also includes jurisdictions with no stated cryptocurrency regulation who have issued announcements that can be classified as taking a wait-and-see approach. Whilst very little can be said of jurisdictions where the regulators have issued no statements whatsoever about cryptocurrencies—mostly in developing countries

[60] Bitlegal, 'Interactive Map' (*Bitlegal* 2017) <http://bitlegal.io/> Accessed 3 July 2017.

in Africa, Asia and South America—some insight can be gained from jurisdictions where the absence of regulation is qualified by the issuing of warnings and the justifications of a wait-and-see approach.

2.3.1.1 Issuing of Warnings

The issuing of warnings can be seen as a first-step strategy for jurisdictions that have yet to define a regulatory approach to cryptocurrencies, as well as an accompaniment to regulations where they do exist. In the absence of regulation, these warnings have not only consisted of cautionary notes to consumers and investors, but also to financial institutions with potential exposure to cryptocurrencies as well—for example, the warnings issued in France by the French Financial Market Authority (Autorité des Marchés Finaciers, AMF), the Prudential Supervisory Authority (Autorité de Contrôle Prudentiel et de Resolution, ACPR) and the French Central Bank (Banque de France). Here, emphasis has been placed on the unregulated nature of cryptocurrencies which are not considered to be financial instruments under French law, and therefore fall outside the purview of the AMF.[61] Further warnings have been issued by the ACPR and Banque de France about the volatility of cryptocurrencies and their potential use in money laundering and terrorist financing.[62] Statements by national regulatory authorities issuing warnings have been both general to the use of cryptocurrencies, like those given in France, or specific to a particular aspect of cryptocurrency use. In Germany, the Federal Financial Supervisory Authority, BaFin, issued a warning specific to ICOs.[63] Here, consumers have been warned about the risks of ICOs, including the risk of loss, the lack of protection, insufficient information, complexity, volatility, fraud risk and lack of regulation.[64] This is similar to the warnings given by the Australian Securities and Investment

[61] N Boring, 'France' in 'Regulation of Cryptocurrencies in Selected Jurisdictions' (*The Law Library of Congress* June 2018) <http://www.loc.gov/law/help/cryptocurrency/regulation-of-cryptocurrency.pdf> Accessed 6 July 2018.
[62] ibid.
[63] BaFin, 'Initial Coin Offerings: High Risk for Consumers' (*BaFin* 15 November 2017) <https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2017/fa_bj_1711_ICO_en.html;jsessionid=F880FC5388DF54C0EE1A65D0AC63407A.1_cid290> Accessed 3 July 2018.
[64] ibid.

Commission, which states that '[t]he exchange platforms on which you buy and sell digital currencies are not regulated, so if the platform fails or is hacked, you will not be protected and will have no legal recourse'.[65]

In Argentina, warnings have been issued for relevant national regulatory institutions to be 'attentive and diligent' when it comes to cryptocurrencies. Here, the Unidad de Información Financiera (Financial Information Unit) of the Ministry of Finance in Argentina issued a resolution in 2014, which warned entities required by law to report suspicious transactions involving money laundering or terrorism financing to be 'particularly alert' with regard to operations carried out with virtual currency.[66] Similarly, in Brazil, regulatory authorities have emphasised the fact that cryptocurrencies are not regulated. Here, the Brazilian Central Bank (Banco Central do Brasil, BACEN) stated that:

> *companies that negotiate or store virtual currencies on behalf of their owners, be they persons or companies, are neither regulated, licensed to operate, nor supervised by BACEN; there is no specific provision governing virtual currencies in the legal and regulatory frameworks associated with the National Financial System; and BACEN, in particular, neither regulates nor supervises transactions involving virtual currencies*[67]*.*

Instead, BACEN issued a warning in 2017 about the risks associated with cryptocurrencies, reiterating that these are neither issued nor guaranteed by any monetary authority.

[65] Australia Securities and Investments Commission, 'Cryptocurrencies' (*ASIC* June 2018*)* <https://www.moneysmart.gov.au/investing/investment-warnings/virtual-currencies> Accessed 6 July 2018.

[66] G Roderiquez-Ferrand, 'Argentina' in 'Regulation of Cryptocurrencies in Selected Jurisdictions' (*The Law Library of Congress* June 2018) <http://www.loc.gov/law/help/cryptocurrency/regulation-of-cryptocurrency.pdf> Accessed 6 July 2018.

[67] Banco Central do Brasil (BACEN), '*Virtual Currencies'* (*BACEN* Communiqué 31, 379 16 November 2017) <http://www.bcb.gov.br/ingles/norms/> Accessed 6 July 2018. 1.

2.3.1.2 Wait-and-See Approach

Wait-and-see approaches can be seen in instances where warnings are qualified and punctuated by the description of the infant-industry state of cryptocurrencies, and the stated intent to put in place regulation based on how the market develops. The Reserve Bank of Australia (RBA) has taken the stance that:

> *digital currencies are currently in limited use and do not yet raise any significant concerns with respect to competition, efficiency or risk to the financial system; and are not currently regulated by the RBA or subject to regulatory oversight.*[68]

However, taking a wait-and-see approach, the RBA indicated that it 'would be assessing whether the current regulatory framework could accommodate alternative mediums of exchange such as digital currencies'.[69] This approach is taken in recognition of what Australian regulators have described as the need for increased monitoring of cryptocurrency in order to better understand how they operate, in anticipation of greater public adoption, prior to regulation.[70] Another leading jurisdiction taking a wait-and-see approach is the UK, which currently has no regulation for cryptocurrencies. The BOE has stated that cryptocurrencies do not as yet pose any risks to monetary and financial stability, and are not yet systemically significant to warrant regulation, although they will continue to be monitored.[71] Similarly, the UK's Financial Conduct Authority (FCA) has no regulations in place for cryptocurrencies.[72] Instead, the FCA has issued warnings

[68] Reserve Bank of Australia (RBA), 'Submission to the Enquiry into Digital Currency' 1 (*Reserve Bank of Australia* September 2014) < https://www.rba.gov.au/publications/submissions/financial-sector/pdf/inquiry-digital-currency-2014-11.pdf> Accessed 6 July 2018. 9.

[69] ibid.

[70] Australian Transaction and Analysis Centre (AUSTRAC), 'Draft AML.CTF Rules' (*AUSTRAC* 2 July 2018) <http://www.austrac.gov.au/draft-aml-ctf-rules> Accessed 6 July 2018.

[71] Bank of England, 'Digital Currencies' (*Bank of England* 22 August 2018) <https://www.bankofengland.co.uk/research/digital-currencies> Accessed 11 November 2018.

[72] H Murphy, ''Wild West' Crypto-Asset Markets Need UK Regulation, say MPs' (*The Financial Times* 19 September 2018) <https://www.ft.com/content/dbea3cac-bb3c-11e8-8274-55b72926558f> Accessed 11 November 2018.

on cryptocurrency derivatives and ICOs, stating that many ICOs will fall outside of the regulatory space.[73]

2.3.2 Jurisdictions with Restrictive Regulations

The first category of jurisdictions restrictive to cryptocurrencies are those that have made it illegal to use cryptocurrencies, issue ICOs and crypto-derivatives, and operate cryptocurrency intermediaries. These restrictions can be either blanket restrictions, instituting the banning of all cryptocurrency-related activities, or targeted restrictions, permitting some whilst restricting other cryptocurrency-related activities.

China is the most prominent amongst jurisdictions that have issued blanket restrictions on cryptocurrencies and cryptocurrency-related activities. In China, running or operating an ICO is prohibited, with regulators calling for individuals and organisations to reimburse any funds generated in that manner.[74] This ban on ICOs followed a similar ban on all cryptocurrency to fiat exchanges operating in China and offshore, as well as a ban on banks dealing in cryptocurrency.[75] In place since 2013, this ban states that:

> *banks and payment institutions in China must not deal in Bitcoins; use Bitcoin pricing for products or services; buy or sell Bitcoins; or provide direct or indirect Bitcoin-related services, including registering, trading, settling, clearing, or other services. They are also prohibited from accepting Bitcoins or using Bitcoins as a clearing tool, or trading Bitcoins with Chinese yuan or foreign currencies.*[76]

[73] Financial Conduct Authority (FCA), 'Initial Coin Offerings' (*FCA* 12 September 2017) <https://www.fca.org.uk/news/statements/initial-coin-offerings> Accessed 6 July 2017.

[74] K Vaswani, 'China Bans Initial Coin Offerings Calling Them 'Illegal Fundraising'' (*BBC* News 5 September 2017) <https://www.bbc.co.uk/news/business-41157249> Accessed 3 July 2018.

[75] K Rapoza, 'Cryptocurrency Exchanges Officially Dead in China' (*Forbes* 2 November 2017) <https://www.forbes.com/sites/kenrapoza/2017/11/02/cryptocurrency-exchanges-officially-dead-in-china/#3631935d2a83> Accessed 3 July 2018.

[76] L Zhang, 'China' in 'Regulation of Cryptocurrencies in Selected Jurisdictions' (*The Law Library of Congress* June 2018) <http://www.loc.gov/law/help/cryptocurrency/regulation-of-cryptocurrency.pdf> Accessed 6 July 2018.

Similar prohibition of banks dealing with cryptocurrency have been imposed in India[77] and Iran, preventing all financial institutions from handling cryptocurrencies.[78]

Another jurisdiction with a blanket ban on cryptocurrencies is Pakistan, where the State Bank of Pakistan announced it 'has not authorised or licensed any individual or entity for the issuance, sale, purchase, exchange or investment in any such Virtual Currencies/Coins/Tokens in Pakistan', and further stated that:

> *all Banks / DFIs / Microfinance Banks and Payment System Operators (PSOs) /Payment Service Providers (PSPs) are advised to refrain from processing, using, trading, holding, transferring value, promoting and investing in Virtual Currencies/Tokens [or facilitating] their customers/account holders to transact in VCs/ICO Tokens.*[79]

Other countries where cryptocurrency use is banned are Indonesia, Algeria, Bangladesh, and Kyrgyzstan, although it has been suggested that this is likely to change following the declaration of cryptocurrency as *halal* under Sharia law in April 2018.[80] Cryptocurrency use is also explicitly prohibited in Zimbabwe, Thailand, Vietnam, Bangladesh, Taiwan and Bolivia.[81]

[77] P Motiani, 'Your Bank Will Not Allow You to Buy Bitcoin Anymore' (*The Economist* 6 April 2018) <https://economictimes.indiatimes.com/wealth/personal-finance-news/your-bank-will-not-allow-you-to-buy-bitcoins-anymore/articleshow/63627123.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst> Accessed 6 July 2018.

[78] L Nasseri, 'Iran's Central Bank Imposes Ban on Cryptocurrency Transactions' (*Bloomberg* April 23, 2018) <https://www.bloomberg.com/news/articles/2018-04-23/ban-on-cryptocurrency-transactions-imposed-by-iran-central-bank> Accessed 6 July 2018.

[79] State Bank of Pakistan, 'Prohibition of Dealing in Virtual Currency/Tokens' (*State Bank of Pakistan* BPRD Circular No 03 of 2018 6 April 2018 <http://www.sbp.org.pk/bprd/2018/C3.htm> Accessed 17 July 2018.

[80] A Cuthbertson, 'Bitcoin Market Opens to 1.6 Million Muslims as Cryptocurrency Declared Halal Under Islamic Law' (*Independent* 13 April 2018) <https://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-islamic-law-muslims-cryptocurrency-market-permissible-sharia-news-price-surge-a8302761.html> Accessed 18 October 2018.

[81] P Bajpai, 'Countries Where Bitcoin is Legal and Illegal' (*Investopedia* 11 October 2018) <https://ww.investopedia.com/articles/forex/041515/countries-where-bitcoin-legal-illegal.asp> Accessed 18 October 2018.

2.3.2.1 Motivations behind the bans

The case of South Korea provides some insight into motivations for restrictive regulatory approaches vary. Here, there was growing concern about the ‘speculative mania’ around cryptocurrencies, where Bitcoin prices in South Korea were 50 per cent higher than those in America, and the *won* accounted for more than 10 per cent of trade in Bitcoin for most of the second half of 2017.[82] Similarly, regulators intervened with more restrictive measures after cryptocurrency was selling at a premium in the country, and because of an ongoing liquidity crisis. In this case, as was the case in Nigeria after the unpegging of *naira*, macroeconomic policy around capital flight was being circumvented by the use of cryptocurrency.

In Iran, a ban was issued, as authorities were working to control both the official and unauthorised currency markets as the country unified its official and unregulated rates in order to prevent further weakening of the *rial* in April 2018, amid Iranians’ fear of a return of economic sanctions banning the country from using the money-transfer messaging system SWIFT, as part of sanctions over its nuclear programme.[83]

In some instances, bans are issued whilst the country is simultaneously developing its own central bank-issued digital currency. Despite cracking down on privately-issued cryptocurrencies, China’s central bank, the PBOC, is reportedly considering issuance of its own digital currency, having completed trial runs on the algorithms needed for a digital currency supply, ‘taking it a step closer to addressing the technological challenges associated with digital currencies’.[84] In this way, some of these jurisdictions are not anti-cryptocurrency per se—they are more concerned with control of cryptocurrency, harnessing its

[82] Bloomberg, ‘Why the Cryptocurrency World is Watching South Korea’ (*Bloomberg News* 2 February 2018) <https://www.bloomberg.com/news/articles/2018-02-04/why-the-cryptocurrency-world-is-watching-south-korea-quicktake> Accessed 3 July 2018.

[83] L Nasseri (n 77).

[84] W Yanfei, ‘PBOC Inches Closer to Digital Currency’, (*China Daily* 14 October 2017) <http://www.chinadaily.com.cn/business/2017-10/14/content_33235955.htm> Accessed 6 July 2018.

benefits for the state and maintaining state monopoly over the generation of value and subsequently, monetary and fiscal policy.

2.3.2.1 Targeted Restrictions and Stringent Restrictions

Targeted restrictions allow some cryptocurrency activity but not others. One such jurisdiction is South Korea, where deposits to cryptocurrency-linked bank accounts are disallowed, and where ICOs were banned in September 2017.[85] Whilst regulators are considering the extension of this ban to cryptocurrency exchanges, these are, as yet, still permitted to operate.[86]

An additional variation to blanket bans in restrictive regimes is the putting in place of highly stringent regulations. One such jurisdiction is the state of New York in the US. The New York Department of Financial Services was the first state to propose bespoke regulation of cryptocurrencies in July 2014, releasing a comprehensive framework for regulating digital currency firms operating in the state of New York, called the Bitlicense.[87]Containing a comprehensive and wide-reaching regulatory framework including consumer protection, anti-money laundering compliance, and cyber security rules tailored for digital currency companies—as well as bank-level requirements to apply for a license, including fiat-equivalent deposit insurance—the Bitlicense is widely recognised as the most stringent and restrictive cryptocurrency regulatory regime in the world.[88]

2.3.3 Neutral Jurisdictions

Unlike restrictive jurisdictions where cryptocurrencies are expressly prohibited, regulatory initiatives in neutral jurisdictions neither ban nor promote the use of cryptocurrency. As in the case of Canada, in these jurisdictions, '[y]ou can use

[85] Bloomberg (n 81).

[86] ibid.

[87] New York Department of Financial Services (*NYDFS* 2015), 'BitLicense Regulatory Framework' <https://dfs.ny.gov/legal/regulations/bitlicense_reg_framework.htm> Accessed 3 July 2018.

[88] J Weiczner, 'Inside New York's Bitlicense Bottleneck: An 'Absolute Failure'? (*Fortune* 25 May 2018) <http://fortune.com/2018/05/28/bitcoin-cryptocurrency-new-york-bitlicense/> Accessed 6 July 2018.

digital currencies to buy goods and services on the Internet and in stores that accept digital currencies' and 'you may also buy and sell digital currency on open exchanges, called digital currency or cryptocurrency exchanges'.[89] This permission to use cryptocurrency can be seen to be premised on the use of like-for-like regulation, applying similar rules and regulations for similar existing financial products and services. This form of neutral regulation can be seen in the areas of taxation, the regulation of cryptocurrency intermediaries, and the regulation of cryptocurrency securities.

2.3.3.1 Taxation

The first category in which a like-for-like regulation of cryptocurrencies can be observed is in their tax treatment. In most jurisdictions, the tax authorities were the first amongst all regulators to provide cryptocurrency regulation. In Argentina, the tax treatment of cryptocurrency corresponds with the treatment of profits on securities and bonds, where profited derived from the sale of cryptocurrencies is seen as income, and is taxed as such, at 15 per cent when derived from either Argentine or foreign sources.[90] Similarly, the Australian Taxation Office—well in advance of the first parliamentary enquiry on cryptocurrencies in 2015—had already produced several public rulings regarding different aspects of the tax treatment of cryptocurrencies, holding that transactions involving such currencies should be treated in a similar manner to barter arrangements for the purposes of income tax.[91]

Further jurisdictions employing like-for-like regulation in taxation of cryptocurrencies include South Africa, where the South African Revenue Service (SARS) stated that 'there is an existing tax framework that can guide SARS and affected taxpayers on the tax implications of cryptocurrencies, making a separate

[89] Financial Consumer Agency of Canada, 'Digital Currency' (*Financial Consumer Agency of Canada*, 19 January 2018) <https://www.canada.ca/en/financial-consumeragency/services/payment/digital-currency.html> Accessed 6 July 2018.
[90] G Roderiquez-Ferrand (n 65).
[91] K Buchanan, 'Australia' in 'Regulation of Cryptocurrencies in Selected Jurisdictions' (*The Law Library of Congress* June 2018) <http://www.loc.gov/law/help/cryptocurrency/regulation-of-cryptocurrency.pdf> Accessed 6 July 2018.

Interpretation Note unnecessary for now'.[92]More specifically, in this case, 'normal income tax rules' (including Capital Gains Tax) apply to profit from cryptocurrency through mining activities, with further tax liability similar to barter transactions (where cryptocurrencies are exchanged for goods and services) and normal cash transactions (where cryptocurrencies are exchanged for fiat currency through exchange).[93] Similar to other jurisdictions, cryptocurrency is exempt from VAT in South Africa. In the USA, the Internal Revenue Service (IRS) clarified the tax treatment of virtual currency transactions in 2014. Here, it was stated that general tax principles applicable to property transactions apply to transactions using virtual currency.[94] This like-for-like approach in the USA is similar to that of multiple jurisdictions which have defined cryptocurrency as property for tax purposes. In sum, whilst the regulatory frameworks governing the taxation of cryptocurrencies differ significantly depending on whether or not cryptocurrencies are defined as currency, property, or assets, each jurisdiction deploys a similar approach to similar categories of taxable goods and services.

2.3.3.2 Intermediaries—Money Service and Money Transfer Rules

The like-for-like treatment of cryptocurrencies for regulatory purposes is also evident in the application of Money Service Business (MSB) and Money Transmitter (MT) rules to cryptocurrency intermediaries. This equivalent approach is instituted by the requirement that cryptocurrency exchanges and wallet providers apply for an MSB or a MT license, similar to those needed by agencies such as Western Union and MoneyGram, before they are allowed to operate. In addition to meeting the requirements to obtain a licence, these entities must also adhere to the concomitant requirements around AML and CTF,

[92] South African Revenue Service (SARS), 'SARS' Stance on the Tax Treatment of Cryptocurrencies' (*South African Revenue Service* 6 April 2018) <http://www.sars.gov.za/Media/MediaReleases/Pages/6-April-2018---SARS-stance-on-the-tax-treatment-of-cryptocurrencies-.aspx> Accessed 6 July 2018.

[93] ibid.

[94] Internal Revenue Service, 'Internal Revenue Bulletin: 2014-16' (*IRS* 14 April 2014) <https://www.irs.gov/irb/2014-16_IRB#NOT-2014-21> Accessed 6 July 2018.

mainly consisting of Know-Your-Customer(KYC) customer identity verification, record-keeping rules and Suspicious Activity Reporting.[95]

For example, in France, it is stated that 'entities that habitually engage in the activity of purchasing or selling cryptocurrencies in exchange for actual legal tender must be licensed as payment services providers by the ACPR'[96] and, in Australia, cryptocurrency exchanges operating in Australia 'need to register with the relevant regulatory body, implement an AML/CTF programme, maintain certain records, and report suspicious transactions'.[97]The majority of Mt using the application of pre-existing MSB and MT rules has taken place in the US. Here, at the federal level, the Department of Treasury Financial Crimes Enforcement Network (FinCEN) invokes the Bank Secrecy Act of 1970 (BSA) and the USA Patriot Act of 2011 to require cryptocurrency exchanges to register as MSBs, and comply with the accruing AML and CTF requirements. According to FinCEN (2013), this licensing requirement applies to any 'administrator or exchanger that (1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency for any reason' and, in so doing, meets the FinCEN definition of a Money Transmitter, a category of MSB. In addition to FinCEN MSB licensing and registration, some states require additional Money Transmitter Licensing, with more locally defined legal obligations.

This has formed the basis of the majority of enforcement action related to cryptocurrency intermediaries. In 2015, Ripple Labs Inc settled criminal and civil allegations for BSA violations. Ripple Labs violated several requirements of the BSA 'by acting as a Money Services Business (MSB) and selling its virtual currency without first registering with the Financial Crimes Enforcement Network (FinCEN) and by failing to implement an adequate AML and CFT programming'.[98]

[95] Financial Action Task Force, 'Guidance for a Risk-Based Approach: Virtual Currencies' (FATF June 2015) <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf> Accessed 7 June 2016.
[96] Boring (n 61) 34.
[97] Buchanan (n 91) 5.
[98] FinCEN, 'FinCEN Fines Ripple Labs Inc in First Civil Enforcement Action Against a Virtual Currency Exchanger (5 May 2015) <https://www.fincen.gov/news_room/nr/html/20150505.html> Accessed 7 June 2016

Further cases in which BSA violations took place include *United States v Murgio*[99] and *United States v Lebedev* ,[100] where Murgio and Lebedev allowed customers to exchange cash for bitcoins, knowing that their customers were transacting in the proceeds of criminal activity, and exchanged cash for bitcoins for victims of cyber-attacks, in which criminals had blocked access to a victim's computer system until a bitcoin ransom was paid.

A further example of the application of MSB and MT laws is the 2014 amendment of Canada's Proceeds of Crime (Money Laundering) and Terrorist Financing Act to include 'regulating those dealing in digital currencies as money services businesses, so that they are subject to record keeping verification procedures, suspicious transaction reporting, and registration requirements'.[101] Other jurisdictions are still at the formulation stages in the application of similar laws. In the EU, plans are being made by the EU Commission to push forward the implementation of the 4th Anti-Money Laundering Directive (4AMLD) with tabled amendments to include the regulation of cryptocurrency exchanges under both 4AMLD and the Payment Services Directive.[102]

2.3.3.3 Intermediaries—Consumer Protection Laws

Beyond regulations targeted at AML and CFT, further regulation to do with consumer protection—put in place to address the risks involved with cryptocurrency—can also be seen as a form of like-for-like regulation. In the US, these concerns are addressed more at the state level, with the most robust requirements having been issued by the New York Department of Financial

[99] *United States v Murgio,* No 15-CR-769 (AJN) (SDNY 21 April 2016) <https://casetext.com/case/united-states-v-murgio> Accessed 27 January 2020

[100] *United States v Lebedev*, No 17-3691 (2d Cir 2019) <https://law.justia.com/cases/federal/appellate-courts/ca2/17-3691/17-3691-2019-07-26.html> Accessed 27 January 2020.

[101] Financial Transactions Reports and Analysis Centre of Canada, 'FINTRAC Advisory Regarding Money Services Businesses Dealing in Virtual Currency (July 2014) <http://www.canafe-fintrac.gc.ca/new-neuf/avs/2014-07-30-eng.asp> Accessed 7 June 2016.

[102] European Commission, 'Communication from the Commission to the European Parliament and the Council on an Action Plan to for Strengthening the Fight Against Terrorism Financing' (COM 50/2 2016) <http://ec.europa.eu/justice/criminal/files/com_2016_50_en.pdf> Accessed 7 June 2016.

Services's Bitlicense, which draws from existing consumer protection laws applicable to other financial service providers. These include having a board-approved cybersecurity programme, which includes the employment of a qualified Chief Information Security Officer; the protection of consumers by providing initial and per transaction disclosures of risks, terms and conditions, complaints policies and disclosures, advertising and marketing requirements; the safeguarding of assets through the holding of capital, surety bonds and full reserves for custodial assets; and becoming subject to exams, reports and oversight, including reporting of transactions exceeding a certain amount and a customer identification programme.[103]

A similar state-based (or, in this case, province-based) approach is taken in Canada, where in particular, Ontario and British Columbia have applied the Ontario Consumer Protection Act and the British Columbia Business Practices and Consumer Protection Act respectively, to cryptocurrency-related activities.[104] An example of enforcement action based on consumer protection law is *FTC v BF Labs Inc,* where the US Federal Trade Commission (FTC) filed a complaint against Butterfly Labs for unfair and deceptive marketing practices, after customers were coaxed into pre-ordering specialised computers which were either not delivered, or delayed in delivery until the machines became obsolete, in violation of Section 5 of the FTC Act.[105] Of further relevance here is the US Consumer Financial Protection Bureau's 2013 consumer protection regulation of remittance transfers that applies to some transactions by cryptocurrency payment transaction executors.[106]

[103] New York Department of Financial Services (n 86).

[104] M Burgonye, 'Canadian Provincial Bitcoin Law: It's All about Protecting the Consumer' (*Coindesk* 23 December 2013) <https://www.coindesk.com/canadian-bitcoin-law-consumer-protection> Accessed 7 June 2016.

[105] *Federal Trade Commission v BF Labs Inc et al,* 201No 4:14-cv00815- BCW (WD Mo Apr 16) <https://www.ftc.gov/enforcement/cases-proceedings/142-3058/bf-labs-inc> Accessed 21 January 2020.

[106] S Hughes and S Middlebrook, 'Advancing a Framework for Regulating Cryptocurrency Payments Intermediaries' [2015] 32 Yale J on Reg.

2.3.3.4 Securities Regulation

The final area in which like-for-like regulations towards cryptocurrencies have been implemented is in the regulation of cryptocurrency derivatives, including options, futures, swaps, CFDs, ICOs and other cryptoassets. The US is notable in this regard, through the application of the Howey Test, to ascertain whether or not ICO tokens can be classified as securities in order for Securities Exchange Commission (SEC) rules to be applied in a like-for-like manner.[107] Similar 'financial instrument tests' have been put in place by the government of Malta, which has put in place an extensive regulatory framework for cryptocurrencies, with a like-for-like approach being deployed in the treatment of cryptoassets.[108]

In jurisdictions where cryptoassets and ICOs have been classified as securities, the relevant existing securities regulations apply. In France, it was concluded that 'cash-settled cryptocurrency contracts may qualify as a derivative' and that, as a result,

> *online platforms which offer cryptocurrency derivatives fall within the scope of MiFID 2 [the European Union Markets in Financial Instruments Directive 2] and must therefore comply with the authorisation, conduct of business rules, and the European Market Infrastructure Regulation (EMIR) trade reporting obligation to a trade repository.*[109]

Notable instances involving securities regulation are the US SEC's charges against Erik T Voorhees and Ethan Burnside, respectively, for failure to register Bitcoin-related securities offerings. In a settlement order involving Erick Voorhes,

[107] W Hinmah, 'Digital Asset Transactions: When Howey Met Gary (Plastic)' (*SEC* 14 June 2018) <https://www.sec.gov/news/speech/speech-hinman-061418> Accessed 11 November 2018.

[108] Malta Financial Services Authority (MFSA), 'Discussion Paper on Initial Coin Offerings, Virtual Currencies and Related Service Providers' (*MFSA* 11 January 2018) <https://www.mfsa.com.mt/pages/readfile.aspx?f=/files/Announcements/.../2017/> Accessed 11 November 2018.

[109] Autorité des Marchés Financiers (AMF), 'The AMF Considers that the Offer of Cryptocurrency Derivatives Requires Authorization and that it is Prohibited to Advertise such Offer via Electronic Means' (News Release *AMF* 22 February 2018) <https://www.amf-france.org/en_US/Actualites/Communiques-de-presse/AMF/annee-2018?docId=workspace://SpacesStore/a225bf1d-de35-4f58-89e3-f03cb7e9e551> Accessed 6 August 2018.

Voorhes admitted to publicly offering unregistered securities, raising 50,600 bitcoins (worth USD$722,659 at the time) by selling 13 million shares to the public.[110] Similarly, the SEC brought administrative charges against programmer Ethan Burnside for the unlawful operation of two online platforms used to trade securities using virtual currencies, essentially operating a 'virtual stock exchange' without registration, in violation of Section 5 of the Exchange Act.[111]

2.3.4 Promotive Jurisdictions

Promotive jurisdictions are those which actively seek to promote the use of cryptocurrencies, with the strategic view of developing vibrant cryptocurrency markets and attracting investment in this industry. Examples of these jurisdictions, which also state the intention of harnessing the potential of cryptocurrency's underlying blockchain technology, include Belarus, Gibraltar, Malta, Estonia, Madagascar and Switzerland.

In 2018, Belarus declared itself to be the first jurisdiction in the world to have comprehensive regulation of businesses based on blockchain technology, and the first country in the world to legalise smart contracts at the national level. This was done through the issuing of a Presidential Decree on the development of the digital economy, which took effect on 28 March 2018. The Decree created a legal framework for buying, selling, exchanging, creating, and mining cryptocurrencies and tokens. The provisions of this decree extend only to legal entities operating on the territory of the High Technologies Park—a Special Economic Zone. Described as 'legal experiment', residents of the High Technologies Park are permitted to use smart contracts and elements of English contract law, such as convertible loans, options, clauses of indemnity, and non-solicitation and

[110] Securities and Exchange Commission, 'SEC Charges Bitcoin Entrepreneur With Offering Unregistered Securities' (*SEC* 3 June 2014) <https://www.sec.gov/news/press-release/2014-111#.U49HUPldV8G> Accessed 6 July 2018.

[111] Securities and Exchange Commission, 'SEC Sanctions Operator of Bitcoin-Related Stock Exchange for Registration Violations' <https://www.sec.gov/news/press-release/2014-273> Accessed 6 July 2018.

noncompetition agreements, to create a 'venture ecosystem'.[112] The decree is also seen as legally significant due to its provision of definitions, at a legislative level, of cryptocurrencies, tokens, smart contracts and blockchain technology, with the latter being defined broadly to encompass other digital information systems with elements of centralisation.[113] According to Reuters, 'the decree is designed to attract digital coin entrepreneurs, who are moving businesses to locations more welcoming to cryptocurrencies as they face intensifying scrutiny from regulators'.[114]

Also classified as promotive are jurisdictions that are putting in place regulatory sandboxes and innovation hubs. Leading the field in this is in the UK's FCA which, in 2014, launched an innovation hub 'focused on encouraging innovation in financial services in the interests of consumers by supporting innovator businesses with a range of services'.[115]In its first year, amongst other achievements, the innovation hub 'helped over 175 innovative businesses' and 'worked with government on plans to introduce regulation for digital currencies'.[116] This is in line with the innovation hub's objectives to support innovator businesses through activities such as helping 'non-regulated businesses understand more about [the FCA's] regulatory framework and what it means for them',[117] and engagement with innovative businesses in order to understand more about their needs, products and services.[118] Following up from the launching of the innovation hub, the FCA published a report in 2015 on the feasibility and practicalities of developing a regulatory sandbox that is a 'safe space' in which businesses can test innovative products, services, business

[112] N Isajanyan, 'Belarus' in 'Regulation of Cryptocurrencies in Selected Jurisdictions' (*The Law Library of Congress* June 2018) <http://www.loc.gov/law/help/cryptocurrency/regulation-of-cryptocurrency.pdf> Accessed 6 July 2018. 17.

[113] I Chelyshava, 'Belarus Cryptocurrency Experiment: Why the World Should Take Notice' (*Jurist* Academic Commentary, 10 January 2018) <http://jurist.org/forum/2018/01/Iryna-Chelyshava-Belarus-cryptocurrency.php> Accessed 6 July 2018.

[114] A Makhovsky, 'Belarus Adopts Crypto-Currency Law to Woo Foreign Investors' (*Reuters* 22 December 2017) Accessed 6 July 2018.

[115] Financial Conduct Authority, 'Innovation Hub' (*FCA* 2018) <https://innovate.fca.org.uk/innovation-hub/objectives-innovation-hub> Accessed 6 July 2018

[116] ibid.

[117] ibid.

[118] ibid.

models and delivery mechanisms without immediately incurring all the normal regulatory consequences of engaging in the activity in question'.[119]

Having opened for its first round of applications on 9 May 2016,[120] the sandbox allowed unauthorised firms to apply for restricted authorisation 'to allow testing by firms who need to become authorised to trial their new products or services',[121] with restrictions only being lifted once the firm is able to meet 'full' requirements. Companies operating in the cryptocurrency industry, arguably at the forefront of fintech, have joined the Innovation Hub. The UK's regulatory sandbox is an innovative regulatory model that has attracted the attention and interest of other regulatory authorities around the world. Jurisdictions that have followed suit in establishing their own cryptocurrency regulatory sandboxes and innovation hubs include Singapore, South Africa, Australia, Hong Kong, Malaysia, Indonesia, Netherlands, Denmark and Canada.[122]

2.4 Conclusion

The aim of this chapter has been to provide an overview of both international and national responses to the regulation of cryptocurrencies. The first section of the chapter described the international regulatory environment for cryptocurrencies. This was based on the analysis of the recommendations, warnings, opinions and statements of international organisations, whose mandates and purview include and intersect with the issues of regulatory concern raised by cryptocurrencies. This section has shown that, whilst there is variation in the emphasis of regulation depending on institutional mandate, there are three significant themes in the recommendations on cryptocurrency regulation. The first theme is the concerted call for a global approach to the regulation of cryptocurrencies, in line with a recognition of the need for

[119] ibid.
[120] ibid.
[121] ibid.
[122] FinExtra, 'The Role of Regulator Sandboxes in Fintech Innovation' (*FinExtra* 10 September 2018) <https://www.finextra.com/blogposting/15759/the-role-of-regulatory-sandboxes-in-fintech-innovation> Accessed 11 November 2018.

combined supra-jurisdictional oversight to ensure regulatory effectiveness and the role of these institutions in standards-setting. The second theme observable in the recommendations of international organisations is the identification of cryptocurrency intermediaries (exchange and wallet providers) as the sole regulatory targets, and the advocating of like-for-like regulation based on the functions performed by these institutions. The final theme observed in this analysis is an increasing awareness of the potential use of the technology itself as a regulatory tool and mechanism, as stated by both the IMF and the BIS, and, as observable in the enforcement-oriented initiatives of the TITANIUM project, the UNDOC and Interpol.

Following on from this, the second section of the chapter focused on national approaches to the regulation of cryptocurrencies. These have been categorised as jurisdictions with (a) no regulation, (b) restrictive regulations, (c) neutral regulation, and (d) promotive regulations. With regards to jurisdictions with no regulation, it has been found that these have issued statements providing warnings around the use of cryptocurrencies. Also in this category are jurisdictions that have adopted a wait-and-see approach, in light of the emerging nature of the cryptocurrency industry. The second classification used in this chapter is that of restrictive jurisdictions. This category has included jurisdictions that have issued bans making cryptocurrency use illegal, as well as jurisdictions that have put in place relatively restrictive regulations towards the cryptocurrency market. In the third category of jurisdictions, it has been noted how neutrality in cryptocurrency regulation consists of the application of like-for-like rules and regulations, without distinguishing cryptocurrency financial products, services and institutions from similar products, services and institutions. In this instance, examples of like-for-like regulation included the similar application of tax laws, MSB/MT laws, consumer protection laws and securities laws. The final category of national regulatory approaches identified is that of promotive jurisdictions. These are areas where the use of cryptocurrencies is actively encouraged and supported through regulation.

The regulated financial products, regulated activities and regulated institutions can be summarised succinctly, as I have presented them below, in Figure 3.

Figure 3: Regulated Financial Products, Activities and Institutions

Regulated Financial Products	Regulated Activities	Regulated Institutions
•Cryptocurrency •Crypoassets (cryptocurrency securities) •Initial Coin Offerings (cryptocurrency tokens)	•Storing •Exchanging •Remitting (transmitting) •Payments •Trading	•Exchanges •Wallet Providers •Payment Processors •Remittance Services

What follows, in Chapter 3, is an examination and evaluation of both these international and national approaches to the regulation of cryptocurrencies, with a focus on enforcement and compliance challenges, in order to highlight the need for an alternative regulatory response.

Chapter Three: Evaluation of Current Regulation

3.1 Introduction

This chapter is aimed at highlighting the shortcomings of current cryptocurrency regulation, in order to show why there is a need for an alternative regulatory approach. This will be done firstly by discussing the enforcement challenges regulators face when existing substantive laws are applied to cryptocurrencies. Thereafter, the chapter will discuss the compliance challenges faced by the cryptocurrency industry when seeking to adhere to existing regulation. The chapter will then conclude by discussing the need for an alternative approach to cryptocurrency regulation, with an emphasis on what such an approach must be able to address in order to be fit for purpose.

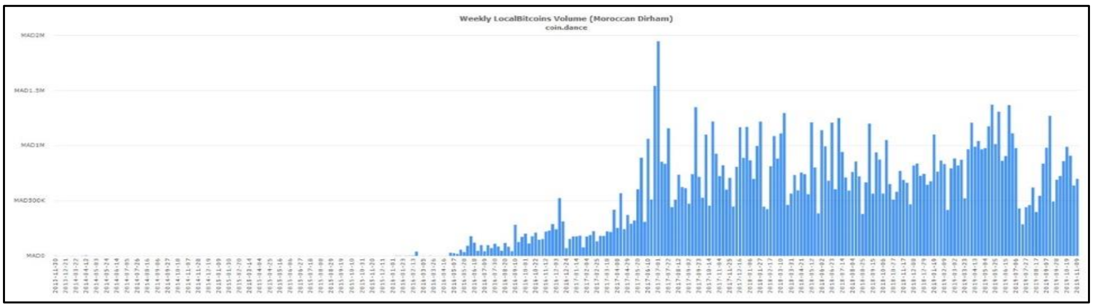
3.2 Enforcement Challenges

The first observation that can be made about the current approach to cryptocurrency regulation, at both the global and national levels, is regarding the obstacles to enforcement. More specifically, banning restrictions are circumvented by peer-to-peer (P2P) and distributed exchanges (DEX); AML, KYC and CFT regulations are curtailed by blockchain pseudonymity and anonymity; all other regulatory actions are made difficult by the decentralised and distributed nature of cryptocurrencies, which present challenges to do with establishing jurisdiction and arbitrage. These three challenges will be discussed in turn.

3.2.1 Peer-To-Peer and Distributed Exchanges

As discussed in the preceding chapter, restrictive jurisdictions have attempted to curtail the use of cryptocurrency, by making it illegal to possess and transact in cryptocurrency, not permitting banks and financial institutions to facilitate cryptocurrency transactions, and disallowing citizens from trading in cryptocurrency within national borders.[1] However, continued increases in cryptocurrency trading volumes, and cryptocurrency-driven market activity indicate that these restrictions have been largely ineffective. Examples of this can be seen in Pakistan and Morocco. As has previously been alluded to, the State Bank of Pakistan (SBP) banned investment and trading in cryptocurrencies, ordering the country's only cryptocurrency exchange, Urudubit, to shut down in April 2018. However, despite this crackdown, in the immediate aftermath of the prohibition commentators stated that 'banning or not banning makes no difference for the time being as there are no means to track people who want to trade in cryptocurrencies'.[2] This is partly due to the existence of P2P and DEXs. In particular, Morocco, which also has a cryptocurrency ban in place, has an active LocalBitcoins cryptocurrency market. As displayed in Figure below, trade in cryptocurrency peaked at nearly 2 million Moroccan *dirhams* (MAD) in the first week of July 2017, and at the time of writing[3], the weekly volume was MAD637, 819. Similar active trade is evident in other banned jurisdictions, including Bolivia and Vietnam.[4]

Figure 4: Weekly Local Bitcoins Volume (Moroccan Dirhams)



Source: Coindance[5]

[1] Library of Congress, 'Regulation of Cryptocurrency around the World' (2019) <https://www.loc.gov/law/help/cryptocurrency/world-survey.php> Accessed 8 November 2019.

[2] U Hanif, 'As Pakistan Bans Cryptocurrencies, People May Find Alternative Means' (*Tribune* 13 May 2018) <https://tribune.com.pk/story/1708782/2-pakistan-bans-cryptocurrencies-people-may-find-alternative-means/> Accessed 3 July 2018.

[3] November 2019.

[4] ibid.

[5] Data from Coindance <https://coin.dance/volume/localbitcoins/MAD> Accessed 8 November 2019.

Local Bitcoins is a popular P2P cryptocurrency exchange, where those who wish to purchase cryptocurrency can do so without having to provide any documentation verifying their identity. In the sporadic instances where traders do request for identification (ID) verification before buying, this requirement changes 'from country to country and trader to trader'.[6] Another example of a P2P cryptocurrency exchange is Bisq. Bisq is an open-source P2P application that allows users to buy and sell cryptocurrencies in exchange for national currencies.[7] Users can download the Bisq application with no ID verification required prior to use. In this way, these services allow for the purchase, selling and exchange of cryptocurrencies to fiat directly between two parties over an online platform. The loose or entirely absent requirements for customer ID effectively means that any person intent on acquiring or selling cryptocurrency anonymously can do so, by forum shopping and targeting traders who waive ID requirements.[8] In this way, P2P exchanges and DEX undermine and, in effect, void the AML and CFT regulations currently in place for cryptocurrency exchange services, whilst additionally providing a means by which to circumvent any existing bans on cryptocurrency use imposed by regulators.

Beyond P2P and DEX, there has been some successful enforcement action on cryptocurrency exchanges. For example, in the US, BTC-e (a now-defunct cryptocurrency exchange) and Alexander Vinnick were indicted in July 2019 for money laundering, operating an unlicensed exchange and unlawful money services business, and other related charges.[9] Similarly, in South Korea, the Korea Communication Commission (KCC) fined eight local cryptocurrency exchanges for insufficiently protecting users' personal data.[10] However, these enforcement

[6] LocalBitcoins, 'About LocalBitcoins.com' (*LocalBitcoins* 2019) <https://localbitcoins.com/about> Accessed 8 November 2019.

[7] Bisq, 'Bisq Network' (2019) <https://bisq.network/> Accessed 8 November 2019.

[8] Local Bitcoins (n 6).

[9] *United States of America v BTC-e a/k/a Canton Business Corp and Alexander Vinnik*, United States District Court, Northern District of California, San Francisco Division, No 3:19-CV-04281 (ND Cal Jul 25, 2019).

[10] Y Lee, 'Penalties Imposed on 8 Cryptocurrency Exchanges… Violation of 'Not Enough Privacy Measures' (*Byline Network* 24 January 2018) <https://byline.network/2018/01/1-997/> Accessed 8 November 2019.

actions were made possible by the fact that the named exchanges were centralised entities with dedicated operators. However, P2P and DEX are completely decentralised, enabling cryptocurrency holders to trade freely on their own terms, without the ID requirements that are essential to ensuring compliance with AML and CFT regulations. These requirements are also vital in assessing the robustness of the data protection and other consumer protection-related safeguards leaving consumers trading on P2P and DEX particularly vulnerable.

This enforcement challenge to cryptocurrency regulation is particularly significant when the volumes of transactions and trades occurring through P2P platforms are considered. In the UK alone, survey data showed that 47 per cent of respondents acquired their bitcoin primarily through P2P and brokerage services, with 41.7 per cent of these doing so through LocalBitcoins.[11] Along with the regulatory implications (particularly for AML) of local trades being conducted in cash, these are also often carried out face-to-face, and without any escrow facility in place, further jeopardising consumer protection. The reach of current cryptocurrency regulation extends only towards centralised exchanges. P2P and DEX—which function exclusively online—lie beyond the reach and limits of current regulation.

3.2.2 Pseudonymity and Anonymity

Closely associated with the regulatory enforcement challenges presented by P2P and DEXs are the obstacles to regulation resulting from pseudonymity and anonymity. In this instance, enforcement is made difficult by the fact that there are no explicit identity markers for cryptocurrency users. This is because each individual trading in cryptocurrency does so, not through a traditional bank

[11] Coinjournal, 'Bitcoin Usage in the UK' (*Coinjournal* 2015) <http://coinjournal.net/bitcoin-usage-in-the-uk/> Accessed 8 November 2019.

account assigned to a known individual, but through public wallets, which are a string of randomly assigned letters and numbers displayed on a blockchain.[12]

More specifically, as discussed in Chapter 1, cryptocurrencies operate on public, permission-less blockchains, characterised by decentralisation and pseudonymity. This makes it difficult—in some instances, impossible¯to track and trace the parties of cryptocurrency transactions. As explained by Matonis, in instances where cryptocurrency is released via smart contract,[13] it is infeasible to restrict private party contracts that do not require the judicial system due to 'cryptographic protocols and smart contracts with time-release amounts and multisignature transactions'.[14] Moreover, where smart contracts are banned by statute within restrictive jurisdictions, this 'would probably only drive them underground'.[15] An example of technically enabling transactions to go underground are privacy coins or anonymous cryptocurrencies such as Dash, Monero, Zcash, PIVX, Verge and Namecoin.[16] As explained by Tziakouris of Interpol, Monero, Dash, Zcash and other privacy coins enable users to keep their activity history and balances private, which ultimately restricts law enforcement investigators from identifying and tracing suspicious transactions.[17] This is done using methods such as stealth addresses to obfuscate the origins, amounts, and destinations of transactions and protocols, such as the Zerocoin protocol that converts public Personal Identity Verification (PIV) into anonymous PIV, to

[12] S Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (*Unpublished Manuscript* 2008).

[13] Smart contracts use computer programming to automatically execute the terms of a contract by using 'if-then' statements that lead to the execution of a corresponding contractual clause when a pre-programmed condition is triggered. Smart contracts shall be further discussed in Chapter 5.

[14] J Matonis, 'Why the OECD Needs to do its Homework on Cryptocurrencies' (*Coindesk* 1 July 2014) <https://www.coindesk.com/oecd-needs-homework-bitcoin/> Accessed 3 July 2018.

[15] ibid.

[16] A Batabyal, '10 Best Privacy Coins in 2019' (*Coinswitch* 7 June 2019) <https://coinswitch.co/news/10-best-privacy-coins-in-2019-latest-review> Accessed 8 November 2019.

[17] G Tziakouris, 'Cryptocurrencies—A Forensic Challenge or Opportunity for Law Enforcement? An INTERPOL Perspective' [2018] IEEE Security and Privacy 13(4).

conceal the pseudo-identity of the sender, or any traces that can lead to the sender's real identity.[18]

This technical capability to prevent traceability can be enhanced by the use of what are known as 'tumblers' and 'mixers'. Cryptocurrency mixing and tumbling services prevent the tracing of transactions to a particular wallet by resending the equivalent amount of other people's cryptocurrency sent to them by the wallet owner at random intervals.[19] This allows them to 'clean' coins tainted by association with certain websites or addresses, and makes it difficult for law enforcement to follow their transactions. [20] Whilst these evasive mechanisms are fairly technologically sophisticated, there are simpler means by which cryptocurrency regulations can be avoided. For example, in China, cryptocurrency investors seeking to by-pass the country's restrictive cryptocurrency regulations and access exposure to ICOs simply use middle-men agencies available on Wechat[21] to facilitate their transactions.[22]

When cryptocurrency transactions cannot be linked to individuals, this enables and facilitates criminal cyber activity, including the use of ransomware and the purchase of illicit goods and services online. Closely linked to this enforcement challenge is the existence of the Dark Web and Tor Network, that enable anonymous communication, as described in Chapter 1. The difficulty in tracking and tracing cryptocurrency users[23] makes it challenging to enforce AML and CFT

[18] ibid.

[19] Cryptalker, '9 Best Bitcoin Tumbler (Mixer) Services' (*Cryptalker* 2009) <https://cryptalker.com/best-bitcoin-tumbler/> Accessed 8 November 2019.

[20] Tziakouris (n 16).

[21] Wechat is a popular Chinese messaging application.

[22] S Haig, 'Chinese Investors Use Wechat Brokers to Bypass ICO Ban' (*Bitcoin.com* 30 March 2018) <https://news.bitcoin.com/chinese-investors-use-wechat-brokers-bypass-ico-ban/> Accessed 3 July 2018.

[23] Whilst privacy coins and tumbler services make cryptocurrency transactions nearly impossible to track, it is difficult—but possible—to identify the owners of cryptocurrency public keys, as is seen by the work of companies such as Elliptic <https://www.elliptic.co/> and the success in tracking Ross Ulbricht in 2013 and later, Thomas White of Silk Road <https://www.theguardian.com/technology/2019/apr/12/uk-man-jailed-guiding-mind-behind-silk-road-drugs-site-dark-web> Accessed 8 November 2019.

regulations in a similar manner to which these regulations are enforced with regards to fiat currency.

3.2.3 Jurisdiction and Arbitrage

An additional enforcement challenge presented by cryptocurrencies has to do with establishing jurisdiction and regulatory arbitrage. Establishing jurisdiction with cryptocurrency is a key regulatory challenge, due to the fact that cryptocurrencies are generated and transferred online between pseudonymous parties, providing the ability to transact from anywhere in the world. As explained by He, Habermeiser and others, 'asserting jurisdiction over a particular VC transaction, market participant, or scheme may prove challenging for national regulators in light of the cross-border reach of the technology'.[24] For example, Paech highlights how the methods traditionally used to determine which law should apply to the question of attribution (law of the place of asset *lex rei sitae,* the law of either the acquirer or the disposer, and the law of the issuer) would be problematic where cryptocurrency is involved. This is because it would lead to numerous different laws being applicable within the same platform as the cryptocurrencies, as cryptocurrency holders could 'literally be anywhere'[25].

In particular, the intrinsically global reach of cryptocurrencies creates a difficulty in establishing jurisdiction whenever cryptocurrency disputes are brought to court. For example, the issue of jurisdiction was the basis for the *Ang v Reliantco Investments Ltd* case.[26] In this case, the defendant Reliantco, a company incorporated in Cyprus offering financial products and services, made an application challenging the jurisdiction of an English court to try them. The company contended that Ms Ang was bound by its standard terms and

[24] D He, K Habermeiser, R Lecklow and others, 'Virtual Currencies and Beyond, Initial Considerations' (2016) IMF Staff Discussion Note <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf> Accessed 18 June 2018.

[25] P Paech, 'Integrating Global Blockchain Securities Settlement with the Law—Policy Considerations and Draft Principles' (*SSRN* 7 August 2016) <https://ssrn.com/abstract=2792639> Accessed 18 June 2018. 25.

[26] *Ang v Reliantco Investments Ltd* [2019] Queen's Bench Division (Commercial Court) EWHC 879 (Comm).

conditions, which provided that the courts of Cyprus are to have exclusive jurisdiction over 'all disputes and controversies arising out of or in connection with' her customer agreement. Whilst it is possible to arrive at a decision, establishing the relevant jurisdiction in this way, it is nonetheless time-consuming and taxing to the judicial system.

The issue of varying jurisdictional oversight creates a further enforcement challenge to do with regulatory arbitrage, where cryptocurrency firms can 'shop' for the least burdensome and most lenient jurisdictions in which to conduct their activities.[27] For example, after the banning of cryptocurrency exchanges in China, the majority of these moved to Hong Kong—which has been described as a 'regulatory-friendly jurisdiction' for cryptocurrencies.[28] Similarly, Binance (a cryptocurrency exchange initially based in Japan) joined dozens of cryptocurrency companies relocating to Malta, which is largely seen as a cryptocurrency-friendly jurisdiction, after the Japanese government took a 'tougher regulatory stance' on cryptocurrency.[29] This phenomenon has led to calls for the harmonisation of cryptocurrency regulation, which we will address in Chapter 6.

3.3 Compliance Challenges

In addition to the enforcement challenges being faced by regulators, the regulatory targets in the cryptocurrency ecosystem (including exchanges and wallet providers) are faced with challenges that make it difficult to comply with

[27] A Poster, 'Cryptoassets Regulatory Arbitrage—A Clear and Present Danger' (*Forbes* 9 December 2019) <https://www.forbes.com/sites/amyposter/2019/12/09/crypto-assets-regulatory-arbitragea-clear-and-present-danger/#395730477438> Accessed 10 December 2019.

[28] J Young, 'China's Stricter Bitcoin Regulations Will Strengthen Hong Kong Market' (*Cointelegraph* 16 September 2017) <https://cointelegraph.com/news/chinas-stricter-bitcoin-regulations-will-strengthen-hong-kong-market> Accessed 3 July 2018.

[29] Y Nakamura, 'The World's Biggest Cryptocurrency Exchange Heading to Malta' (*Bloomberg,* 23 March 2018) <https://www.bloomberg.com/news/articles/2018-03-23/the-world-s-biggest-cryptocurrency-exchange-is-moving-to-malta> Accessed 18 June 2018, see also S Mamudi, 'On the G20 Agenda: A Shared Desire to Clamp Down on Crypto' (*Bloomberg* 19 March 2018) <https://www.bloomberg.com/news/articles/2018-03-19/on-g-20-agenda-a-shared-desire-to-calm-down-crypto-quicktake> Accessed 18 June 2018.

current substantive legal requirements and regulations. As was noted by McBarnet and Whelan, much of regulation research is concerned with 'the extent to which target populations comply with the law, why people comply, or fail to comply, and how regulators and the targets of regulation construct the meaning of compliance'.[30] In this instance, barriers to compliance created by the limitations of cryptocurrency regulation in its current form have to do with compliance costs, regulatory exclusions and oversights, and the confusion brought about by the lack of a harmonised global approach and use of multiple legal definitions for cryptocurrencies.

3.3.1 Compliance Costs and Proportionality

The first obstacle to compliance with current cryptocurrency regulation has to do with compliance costs[31]. In this instance, we will consider the issue of jurisdictions imposing capital requirements on cryptocurrency exchanges and wallet providers. In the US, FinCEN's Money Transmitter licensing requirements are targeted at 'non-bank entities that receive and hold consumer funds, with promise of making funds available later or sending funds elsewhere as well as entities that issue or sell payment instruments'[32], including cryptocurrency exchanges and wallet providers. Here, the main requirements for this license in the US are: minimum capitalisation of US$50,000–US$1 million, a background check on principals, holding 100 per cent of consumer funds in permissible investments, as well as regular reports, filings and audits.[33] In Indonesia, the onerous minimum capital requirements to cryptocurrency futures trading of 1 trillion *rupiah* (over US$70 million) has been met with anger, as it costs a fraction

[30] D McBarnet and C Whelan, 'The Elusive Spirit of the Law: Formalism and the Struggle for Legal Control' (1991) 54 MLR 848.
[31] Compliance cost refers to all the expenses that a firm incurs to adhere to industry regulations. These include salaries of people working in compliance, time and money spend on reporting and so on. See W Kenton, *Investopedia* 18 April 2018 <https://www.investopedia.com/terms/c/compliance-cost.asp> Accessed 10 December 2019.
[32] FinCEN, 'Guidance: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies' (*FinCEN* 2013) <https://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html> Accessed 10 December 2019.
[33] ibid.

of this amount—2.5 billion *rupiah* (US$178, 000) to begin trading traditional commodities.[34] In addition to questioning the proportionality of these regulations relative to the size of the cryptocurrency market[35], the use of capital requirements in this context has been questioned, as 'capital adequacy rules cannot adjust fast enough or be sufficiently contextually attuned to specific markets to do the job'. [36] In addition to the costs associated with these capital requirements, there are also the costs associated with complying with KYC requirements. It has been noted that if large banks are finding KYC compliance costs onerous (which average US$550m a year), these costs 'could be fatal for cryptocurrency exchanges, particularly new entrants to the market'.[37]

In addition to this, there are the compliance costs of a non-monetary nature associated with existing cryptocurrency regulations. For example, as noted by Jury, 'it takes 24 days, on average, for a commercial bank customer to pass the entire compliance process … this delay isn't attractive to crypto[currency] traders and investors who may simply use a platform with less scrupulous checks'.[38] With these issues in mind, the BIS recommends that within applicable statutory authorities and jurisdictions, supervisors should consider whether these frameworks are:

> *Sufficiently proportionate and adaptive to appropriately balance ensuring safety and soundness and consumer protection expectations with mitigating the*

[34] W Suberg, 'Indonesia: $70 Million Capital Requirement for Bitcoin Futures Sparks Anger' (*Cointelegraph* 14 February 2019) <https://cointelegraph.com/news/indonesia-70-million-capital-requirement-for-bitcoin-futures-sparks-anger> Accessed 14 February 2019.

[35] S Hughes and S Middlebrook, 'Advancing a Framework for Regulating Cryptocurrency Payments Intermediaries' [2015] 32 Yale J on Reg.

[36] C Parker and J Braithwaite, 'Regulation' in M Tushnet and P Cane (eds), *Oxford Handbook of Legal Studies* (OUP 2005).

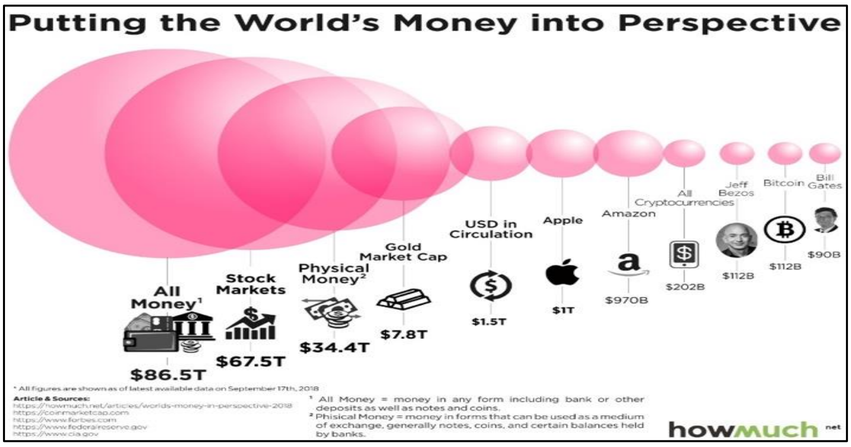
[37] A Jury, 'Is the Regulation That Threatens the Free-Spirited Nature of Cryptocurrency Actually the Key to its Future?' (*Bureau Van Dijk* 14 August 2019) <https://www.bvdinfo.com/en-gb/blog/compliance-and-financial-crime/regulation-of-cryptocurrency-actually-the-key-to-its-future> Accessed 3 December 2019.

[38] ibid.

> *risk of inadvertently raising barriers to entry for new firms or new business models.*[39]

Of particular relevance is the proportionality principle—which entails tailoring regulatory requirements to a firm's size, systemic importance, complexity, and risk profile—with the aim of avoiding excessive compliance costs or regulatory burden without prudential justification.[40] Arguably, there is little or no prudential justification for the capital requirements imposed on cryptocurrencies in some jurisdictions. In an infographic comparing cryptocurrency against the entire world's wealth (Figure below), figures compiled by howmuch.net show how all the cryptocurrencies in existence are worth only 0.59 per cent of the world's physical money (US$34.4 trillion vs US$202 billion), and that the entire market capitalisation of Amazon is US$858 billion larger than Bitcoin.

Figure 5: Putting the World's Money into Perspective



Source: howmuch.net[41]

[39] Basel Committee on Banking Supervision, 'Sound Practices: Implications of Fintech Developments for Banks and Bank Supervisors' (*Bank of International Settlements* February 2018*)* < https://www.bis.org/bcbs/publ/d431.pdf>   Accessed 3 December 2019. 48.

[40] S Lautenschläger, 'Is Small Beautiful? Supervision, Regulation and the Size of Banks' (Speech at an IMF seminar, Washington DC, 14 October 2017) <https://www.ecb.europa.eu/press/key/date/2017/html/ecb.sp171014.en.html> Accessed 3 December 2019.

[41] Howmuch.net, 'Comparing Cryptocurrency against the Entire World's Wealth in One Graph' (*Howmuch.net* 2018) <https://howmuch.net/articles/worlds-money-in-perspective-2018> Accessed 3 December 2019.

The corollary of this disproportionate regulation is the reduction of competition and the curtailing of the innovation potential of blockchain and cryptocurrencies which are described in Chapter 1. In this way, it can be seen that the monetary and non-monetary costs of compliance associated with current cryptocurrency regulation presents a challenge that must be addressed.

3.3.2 Regulatory Exclusions and Oversights

Further barriers to compliance are presented by regulatory exclusions and oversights, which can also be seen as fissures and shortcomings in current regulation. The first of these is poorly designed licensing regimes for cryptocurrency intermediaries. As has been noted by the Basel Committee on Banking Supervision,

> *current bank regulatory, supervisory and licensing frameworks generally predate the technologies and new business models of fintech firms. This may create the risk of unintended regulatory gaps when new business models move critical banking activities outside regulated environments.*[42]

This is partly true for cryptocurrency firms, where there is a lack of resolution mechanisms, ineffective licensing, and an exclusion of oversight in payments, private and commercial law.

The first observation that can be made with regards to regulatory oversight has to do with the lack of resolution mechanisms for failed cryptocurrency intermediaries. Upon its collapse, Mt Gox announced that over US$450million worth of Bitcoin was missing or stolen.[43] Although a formal claims process was initiated by Mt Gox's bankruptcy trustees, and although security consultancies have been appointed to attempt to trace the missing Bitcoins, most customers have still been left out of pocket. In the 2016 hack of Bitfinex, the exchange resorted to bankruptcy resolution techniques seen in traditional financial

[42] Basel Committee on Banking Supervision (n 39) 6.

[43] R McMillan, 'The Inside Story of Mt Gox, Bitcoins $460million Disaster' (*Wired.Com* 2014) <http://www.wired.com/2014/03/bitcoin-exchange/> Accessed 20 May 2016.

institutions, through a bail-in process in which the customers whose wallets were not hacked were obliged to pay 36 per cent of their own deposits in order to reimburse the 36 per cent of customers whose wallets were hacked into.[44] Similarly, the placing of Mt Gox into receivership—where its remaining customers were effectively taken over by other exchanges—follows models evident in traditional bank resolution. However, this ad hoc arrangement is not universal, and there are no industry guidelines by regulators on this subject. As found in a survey by the CCAF,

> *only 53% of small exchanges that act as a custodian by controlling customer keys have a written policy that outlines what happens to customer funds in the event of a security breach that could lead to the loss of customer funds. In contrast, 78% of large custodial exchanges have such a written policy.*[45]

The second issue to consider is the current licensing regime for cryptocurrency exchanges and wallet providers. The regulation of these intermediaries does not extend its reach to cover P2P and DEX, which operate exclusively online. However, even where exchanges and wallet providers are required to operate with licenses, there is evidence that not all of these intermediaries in operation have licenses. The CCAF found that only 24 per cent of surveyed incorporated wallets have a formal license from a regulatory authority, and all of them are wallet providers that offer national-to-cryptocurrency exchange services; 25 per cent of wallets providing centralised national-to-cryptocurrency exchange services do not have a government license.[46] The survey further found that 85 per cent of all exchanges based in Asia-Pacific do not have a license, whereas 78 per cent of North American-based exchanges, 47 per cent of European-based

[44] L Coleman, 'Bitfinex 'Bail-In'—New Financial System Offers Laboratory for Handling Unexpected Losses' (*Cryptocoin News* 12 August 2016) <https://www.cryptocoinsnews.com/bitfinex-bail-new-financial-system-offers-laboratory-handling-unexpected-losses/ > Accessed 22 August 2016.

[45] G Hileman and M Rauchs, 'Global cryptocurrency benchmarking study' (*Cambridge Centre for Alternative Finance* 2017) <https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf> Accessed 2 December 2019. 27.

[46] ibid.

exchanges, and 43 per cent of Latin American-based exchanges, respectively, hold a formal government license or authorisation.[47] This finding is significant, because licensing and licensing requirements are a key component of currency cryptocurrency regulation.[48] The practical implication of this is that, for example, if only 25 per cent of surveyed wallets have a formal license, then only 25 per cent of wallets are complying with licensing requirements such as KYC, AML and CTF reporting, and are putting in place required consumer protections.

Finally, it has been put forward that the current regulatory interventions for cryptocurrency, focusing predominately on AML and CTF, are insufficient. The ECB notes that,

> *we need a broader perspective on regulatory intervention for VC facilitators that extends beyond the fields of AML and CTF. Possible regulatory action should be explored, as well as amending or broadening existing frameworks such as the revised Payment Services Directive (PSD2) so that the licensing and supervision rules also apply to VC facilitators.*[49]

If this recommendation were followed, cryptocurrency intermediaries could be classified as Payment Institutions, and by so doing, under UK law this would make them subject to Payment Services Regulation, which would consider consumer protection issues such as governance, safeguarding measures, internal controls, and risk management procedures more robustly.[50] This proposal is in line with recent initiatives within Europe, where, in addition to the inclusion of cryptocurrencies in the 4th AMLD, the Council called for a similar amendment in

[47] ibid.

[48] FATF, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' (*FATF* 2019) <www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html> Accessed 3 December 2019.

[49] Y Mersch, 'Virtual or Virtueless? The Evolution of Money in the Digital Age' (*ECB* 8 February 2018) <https://www.ecb.europa.eu/press/key/date/2018/html/ecb.sp180208.en.html> Accessed 3 July 2018.

[50] A Vaziri, 'Bitcoin Exchanges as Payment Institutions' (*Neopay* 2014) <http://neopay.co.uk/site/wp-content/uploads/Diacle-Bitcoin-Regulation.pdf > Accessed 3 July 2018.

the 2nd Payment Services Directive.[51]In the US, the same gap in the regulation of payment systems brought about by the advent of cryptocurrency and mobile payments can be seen. It has been shown that 'private contract law (might need to be) expanded to fill the gaps where payment technology has exceeded the scope of public law' through the use of the Uniform Commercial Code.[52] Similarly calling for the application of alternative existing sources of law is Hody,[53] who proposed the application of laws on custody, authorisation and possession to cryptocurrencies. Noting that 'possession of your keys by someone else (intermediaries) does not, in the eyes of the law, negate your ownership of those keys'[54], leaving scope and precedent to apply legal consideration of topics to do with custody, possession and authorisation similar to the laws on car accidents or other instances involving custodial relationships. Hughes and Middlebrook propose further applicability of existing law, affirming, 'transaction-execution rules for cryptocurrency payments are the missing link in the regulation of cryptocurrency transactions'. [55]Here, they additionally note how current regulation of cryptocurrency is primarily for public law purposes, such as collecting taxes or deterring money laundering, and for market-enhancing purposes, such as licencing and prudential requirements, whilst neglecting regulations serving specific commercial or private law purposes.[56] Finally, also calling for a variation of the regulatory approach to cryptocurrencies is Chiu, who proposes a systemic and holistic approach beyond financial regulation for the governance of the crypto-economy in the EU, based on Innovation Policy.[57]

[51] Council of the European Union, 'Council Conclusions on the Fight Against the Financing of Terrorism' (Press Release 50/16 2016)<http://www.consilium.europa.eu/en/press/press-releases/2016/02/12-conclusions-terrorism-financing/ > Accessed 19 August 2016.
[52] M Burge, 'Apple Pay, Bitcoin and Consumers: The ABC's of Future Public Payments Law' (2016) 67 Hastings Law Journal 5; Hughes and Middlebrook (n 35).
[53] S Hody, 'Ownership Does Not Require Possession' (*Medium* 2016) <https://medium.com/@SHodyEsq/ownership-doesnt-require-possession-5eac8e29e460#.itw4rw4f7> Accessed 19 August 2016.
[54] ibid.
[55] Hughes and Middlebrook (n 35) 496.
[56] ibid.
[57] I Chiu, 'Pathways to European Policy and Regulation in the Crypto-Economy' (2019) 10 European Journal of Risk Regulation 738.

These various proposals to extend the legal boundaries currently placed on cryptocurrencies highlight the oversights and fissures of current cryptocurrency regulation. However, whilst instructive, none of these proposals address the enforcement issues relating to online cryptocurrency activities, highlighted above. This suggests that that the solution to more effective cryptocurrency regulation lies not in increasing the layers of applicable substantive law around cryptocurrency, but by looking beyond substantive law to achieve regulatory objectives as shall be further discussed below.

3.3.3 Lack of a Global Approach

The final factor that makes compliance difficult for those involved in the cryptocurrency industry has to do with the lack of a global approach to cryptocurrency regulation. As was discussed in detail in the preceding chapter, cryptocurrency regulation varies largely across jurisdictions: no regulation, restrictive, neutral and permissive regulations. As explained by Weinstein, Cohn and Parker,

> *the disparate approaches taken by different countries, or even by different agencies within the U.S., have led to confusion on the part of blockchain companies about the jurisdictions and regulatory regimes to which their products and services will be subject.*[58]

This highlights how the issues of jurisdiction highlighted above, which are enhanced due to cryptocurrency's use of DLT, have implications beyond regulatory arbitrage—they also result in an inability to comply, based on uncertainty and confusion about which regulations apply. It has been stated that 'keeping track of what's legal has become just as daunting as figuring out which newfangled token might turn into the next Bitcoin … rules can vary wildly by

[58] J Weinstein, A Cohn and C Parker, 'Promoting Innovation through Learning' in J Dewey (ed) *Global Legal Insights—Blockchain and Cryptocurrency Regulation* (Global Legal Group 2019). 2.

country, given a lack of global coordination among authorities'.[59] A similar observation was made by JP Morgan researchers, who described current cryptocurrency regulation as 'piecemeal efforts, with various nations staking independent regulatory position, and there has been little global coordination on cryptocurrency regulation'.[60]

The effects of this regulatory uncertainty can be seen when considering the regulation of ICOs. As was noted by Hacker and Thomale,

> *regulators should decide how to deal with ICOs. For example, while some countries, such as China and South Korea, have prohibited ICOs, other jurisdictions (eg, Mexico) require authorisation for any issuance of tokens (no matter whether they are security or non-security tokens), and other countries, including the United States, Singapore, and Switzerland, subject ICOs to a selective control ex ante to determine whether the offering involves security tokens.*[61]

The same observation was summarised by the OECD, which noted that so far, the response from regulators on ICOs has been fragmented, with many applying existing regulation to ICOs on a case-by-case basis; others have acknowledged that most ICOs largely fall outside the realm of law and supervision; several authorities have issued investor warnings about ICOs, while still others have effectively banned them outright.[62] This means that 'industry and investors lack the kind of certainty needed to fully realise the potential of ICOs, while the regulatory and legal void makes criminal activity difficult to detect and counter'

[59] Bloomberg 'Making Sense of the World's Cryptocurrency Rules' (*Bloomberg News* 18 March 2018) <https://www.bloomberg.com/news/articles/2018-03-19/is-this-legal-making-sense-of-the-world-s-cryptocurrency-rules> Accessed 18 June 2016.

[60] JP Morgan, 'Decrypting Cryptocurrencies: Technology, Application and Challenges' (*JP Morgan Perspectives* 9 February 2018) <http://forum.gipsyteam.ru/index.php?act=attach&type=post&id=566108> Accessed 20 June 2018.

[61] ibid.

[62] G Medcraft, 'The OECD and the Blockchain Revolution' (*OECD*, Presentation at the OECD Friends of Going Digital Meeting, Paris 29 March 2018) <http://www.oecd.org/parliamentarians/meetings/meeting-on-the-road-london-april-2018/The-OECD-and-the-Blockchain-Revolution-Presentation-by-Greg-Medcraft-delivered-on-29-March-2018.pdf> Accessed 30 June 2018.

with commentators recommending that ‘the wide range of treatments across jurisdictions … must be co-ordinated internationally’.[63] In this instance, it can be seen that compliance with ICO regulations is challenging to cryptocurrency industry participants, due to the confusion and uncertainty generated by disparate and contradictory global regulatory arrangements.

The IMF, the OECD and other supranational authorities have called for a unified global response to cryptocurrency regulation, and stated that greater international discussion and cooperation is needed in order to address the regulatory challenges posed by cryptocurrencies. However, it may be difficult to arrive at a unified global approach to cryptocurrency regulation. Firstly, there are overarching limitations inherent in international law, due to the fact that ‘global regulation inevitably is at the cross-road of conflicting interests, and the incestuous relationship between power and money, politics and finance that this undertaking extraordinarily complex’.[64] This often results in sub-optimal decisions being made at the level of global regulation, because governments and parliaments might not want to ‘use any of their political capital to take the right global decisions if they hurt their constituencies’.[65] For example, the FATF’s beneficial ownership requirements are already difficult to enforce, without adding the complexities of cryptocurrencies. Evaluations show that 40 out of 44 jurisdictions need to make fundamental or major improvements in their anti-money laundering and countering terrorist financing systems to prevent the misuse of legal persons and arrangements and ensure availability of beneficial ownership information.[66]

This suggests that, while the need for a global approach to cryptocurrency regulation has been noted and encouraged, the use of traditional forums and

[63] ibid.

[64] G Ugeux, *International Financial Regulation: The Quest for Financial Stability* (Wiley 2014) 168.

[65] ibid.

[66] FATF, ‘FATF Report to the G20 Finance Ministers and Central Bank Governors’ (*FATF* March 2018) <http://www.fatf-gafi.org/media/fatf/documents/FATF-G20-FM-CBG-March-2018.pdf> Accessed 19 June 2018.

approaches to global regulation are unlikely to be as effective as envisaged, given the inherent pitfalls of international law which would be amplified by the complexities surrounding cryptocurrencies—as shall be described in the next chapter.

3.3.4 Multiple Legal Definitions

The final compliance challenge that presents itself in current cryptocurrency regulation has to do with the inconsistencies that arise from the existence of multiple legal definitions of cryptocurrency in current regulation. It has been noted that 'while some oversight agencies treat digital currencies as money, other agencies view them as a kind of property. They are traded on exchanges like securities, mined like commodities, and stored like digital information'.[67] This plurality in legal classifications contributes to regulatory confusion and uncertainty which, in turn, presents enforcement challenges related to inconsistencies.

How cryptocurrencies are classified has significant implications when it comes to regulation. As noted by Ramasastry, 'from banking laws to anti-money-laundering laws and tax regulations—whether these laws apply to the use of Bitcoin depends on how Bitcoin is classified'.[68] For example, in highlighting the property-contract legal duality of cryptocurrencies, Berta and Noonan concluded that 'in storage and at rest, Bitcoins are trade secrets to be jealously guarded. But in motion they are digital contracts with aspects of secrecy'.[69] Another form of duality was highlighted by Ireland's Minister of Finance, when considering the tax treatment of cryptocurrencies in Ireland: 'because Bitcoin is a combination of some factors that constitute a commodity and some that constitute a currency,

[67] ibid.

[68] A Ramasastry, 'Is Bitcoin Money? Lawmakers, Regulators and Judges Don't Agree' (*Justia* 9 September 2014) <https://verdict.justia.com/2014/09/09/bitcoin-money> Accessed 7 June 2016.

[69] M Berta and W Noonan, 'The Property-Contract Duality of Bitcoin' (Financier Worldwide Expert Briefing June 2015).

the implications for taxation are varied'.[70] Arguably, this duality extends beyond the property-contracts nexus and the commodity-currency nexus, to a plurality of multiple potential definitions and applications of law. However, these distinctions are not merely issues of theoretical conjecture and debate, they have practical real-world implications for the law.

The legal significance of multiple definitions of cryptocurrency can be seen in *Hashfast Technologies LLC v Lowe.*[71] In this case, a lawsuit was brought to a bankruptcy court against a former employee of a now bankrupt Bitcoin mining company, for receiving fraudulent transfers in Bitcoin. Here, the court's definition of Bitcoin is highly significant, because 'if Bitcoin is 'currency' the trustee would be entitled to the bitcoin historical value or the value on the date or transfer' and 'if Bitcoin is 'property, the trustee would be entitled to receive the value of the BTC at the transfer date or time of recovery *whichever is greater'.*[72] This is particularly significant given Bitcoin price fluctuations. The historical value of the Bitcoins in this case was US$363,861, whereas the value at the date of filing the case had increased to US$1,344,705.[73] In this case, the Bankruptcy Court did not reach a determination of whether Bitcoin was a currency or commodity, stating that 'the court does not need to decide whether Bitcoin are currency or commodities for the purposes of fraudulent-transfer provisions of the Bankruptcy Code'.[74] However, in also concluding that 'Bitcoin are not United States dollars', the court signalled Bitcoin as being more akin to a commodity than currency.[75]

[70] Arthur Cox, 'Cryptocurrencies and the Law: The Irish Position' (Arthur Cox Technology and Innovation Group Briefing June 2014).

[71] *Hashfast Technologies LLC v Lowe* [2016] California North Bankruptcy Court 14-30725-DM (Bankr ND Cal Feb 22, 2016).

[72] M Zuberi, 'Bitcoin Identity Crisis: Currency or Property'? (Lexology 17 February 2016) <http://www.lexology.com/library/detail.aspx?g=65a1f5fb-521f-49f7-90f0-6aaa08ada139> Accessed 7 June 2016.

[73] ibid.

[74] *Hashfast Technologies LLC v Lowe* (n 71) 1.

[75] For further discussion on the legal definitions of cryptocurrency in bankruptcy, see E Illman and R Cox, 'Bitcoin and Bankruptcy: Why Creditors and Bankruptcy Practitioners Need to Understand Cryptocurrencies' (*Westlaw Journal Bankruptcy* 14 December 2017).

It has therefore been evident that the few findings in court cases and regulatory opinions involving cryptocurrencies vary in their determination of asset classification, depending on the regulatory context. For example, the Federal Election Commission (FEC) and the magistrate judge in *SEC v Trendon Shavers and Bitcoin Savings Trust,* mentioned above, have issued differing views on the possible legal classification of Bitcoins. In November 2014, the FEC proposed—but did not approve—a draft advisory opinion that would have permitted the use of Bitcoins for in-kind contributions, under the regulatory category of 'anything of value,' which includes commodities, stock and equipment. The draft advisory opinion, noting the more narrow regulatory definition of 'money' under election law, stated that Bitcoins could not be accepted as a money contribution and would have to be converted to US dollars for deposit in a campaign account. This is in contrast to the magistrate judge in *SEC v Trendon Shavers and Bitcoin Savings Trust,* who, as described above, stated that Bitcoins 'can be used as money' and possess attributes of a 'currency or form of money'.[76]

This expedient consideration of various definitions of cryptocurrency is particularly prevalent in taxation. Of note here is how 'the IRS's designation of cryptocurrencies as 'property' instead of as 'currency' deprives the trader/user of favourable tax treatment afforded to foreign currency transactions'.[77] A more cynical view of this phenomenon was presented by Fournier and Lennard[78], who noted that 'where there is money to be made, there is tax to be levied and where the available tax rules are rooted in past perceptions of what 'money' is, the courts have broad latitude in determining what is just'.[79]

In the UK, the position of HM Revenue and Customs (HMRC) on the tax treatment of cryptocurrencies is in line with that of the EU in its exemption of VAT, but

[76] Federal Election Commission, 'Political Committee May Accept Bitcoin as Contribution' (FEC Advisory Opinion 2014-02 2014) <http://saos.fec.gov/aodocs/2014-02.pdf> Accessed 6 June 2016.

[77] Hughes and Middlebrook (n 34).

[78] O Fournier and J Lennard, 'Rebooting Money: The Canadian Tax Treatment of Bitcoin and Other Cryptocurrencies' Canadian Tax Foundation (2014) Conference Report, 11.

[79] ibid.

however, applies Corporation Tax (CT), Income Tax (IT) and Capital Gains Tax (CGT) liabilities in the same manner as the IRS. Of note here is how the HMRC's position incorporates two separate understandings and definitions of cryptocurrencies: firstly as property (as is the case in the US), and secondly as currency (as is the basis of exemption from VAT in the EU). This application of varying definitions of cryptocurrency has led to regulatory uncertainty, adding to the confusion around compliance for companies operating within the cryptocurrency industry.

3.4 Discussion

The enforcement and compliance challenges highlighted above indicate the need for an alternative approach to cryptocurrency regulation. However, prior to delineating the considerations that should guide an alternative approach, it must be established that 'no regulation' for cryptocurrencies (as is the case in some jurisdictions) is not a viable option and it must be asserted that the regulatory challenges presented by cryptocurrencies are rooted in the features and functions of blockchain technology.

3.4.1 Ineffectiveness of 'No Regulation'

At first glance it may appear counter-intuitive to consider the effectiveness of 'no regulation', as this approach may seem to be, by definition, ineffective. However, insight into cryptocurrency regulation can still be gleaned by observing the impact on social reality that is made by the absence of regulation. The UK is the main outlier amongst key cryptocurrency jurisdictions, having opted to take a wait-and-see approach. However, both legislators and industry participants have raised concerns about such a stance. Calls for regulation have grown, in particular as a result of fears around investor protection and money laundering.[80] Calling the current 'no regulation' approach the 'wild west', Members of Parliament

[80] H Murphy, ''Wild West' Crypto-Asset Markets Need UK Regulation, Say MPs', (*The Financial Times* 19 September 2018) <https://www.ft.com/content/dbea3cac-bb3c-11e8-8274-55b72926558f> Accessed 16 January 2019.

(MPs) in the Commons Treasury Select Committee have stated that the lack of cryptocurrency regulation in the UK has exposed investors to a 'litany of risks', and further, that it is 'unsustainable for the government and regulators to bumble along issuing feeble warnings to potential investors, yet refrain from acting'.[81] Cryptocurrency industry representatives, including the trade association CryptoUK, which has advocated and set out proposals for cryptocurrency regulation in the UK in order to reduce regulatory uncertainty, have echoed these concerns about the lack of regulation in the UK.[82] This potential market-development role of regulation was equally recognised by the Select Committee, which stated 'regulation could lead to positive outcomes for the crypto-asset market, including the move toward a more mature business model and increased liquidity'.[83] This observation is consistent with empirical findings that 'news pointing to the establishment of legal frameworks tailored to cryptocurrencies and initial coin offerings coincides with strong market gains'[84].

As highlighted in the preceding chapter, the category of jurisdictions with no regulation include instances where the sole regulatory activity is the issuing of warnings, and/or the articulation of some version of a 'wait-and-see' approach. There is little evidence to support the efficacy of issuing of warnings on social behaviour in the cryptocurrency space. Indeed the Select Committee noted that 'the FCA's consumer warnings are a feeble corrective to advertisements … that only emphasise the upside opportunities of crypto-asset investing'[85]. Similarly, it has been noted that whilst regulators in Canada have said that that products linked to cryptocurrencies should be considered high risk, at the same time, the

[81] ibid.

[82] A Alexandre, 'CryptoUK Trade Association Calls on MPs to Regulate Cryptocurrency Sector in UK' (*Cointelegraph* May 2, 2018) <https://cointelegraph.com/news/cryptouk-trade-association-calls-on-mps-to-regulate-cryptocurrency-sector-in-uk> Accessed 16 January 2019.

[83] Murphy (n 80).

[84] R Auer and S Claessens, 'Regulating Cryptocurrencies: Assessing Market Reactions' (*BIS Quarterly Review* September 2018), <https://www.bis.org/publ/qtrpdf/r_qt1809f.htm> Accessed 19 February 2019.

[85] House of Commons Treasury Committee, 'Crypto-assets: Twenty-Second Report of Session 2017-19' (2018) <https://publications.parliament.uk/pa/cm201719/cmselect/cmtreasy/910/910.pdf> Accessed 19 February 2019. 33.

country's stock exchanges have become popular destinations for crypto-related stocks and exchange-traded funds.[86] The same ambiguous link between warnings and consumer behaviour is likely to be evident in other jurisdictions where regulators have issued warnings, including France, Germany, Australia, Argentina, South Africa and Japan.

3.4.2 Technical Roots of Regulatory Challenges

As was described in Chapter 1, cryptocurrencies operate using public, permission-less blockchain that is distributed across a global network of independent nodes, and secured cryptographically. This creates both regulatory challenges and regulatory opportunities that are not being considered and accounted for in the majority of current approaches to cryptocurrency regulation.

Cryptocurrencies present enforcement challenges for P2P and DEX, pseudonymity and jurisdiction, because of the technical features of decentralised nodes, public and private key cryptography, and operating in a virtual or online environment. Current regulation of cryptocurrency intermediaries, including exchanges and wallet providers, becomes ineffective when cryptocurrency transactions are conducted exclusively online through P2P and DEX. Regulations fall similarly short when the technical capability to obscure cryptocurrency users through the use of public and private key cryptography is amplified by the use of privacy coins and tumbler services. Finally, current regulations fail to contend with the jurisdictional challenges arising because cryptocurrency can be used by anyone based anywhere in the world who is able to download the cryptocurrency software, and these individuals can send and receive cryptocurrency from anyone else in possession of this software regardless of their geographical location. More specifically, as noted by Paech, 'technical outcomes and legal

[86] Bloomberg News, 'Making Sense of the World's Cryptocurrency rules' (*Bloomberg* 19 March 2018) <https://www.bloomberg.com/news/articles/2018-03-19/is-this-legal-making-sense-of-the-world-s-cryptocurrency-rules> Accessed 3 November 2018.

results may sometimes contradict each other'[87], particularly where legal results cannot be put into practice retroactively, because blockchain transactions are generally difficult to reverse.[88] These tensions between technical features and legal requirements existing in current cryptocurrency regulation are summarised in Table *1*, below.

Table 1*: Legal Implications of Cryptocurrency Technical Features*

Cryptocurrency Technical Feature	**Legal Implications**
Immutability	• Consumer protection concerns as transactions cannot be reversed
Pseudonymity	• Cannot easily detect who is behind the transactions which lends itself to money laundering, terrorist financing and the use cryptocurrencies to facilitate illicit transactions
Distributed	• Jurisdiction challenges are faced due to the existence of global, multiple nodes; • Difficult to ascertain regulatory target and establish liability; • Regulatory arbitrage; • Cryptocurrencies cannot be shut down

[87] Paech (n25) 7.
[88] Paech (n 25).

Virtual/Digital	- Transactions can migrate exclusively online falling outside the reach and scope of existing regulation

Therefore, we can conclude that current cryptocurrency regulation is unenforceable using substantive legal rules and the traditional tools of financial regulation, due to cryptocurrency's technical features. However, in addition to presenting challenges to regulation, the technical features of cryptocurrencies also present unique regulatory opportunities currently un- or under-explored by regulators. As shall be further discussed in the subsequent chapters, the computer code-based nature of cryptocurrency renders itself well suited to code-based regulatory intervention that falls under the broad category of regulatory technology (regtech) and algorithmic regulation. As explained by Cutts and Micheler, Bitcoin has 'built-in cryptographic protections', leading to the conclusion that, particularly in the case of crypto-securities, 'you will need a lot less law'.[89]

3.5 Conclusion

This chapter has shown how current cryptocurrency regulation is faced with enforcement and compliance challenges and limitations. Enforcement challenges have to do with P2P and DEX, pseudonymity, and the challenges of jurisdiction and arbitrage. Compliance challenges have to do with financial and non-financial compliance costs, regulatory exclusions and oversights, and the uncertainties that arise from multiple legal definitions for cryptocurrency regulation, and the

[89] T Cutts, 'Bitcoin Ownership and its Impact On Fungibility' (Coindesk 14 June 2015) <http://www.coindesk.com/bitcoin-ownership-impact-fungibility/> Accessed 16 June 2016.

lack of a harmonised global approach. This indicates the need for an alternative approach to cryptocurrency regulation.

This chapter has additionally shown the problematic nature of having 'no regulation', and identified the root cause of shortcomings with current cryptocurrency regulation as being the failure to take into account the regulatory implications, challenges and opportunities resulting from the technical features and functionality of cryptocurrencies. The alignment of technical features and functions to legal and regulatory objectives can only be internally operationalised, as it relies exclusively on those responsible for the development of cryptocurrency technical functionality—in essence, a form of self-regulation. In this way, a regulatory approach to cryptocurrencies would need to be one that:

a) examines and considers the limitations of substantive law in the regulation of cryptocurrencies;
b) examines and considers both the challenges and opportunities inherent to the technological features and functionality of cryptocurrency, and;
c) examines and considers the role of self-regulation in cryptocurrency.

What follows is a discussion of regulatory theory, and the introduction of Reflexive Regulation—presented as the regulatory framework best suited to addressing the shortcomings related to current cryptocurrency regulation.

Chapter Four: Reflexive Regulation Theory

4.1 Introduction

In the preceding chapter, the need for a change in approach to cryptocurrency regulation was highlighted. The enforcement and compliance challenges presented by cryptocurrencies call for a reconsideration of the role of the law vis-à-vis cryptocurrencies, and the consideration of an alternative regulatory strategy. The aim of this chapter is to present the theoretical foundation for an alternative approach to cryptocurrency regulation based on the theory of reflexive regulation. This will be done by first providing an overview of the key components of reflexive regulation theory, as initially presented by Gunther Teubner. This will be followed by a consideration of where reflexive regulation stands in the spectrum of established regulatory theories and strategies with a particular focus on the differences between reflexive regulation and other self-regulation-based theoretical approaches. The chapter will conclude by discussing the rationale and merits of taking a reflexive law approach to the regulation of cryptocurrencies.

4.2 Overview of Reflexive Regulation

Regulatory theory, is defined as 'a set of propositions or hypotheses about why regulation emerges, which actors contribute to that emergence and typical patterns of interactions between regulatory actors.'[1] The theory of reflexive regulation provides a series of propositions around the patterns of interactions of regulatory actors that are based on three key concepts namely: systems theory and autopoiesis, socially adequate complexity, and proceduralisation, positioned as a replacement for substantive legal rules. Each of these shall be discussed in turn.

[1] M Bronwen and K Yeung, *An Introduction to Law and Regulation: Text and Materials* (CUP 2007) 8.

4.2.1 Systems Theory and Autopoiesis

The starting point of reflexive regulation is an understanding of the world as consisting of independent, closed systems, of which the legal system is only one amongst many others, including the economic system, religious system and the political system. This systems theory of law was developed initially by Niklas Luhmann, who presented the notion that society consists of multiple autopoietic systems.[2],[3] Here, Luhmann began by framing the observation that systems are distinguished by 'functional differentiation',[4] in which each system plays a distinct role in world society, and as such, operates in a unique and individual manner that has its own (legitimate) internal logic. An example of the manifestation of this in the legal system is the manner in which the boundaries of the legal system are defined by the binary code legal/illegal.[5] In this way, systems can be seen as being 'operationally closed'.[6] This operational closure is additionally characterised by the ability of the system to reproduce itself internally, and develop and evolve in a decentralised, organic and independent manner.

In addition to being operationally closed, systems are also 'cognitively open',[7] meaning that they are influenced by other systems and often evolve in a similar manner and direction with other systems through a process of 'structural coupling'. This means in practical terms, for example, that developments in politics influence developments in economics, as has been the case historically, and these, in turn, influence developments in law. Key to the evolution of systems based on their being operationally closed but cognitively open is the concept of 'reflexion', which is the process of (internal) self-awareness that allows each

[2] N Luhmann, 'The Autopoiesis of Social Systems' in F Geyer and J Van d Zeuwen (eds), *Sociocybernetic Paradoxes: Observation, Control and Evolution of Self-Steering Systems* (Sage 1986).
[3] The term 'autopoiesis' refers to a system capable of reproducing and maintaining itself by regulating its composition and conserving its boundaries (Merriam-Webster Dictionary).
[4] N Luhmann, 'The World Society as a Social System' in N Luhmann, *Essays on Self-Reference*. (CUP 1990) 178.
[5] R Rogowski, *Reflexive Labour Law in the World Society* (Edward Elgar 2013) 34.
[6] N Luhmann, *A Sociological Theory of Law* (Routledge and Kegan Paul 1985) 281 -8
[7] ibid.

system to distinguish itself from other systems, through the application of second-order or high-level norms, such as the binary code existing in the legal system. This understanding of the development of systems is particularly poignant, in that it isolates the mechanisms through which norms are developed to form an existential rationale to the functioning of each system. By drawing on the concept of autopoiesis in the formulation of a theory of reflexive law, Teubner allows for its use in the consideration of metatheoretical issues about the role and function of law in a complex society.

4.3.2 Socially Adequate Complexity

The next basis for reflexive law, after the grounding in autopoiesis, is the notion of 'socially adequate complexity'[8] in which 'it is the difference in complexity between a social system and its environment that produces changes in the social systems'.[9] The implications of this in the understanding of reflexive law is that the law has to 'adapt to specific social differentiation',[10] culminating in a combination of norm rationality (explained by autopoiesis) and system rationality,[11] which together 'determine the constraints on the internal conceptual, procedural and organisational structures of the legal system'.[12] What Teubner essentially presents here is the need for the law to take cognisance of the limitations of its ability to directly influence other systems, not only as a matter of practicality, but also as essential to its continued evolution and internal coherence. This direction in Teubner's theory was influenced by Luhmann's observation that the historical change from a stratified to a functionally differentiated society 'demanded a parallel transition in the legal order', with an emphasis on the need for self-reflexion by the legal system.[13]

[8] G Teubner, 'Substantive and Reflexive Elements in Modern Law (1983) 17 Law & Soc Rev 239, 246.
[9] ibid 263.
[10] ibid 263.
[11] ibid 262.
[12] ibid 262.
[13] ibid 244.

Failure to understand the limitations of the law, and how it influences and is influenced by other systems, will result in regulation being trapped in what Teubner describes as a 'regulatory trilemma', in which regulation and legal rules exhibit (a) failure to shape social practices (lack of effectiveness), (b) the values and techniques represented in regulation fail to fit with pre-existing norms and social ordering in the target population (lack of responsiveness), and (c) where 'regulation that is too responsive to customs from civil society may subvert the doctrinal coherence of law's analytic framework' and potentially lead to 'the failure of effective and responsive regulation to secure certainty, consistency, and predictability in legal principles and values' (lack of coherence).[14] According to Teubner, these common regulatory failures are a result of misdirected legalisation and juridification aimed at other social systems where the law is pushed, often by political forces, to go beyond the scope of autopoiesis in a futile attempt to forcibly determine the internal structures of other systems. Here Teubner asserts that it is only by being reflexive that the law can overcome the regulatory trilemma, and simultaneously achieve effectiveness, responsiveness and coherence by facilitating self-regulation in other systems.[15]

4.3.3 Proceduralisation

In addition to providing a normative basis for considering the role of the law in regulation, Teubner's theory on reflexive law is also prescriptive, as it states that self-regulation in other systems can be shaped and (re)directed towards the attainment of regulatory goals through the use of procedures. He posits that it is primarily through putting in place procedural boundaries, aimed at improving the quality of internal self-regulatory processes, that the law can ensure that regulatees conform to desired outcomes. In other words, reflexive law 'seeks to design self-regulating social systems through norms of organisation and procedure'.[16] More specifically, reflexive law relies on 'procedural norms that

[14] C Parker and J Braithwaite, 'Regulation' in M Tushnet and P Cane (eds), *Oxford Handbook of Legal Studies* (OUP 2005) 129.
[15] R Rogowski (n 5).
[16] G Teubner (n 8) 254.

regulate processes, organisation, and the distribution of rights and competencies'.[17] In this way, under the procedural and organisational orientation of reflexive law, legal control of social action is 'indirect and abstract'.[18] Citing the example of contract law, Teubner defines reflexive law as affecting 'the quality of outcomes without determining the agreements that can be reached'.[19] Here it can be seen that the aim of reflexive regulation is to influence regulatees to expand the remit of their internal self-regulatory structures to include addressing issues of regulatory concern. This can be seen as a mechanism which calls for the law to boost or amplify internal governance structures, and strengthen and channel these towards reaching the desired regulatory outcomes. Teubner advocates the use of procedures rather than substantive rules, based on an understanding that 'the role of reflexive law is to structure and restructure semi-autonomous social systems by shaping both their procedures of internal discourse and their methods of coordination with other social systems'.[20]

In sum, reflexive regulation calls for a new form of 'legal self-restraint', where 'instead of taking over regulatory responsibility for the outcome of social processes, reflexive law restricts itself to the installation, correction and redefinition of democratic self-regulatory mechanisms'.[21] In this way, a reading of Teubner informs the view that reflexive regulation is the only way to ensure that regulation significantly shapes the actions of the regulatee (is effective), is assimilated in a way the regulatee understands and can incorporate (responsive), and is done in a manner which does not compromise the doctrinal foundations of the law as an independent system (coherence).

[17] ibid 255.
[18] ibid 256.
[19] ibid 256.
[20] ibid 255.
[21] ibid 276.

4.3 Reflexive Regulation vis-à-vis established regulatory theories and strategies

4.3.1 Beyond Command and Control vs Self-Regulation

Regulatory theory initially oscillated between the concepts of 'command-and-control' and 'self-regulation'. However, regulatory theory has since evolved beyond the simplistic either/or divide between command-and-control and self-regulation, towards more sophisticated and nuanced views embracing both approaches. This has largely been due to the failure of traditional, black-letter, top-down administration of rules, backed by sanctions in preventing market failures and the equally ineffective option of leaving it solely up markets to restrain themselves. In Financial Regulation, command-and-control—or 'mechanisms involv[ing] the state promulgation of legal rules prohibiting specified conduct, underpinned by coercive sanctions (either civil or criminal in nature) if the prohibition is violated'[22] —have generally been sparingly applied, due to the need for a certain level of autonomous market mechanisms—such as demand and supply—to be allowed to work effectively. This means that, were regulation—defined as any policy which alters market outcomes by the exercise of some coercive government power[23]—purely to be command-and-control would move the global economy away from the key tenets of capitalism, introducing inefficiencies.[24] These concerns over the imposition of highly prescriptive rules have been consistently raised, due to the fact that command-and-control systems are often 'expensive, intrusive and inflexible', and that because one size does not fit all, particularly in financial regulation, 'regulations inevitably distort the economic outcome, possibly so much that the end result is

[22] B Morgan and K Yeung, *An Introduction to Law and Regulation* (CUP 2017) 80.

[23] G Stigler, 'The Theory of Economic Regulation' (1971) 2 (1) Bell Journal of Economics and Management Science 3, 4.

[24] An alternative view, which takes issue with the pejorative labels for command-and-control regulation (such as 'socialist central planning'), shows how command-and-control regulation of the environment can be nominally more efficient than market-based regulations (D Cole and P Grossman, 'When Is Command-and-Control Efficient? Institutions, Technology, and the Comparative Efficiency of Alternative Regulatory Regimes for Environmental Protection' (1999) *Articles by Maurer Faculty* Paper 590.

worse than the unregulated starting point'.[25] Other weaknesses of this approach have been that it has been seen to disregard the complexity of risks, impede firms from choosing their own, more effective mechanisms for meeting objectives, it may stifle innovation, and is focused more on processes rather than outcomes (box-ticking in cumbersome red tape and rules escalation).[26]

More tellingly, command-and-control has been described as limiting the incentives of regulatees to monitor and control their own behaviour and to exercise due diligence where necessary. This aspect is particularly pertinent to the financial sector, where free markets require considerable internal infrastructure and self-regulation to function efficiently with minimal transaction costs,[27] and where, more generally, regulators are dependent on the specialised expertise of regulated firms in order to achieve regulatory outcomes. However, these shortcomings of command-and-control regulation, and the recognition of the crucial role of the regulatee in the regulatory process do not mean self-regulation is a panacea for addressing the oversight of markets. Self-regulation is equally problematic. Its understandable appeal, in both theory and practice, lies in its ability to address the limitations of command-and-control in the areas of efficiency, flexibility and cost-effectiveness, based partly on the use of industry expertise to identify and address issues of regulatory concern.[28] An additional boon for self-regulation is that it is based on the recognition that 'the capacity to deliver on regulatory objectives lies primarily with those who are regulated, rather than those who regulate',[29] as it has been acknowledged that regulators are 'inextricably dependent for their success on the behaviour of

[25] C Goodhart and others, *Financial Regulation: Why, How and Where Now?* (Routledge 1998) 4
[26] ibid.
[27] R Coase, 'The Problem of Social Cost' (1960) Journal of Law and Economics 3, 1.
[28] ibid.
[29] C Scott, 'Reflexive Governance, Regulation and Meta-Regulation: Control or Learning?' in O De Schutter and J Lenoble (eds), *Reflexive Governance: Redefining the Public Interest in a Pluralistic World* (Hart 2010) 3.

individuals and organisations which are autonomous and thus inherently ungovernable'.[30]

The application of self-regulatory regimes has led to various waves of deregulation, where the market has been deemed as the most effective and most suitable instrument to correct itself and reduce its own negative externalities. In most instances, self-regulation, particularly when preceded by deregulation, leads to economic growth. Examples of this include the 'Big Bang' in the UK under Margaret Thatcher in the mid-1980s, which was credited with 'changing the character of the City from a 'club' to a competitive, and competed for, marketplace',[31] and the various historical booms in markets such as housing, and sectors such as technology prior to their subsequent 'busts'. These busts are often linked to the inefficacy of self-regulation, and how, time and time again, the lack of accountability and the subjective and selective application of regulation—primarily due to the mismatched incentives between organisations and regulators—have almost always led to 'socially sub-optimal outcomes'. [32]

Manifestations of these shortcomings of self-regulation in the financial sector range from failures of initiatives such as 'comply or explain'[33], which was based on letting the market decide whether or not a set of standards were suitable for individual companies, to failures in internal risk-management structures resulting in the implosion of the global financial system as a whole and the crystallisation of systemic risk. Most tellingly, in what was aptly described as being 'slapped by the invisible hand',[34] the 2007–2008 Global Financial Crisis (GFC) can be attributed to a wide interconnected array of factors, prominent amongst which is the failure of self-regulation. Here, as noted by former chairman of the Federal Reserve and deregulation advocate, Alan Greenspan, in his *mea culpa* to the US House of Representatives in 2008, when he concluded that he was

[30] J Black, 'Regulatory Styles and Supervisory Strategies' in N Moloney, E Ferran, and J Payne (eds), *Oxford Handbook of Financial Regulation* (OUP 2015) 247.
[31] ibid 219.
[32] ibid.
[33] Financial Reporting Council, *UK Corporate Governance Code* (2018) 1.
[34] G Gorton, *Slapped by the Invisible Hand: Banking and the Panic of 2007* (OUP 2010).

wrong in ‘presuming that the self-interests of organisations, specifically banks and others, were such that they were best capable of protecting their own shareholders and their equity in the firms’.[35]

The awareness of the shortcomings of both command-and-control and self-regulation in their purest forms have led to a move in regulatory theory and practice, beyond this dichotomy, towards more holistic and integrated approaches which incorporate aspects of both command-and-control and self-regulation in tool-kit-based regulatory models. With regards to the latter, Julia Black noted how ‘the death of command-and-control has been much exaggerated’, because as a matter of necessity, regulators, particularly in the US, still rely on detailed legal rules backed by criminal sanctions.[36] However, this use of command-and-control has been restricted to specific instrumental usage targeted at specific products, for example, the post-GFC EU prohibition and ban on uncovered short sales on sovereign Credit Default Swaps (CDS) trading,[37] or mandatory restrictions and obligations stipulated in licensing and registration requirements for financial institutions.

Similarly, the benefits of self-regulation, combined with the reality of the practical (and normative) necessity of including regulatees at various stages of the regulatory process in varying capacities, has meant that the principles of self-regulation—like those of command-and-control—are still very much alive. As shall be further discussed below, reappearing in hybrid form in so-called ‘new governance techniques’ including principles-based regulation, meta-regulation, and enrolment,[38] and in parts of initiatives such as ‘smart regulation’ and ‘better

[35] Greenspan A, Testimony before the House Committee on Oversight and Government Reform, ‘The Financial Crisis and the role of Federal Regulators’ (*US Government Printing Office* 2008) <https://www.govinfo.gov/content/pkg/CHRG-110hhrg55764/pdf/CHRG-110hhrg55764.pdf> Accessed 19 June 2018.
[36] J Black, ‘Paradoxes and Failures: ‘New Governance’ Techniques and the Financial Crisis’ [2012] 75(6) MLR 1037, 1041.
[37] Articles 12 and 13 of Regulation EU) No 236/2012 on Short Selling and Certain Aspects of CDSs ([2012] OJ L 86/1)
[38] Black (n 30).

regulation', these regulatory tools and processes in which the regulatee plays a key role have been widely implemented.

Beyond the practical implications and implementations, the recognition of the futility of the dichotomous conceptualisation of regulation between self-regulation and command-and-control has additionally informed the development of regulatory theory. Seminal in this area is the theory of Responsive Regulation, put forward by Ayres and Braithwaite specifically to transcend the regulatory debate and move away from 'crude polarisation', in order to strike a balance between self-regulation and command-and-control regulation.[39] The key contribution of responsive regulation lies in the area of enforcement and compliance, where the authors addressed the question of 'when to punish; when to persuade?' by proposing a 'tit for tat' approach in which 'regulators enforce in the first instance by compliance strategies, but apply more punitive deterrent responses when the regulated firms fail to behave as desired'.[40] This notion is expanded further by Baldwin and Black, who posit that in order to be 'really responsive',

> *regulation has to be responsive not merely to compliance performance but to the attitudinal settings of regulatees; to the institutional environment of regulation; to the operation and interplay of the institutional environment of regulation; to its own performance; and to changes in each of these elements.*[41]

'Really responsive regulation' came about as an ambitious, catch-all rejoinder to the conceptual, practical and constitutional criticisms of responsive regulation. These ranged from the inappropriateness of an escalating response to catastrophic crises, and the difficulties of de-escalation down the enforcement

[39] I Ayres and J Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (OUP 1992) 21.

[40] R Baldwin and J Black, 'Really Responsive Regulation' [2008] 71(1) MLR 59, 62.

[41] ibid 69.

pyramid, to challenges to the assumption that regulatees respond to pressures by regulators and critiques to do with fairness, proportionality and consistency.[42]

As shall be further discussed, whilst the application of various hybrid regulatory strategies, including meta-regulation, principles-based regulation, enrolment, risk-based regulation and other strategies, including better and smart regulation are useful—the complex, inter-connected considerations involved in the regulation of cryptocurrencies calls for a theoretical approach that provides a more systemic view of regulation and a consideration of the role and positioning of the law in world society. With this in mind, this study will consider the theory of Reflexive Law developed by Gunther Teubner, as a theoretical approach that presents a holistic metatheory of regulation, and an understanding of where the law stands, both instrumentally and normatively, in relation to regulatory targets. What follows is a consideration of how this approach differs fundamentally from other self-regulation-based approaches as a re-iteration of the suitability of a reflexive law approach to the regulation of cryptocurrencies.

4.3.2 Reflexive Regulation and other Self-Regulation-Based Approaches

Regulatory models and techniques incorporating aspects of both substantive command-and-control and self-regulation have become ubiquitous. What follows is a brief description of how reflexive regulation differs from principles-based regulation, meta-regulation and the varieties of 'smart-regulation' techniques.

4.3.2.1 Principles-Based Regulation

Principles-based regulation was coined and initiated by the UK's Financial Services Authority (FSA) in 2007, after disenchantment with risk-based regulation—a regulatory approach based on the channelling of regulatory resources to areas that pose the highest levels of risk[43]—in the areas of

[42] ibid.

[43] FSA, A New Regulator for a New Millennium (2000) <https://www.fca.org.uk/old-fsa-website> Accessed 3 May 2015.

prudential regulation, as exemplified by the collapse of Northern Rock and the Royal Bank of Scotland (RBS).[44] Stating that 'our aim is to focus more clearly on the outcomes we as regulators want to achieve, leaving more of the judgement calls on how to achieve those outcomes to senior management of firms'.[45] As paraphrased by Rawling, Georgosouli and Russo, the FSA further explained that:

> *detailed rules placed an enormous burden on industry without preventing misconduct, that rules were less flexible and so unable to respond quickly to innovations, that they led to box-ticking rather than adherence to regulatory standards, and that the sheer volume of rules rendered them inaccessible.*[46]

This shift towards principles-based regulation incorporated aspects of self-regulation, by placing the onus on regulatees to determine how they would achieve regulatory outcomes. A practical example of the implementation of the principles-based approach was the FSA's Treating Customers Fairly initiative put in place in the UK in 2003. Deciding to take a conceptual approach to the principle of 'fairness', the FCA left it to firms to define and set substantive standards, and achieve six outcomes towards fairness without mandating rule-based compliance. However, this initiative was curtailed by the onset of the GFC, and its level of success was brought into question by the mis-selling of payment protection insurance (PPI).[47] After the GFC, the principles-based approach was shelved. However, both the FCA and the Prudential Regulation Authority (PRA) at the BOE stated that their approach will be 'judgement based', displaying a similar concern with the achievement of outcomes that was the basis of principles-based regulation.[48] In practice, it has been noted that this shift from rules-based to principles-based regulation, and the distinction between the two, was purely arbitrary. What was observed, in fact, was that the FSA's approach

[44] J Gray, 'Is it Time to Highlight the Limits of Risk-Based Financial Regulation?' [2009] *Capital Markets Law Journal* 4(1).

[45] FSA, 'Principles-based Regulation: Focusing on the Outcomes that Matter' (*FSA* 2007) <https://www.fca.org.uk/old-fsa-website> Accessed 3 May 2015.

[46] P Rawlings, A Georgosouli and C Russo, *Regulation of Financial Services: Aims and Methods* (Queen Mary University of London, Centre for Commercial Law Studies 2014) 18.

[47] J Black (n 30).

[48] ibid.

‘appeared to be principles-based and was promoted as such’, but was really ‘a mix of rules and principles: principles elaborated by rules in certain areas (eg treating customers fairly) and rules supported by principles to cover gaps of inconsistencies’ where ‘a rules-based system may have a principles-based enforcement or sanctioning regime’.[49]

The realities of their application and strengths and weaknesses of each approach aside, what is evident is that, although principles-based regulation placed the responsibility of implementation on regulatees calling for a certain level of self-regulation, the fact that regulatory objectives were set independently by the regulator and imposed on the regulatee in a top-down manner is what distinguishes principles-based regulation from a reflexive regulatory approach. Indeed, it can be argued that principles-based regulation application and the use of self-regulation suffered from a lack of responsiveness, where the given values and techniques prescribed by regulators failed to fit with pre-existing norms and social ordering in the target population, leading to the observed *de facto* (re)incorporation of rules-based approaches within principles-based approaches. In the case of the FSA’s Treating Customers Fairly initiative, a reflexive approach to the use of principles would have entailed the use of procedures, such as, for example, processes to promote transparency, which could indirectly channel regulatees towards fairer practices, and allow for the development of an organic internal conceptualisation of the notion of ‘fairness’, coupled with regulatory initiatives to support the development and direction of internal processes towards fairness.

4.3.2.2 Meta-Regulation

Displaying similar features to principles-based regulation, meta-regulation—often grouped synonymously with management-based regulation and enforced self-regulation—describes a strategy in which ‘regulators do not prescribe how regulatees should comply, but require them to develop their own systems of

[49] P Rawlings (n 46) 18.

compliance and to demonstrate that compliance to the regulator'.[50] Lauded for its links to community-based governance and co-regulation, this regulatory strategy has the advantages of being able to design internal compliance mechanisms suitable to the regulated firm or industry. However, the main disadvantage of meta-regulation, management-based regulation, or enforced self-regulation is that 'the firm's processes are designed to achieve their own goals, not necessarily those of the regulators' meaning that 'compliance systems may therefore end up running parallel to the organisation's core operations, rather than being integral to them'.[51]

The shortcomings of this approach were seen during the GFC, which led to more scrutiny of the decisions of senior management in financial institutions in the wake of a more intrusive regulatory approach by supervisory authorities. As with principles-based regulation, meta-regulation faces the same lack of responsiveness endemic to norm-asymmetries, and the external imposition of regulatory goals and objectives. However, it too can be implemented reflexively. An example of this is Scott's presentation of a reflexive conception of meta-regulation which 'acknowledges that the capacities of individuals and organisations for self-regulation extends beyond implementation and compliance to include the setting of objectives', but suggests that 'the legitimacy of such activities is liable to be premised upon the inclusiveness and character of such self-regulatory processes'.[52]

4.3.2.3 'Smart Regulation' Models of Regulation

Defined as being a 'pragmatic, flexible and pluralistic approach to regulation involving the use of multiple regulatory techniques and a wide range of regulatory actors to implement a regulatory regime',[53] smart regulation has been characterised by the coining of terms such as decentred regulation, collaborative

[50] J Black (n 30) 227.
[51] ibid 227.
[52] C Scott (n 29) 2.
[53] N Gunningham and P Grabovsky, *Smart Regulation: Designing Environmental Policy* (Clarendon Press 1998) 4.

governance, outsourcing regulation and empowering participants.[54] Included in this catch-all concept are ideas of 'better regulation', with an emphasis on regulatory impact assessments, and the above-mentioned risk-based regulation and meta-regulation, all of which lead to what Julia Black noted to be tensions between fragmentation and centralisation within the regulatory state.[55] This is based on the observation that the fragmentation associated with polycentric regulatory models results in increased centralisation by the government, particularly in the area of enforcement, due to the rise in the need for accountability of government regulators combined with a strain in their ability to coordinate the direction of regulation.[56]

Using the analytical framework of reflexive law, the tensions noted here can be seen as a crisis in the coherence of law, and the failure 'to secure certainty, consistency, and predictability in legal principles and values'.[57] As noted by Black, such tensions can lead to the erosion of the gains intrinsic in polycentric and decentred regulatory approaches through excessive central enforcement.[58] Specifically considering the use of enrolment as a regulatory strategy, it can be seen that this approach—in which regulatory roles are assigned based on an assessment of the functions and capabilities of various regulatory actors[59]—differs from reflexive regulation, where 'the primary function of the democratisation of subsystems lies neither in increasing individual participation nor in neutralising power structures but in the internal reflexion of social identity'.[60] Unlike the various smart regulation options which seek to apply an externally configured logic onto regulated communities, the main thesis of reflexive regulation is that it will 'neither authoritatively determine the social

[54] ibid.
[55] J Black, 'Tensions in the Regulatory State' [2007] PL 58.
[56] ibid 58, 59.
[57] G Teubner (n 8) 273.
[58] J Black (n 30) 58, 67.
[59] J Black, 'Enrolling Actors in Regulatory Systems: Examples from UK Financial Services' [2003] PL 63.
[60] Teubner (n 8) 255.

functions of other subsystems nor regulate their input and output performances'.[61]

4.3.2.4 Incentives-based Approaches

Also to be considered are incentives-based approaches. Incentives-based approaches involve the use of negative and positive taxes by the regulator in order to induce the regulatory target to behave in accordance with the public interest.[62] These approaches rely in part on self-regulation as they leave the decision on how to respond to the imposed incentives to the the regulatee. As explained by Baldwin, Cave and Lodge, in the example of using an incentives-based approach to curb pollution, 'it is up to the regulated firm, not the bureaucrat or regulator, to balance the costs of polluting against those of abatement in a particular context and to devise means of reducing the mischief most efficiently'[63]. Whilst the use of incentives provides numerous advantages including the reduction of the possibility of regulatory capture and lowering of costs, the use of incentives entails the putting in place of 'highly complex systems of rules' which leads them to replicate some of the shortcomings found in command and control regulation.[64] For this reason, it is not a suitable approach to cryptocurrency regulation given then ineffectiveness of rules-based systems as described above.

4.3.2.5 Disclosure Requirements

Another regulatory instrument that relies in part of self-regulation is the use of disclosure requirements. This entails obliging the regulatory target to supply the public with information about various aspects of the product or services offered, such as price, production process and quality, leaving it up to the consumers of the product or service to decide on whether or not to purchase the product or

[61] ibid 275.

[62] R Baldwin, M Cave and M Lodge, *Understanding Regulation: Theory, Strategy and Practice.* (OUP 2012).

[63] ibid 112.

[64] ibid 113.

service.[65] Disclosure requirements are already a key component of the current cryptocurrency regulation regime where concerns around consumer and investor protection have led regulators to mandate the clear and accurate disclosure of the risks involved in the acquisition and trading of cryptocurrency. For example, as highlighted in Chapter 2, various regulators around the world mandate the protection of consumers by providing initial and per transaction disclosures of risks, terms and conditions, complaints policies and disclosures, advertising and marketing requirements.[66] Whilst disclosure requirements are aligned with reflexive regulation in providing 'a mode of regulation that is not heavily interventionist'[67] disclosures have been a component of an inadequate regulatory approach to cryptocurrencies as has been previously alluded to. This may, in part be a result of the inherent weaknesses of a disclosures where consumers 'may make mistakes; they may fail to use the information properly; fail to understand the implications of the data given; mis-assess risks; neglect to collect the full range of relevant information; lack the resources and expertise to research issues fully; and so may come to harm.'[68] This has been particularly true of cryptocurrencies whose novelty and complexity makes it difficult for the average consumer to accurately assess risk as a certain level of technical proficiency and financial literacy is required to understand and assess the merit of each offering. Most significantly, the use of disclosure requirements is a standalone regulatory instrument that can be used, as is currently the case, in combination with other regulatory instruments. It is not, in itself, a theory of regulation in the same way reflexive regulation is.

4.3.2.6 Imposition of Rights and Liabilities

An additional indirect regulatory instrument is the imposition of rights and liabilities. This involves assigning rights to the parties the regulators is aiming to

[65] ibid 119.

[66] For example, see New York Department of Financial Services (*NYDFS* 2015), 'BitLicense Regulatory Framework' <https://dfs.ny.gov/legal/regulations/bitlicense_reg_framework.htm> Accessed 3 July 2018.

[67] R Baldwin, M Cave and M Lodge (n 64) 119.

[68] ibid 120.

protect combined with liabilities to the regulatory target when these rights are violated.[69] The aforementioned consumer and investor protection instruments in financial regulation clearly establish rights relevant to cryptocurrency market participants in particular the duty of care that financial intermediaries have towards investors and consumers. Where these rights are violated, liabilities accrue. An example of this is the enforcement action targeted at cryptocurrency intermediaries that have violated consumer and investor rights, including the ongoing class actions in the US against collapsed cryptocurrency exchanges. However, the key challenges of establishing liability in cryptocurrency transactions has been extensively discussed in Chapter 1 where it was highlighted that the technical features of cryptocurrencies (including decentralisation and pseudonymity) limit the scope of substantive legal instruments. In this way, this regulatory instrument is already in use in current cryptocurrency regulation and has proved inadequate in combination with other regulatory tools currently in use and is not a standalone regulatory theory.

4.3.2.7 Nudge Strategies

The final self-regulation-based regulatory strategy to be considered is nudging. Nudge strategies involve the structuring of decisions or choice architectures, so that it is easier for regulatees to act in a desirable manner.[70] On the surface, nudging appears well-aligned to reflexive regulation as reflexive regulation calls for the law to structure and restructure the target social system by 'shaping both their procedures of internal discourse and their methods of coordination with other social systems'.[71] However, by being premised on the notion of 'libertarian paternalism' which in essence calls for the 'rigging of the decision architecture'[72] nudging deviates from reflexive regulation by failing to account for and appreciate the operational closure and legitimate internal logic of systems, focusing on the manipulation of outcomes rather than on improving the quality

[69] ibid 121.
[70] ibid 123.
[71] G Teubner (n 8) 255.
[72] R Baldwin, M Cave and M Lodge (n 64) 123.

of internal self-regulatory processes. Similarly, the observation that processes of nudging are 'value-laden yet low in transparency' and that 'evaluation of an outcome's merits may reflect the nudger's conception of the good rather than the nudgee's'[73] is incompatible with the reflexive stance not to impose purpose-orientationon regulatory targets as shall be described below. It can be envisaged that this approach would be particularly problematic in cryptocurrency regulation, where the complexity of the cryptocurrency system extends beyond the 'opt-out' option favoured by nudge strategies[74], and where the novelty and diverse approaches to cryptocurrency regulation means that 'nudge outcomes whose merits are debatable and contested'[75] are highly likely to develop, resulting in a lack of legal coherence as depicted in the regulatory trilemma.

4.4 Discussion

4.4.1 Reflexive Regulation and Self-Regulation

In sum, the overall similarities between reflexive regulation and the above-mentioned approaches have to do with the provision of a role of self-regulation. At this point, it would be useful to make explicit the difference between reflexive regulation and the understanding of self-regulation as a stand-alone regulatory strategy, as presented in section 4.3.1 of this chapter. Rather than delegating aspects of the regulatory process to the regulatee, in expectation of compliance to prescribed outcomes, reflexive regulation is aimed at regulating self-regulation, primarily through proceduralisation and institutionalisation.

The manner in which reflexive regulation differs from self-regulation is illustrated by how Teubner notes the existence of reflexivity in areas where self-regulation has been seen to fail, such as consumer protection. By citing the example of the artificial creation of autonomous institutions in Germany that provide consumer information and consumer representation, Teubner notes

[73] ibid.
[74] ibid.
[75] ibid 124.

how in this case, taking a reflexive approach means that 'the law does not decide what constitutes consumer's interest, it restricts itself to defining competencies for the articulation of consumer interests and to securing their representation'.[76] In this way, in reflexive regulation, the focus of legal attention is on 'creating, shaping, correcting, and redesigning social institutions that function as self-regulating systems',[77] similar in some ways to the regulatory strategies discussed above. However, the key distinguishing feature of reflexive regulation is that this is done in order to 'produce a harmonious fit between institutional structures and social structures *rather than influence the social structures themselves*'.[78] Moreover, in addition to not prescribing ways and means of social integration, a reflexive approach does not apply formal rules that lead to the infusion of 'purpose-orientation'.[79] Instead, the task of the legal system in reflexive law is 'neither to develop its own purposive programme nor to decide goal conflicts between competing policies. It is to guarantee coordination processes and to compel agreement'.[80]

In this way, reflexive regulation differs from other regulatory approaches by providing a complete theory of regulation that provides grounding of the role and purposes of the law, and the mechanisms through which this purpose can be realised. The justification of law in reflexive legal rationality is the controlling of self-regulation; the external functions of law are the structuring and restructuring of systems for internal discourse and external coordination; and the internal structures of law have a procedure orientation.[81]

4.4.2 Learning over Compliance

The final factor that distinguishes reflexive regulation from other regulatory models is the emphasis on learning as a regulatory outcome. Learning is a natural

[76] ibid 277.
[77] ibid 251.
[78] ibid (emphasis added).
[79] ibid 255.
[80] ibid 277.
[81] ibid 257.

by-product of the reflexive process because, as Teubner asserts, when law serves as an institution that facilitates self-regulatory processes of communication and learning, it plays a role that is 'congruent with emergent forms of discursive rationality', and because of its procedural orientation, is 'well-suited to the legitimation problems of post-modern society'.[82] This learning capacity of reflexive law is illustrated by the European Commission's Reflexive Governance (REFGOV) project, which is based on the attempts to redefine governance on the basis of the learning imperative.[83] In this project, the various methods aimed at implementing reflexive governance range from neo-institutionalism to collaborative-relational models, that are all based on the recognition of learning as a corollary to the implementation of reflexive governance structures, in which learning is not taught and solutions are not to be imposed from above, but rather emerge organically from below. [84]

Taking the same view, comparing reflexive governance to meta-regulation with the former characterised by learning and the latter characterised by control, Scott opines that the GFC can be attributed to a lack of understanding of the functioning and interdependence of global markets; in this view, 'it is developing a better capacity for learning, rather than control, that has potential to prevent the re-emergence of crisis of this kind'.[85] The learning component of reflexive law has to do with the fact that it allows for the 'harnessing of the learning capacity associated with non-state actors', and its focus on procedures rather than on prescribed goals facilitates and encourages 'deliberation and mutual learning between organisations'.[86] Embedded in an understanding of autopoiesis and facilitated by communication, this learning process is bi-directional, and propels both the regulated and the regulatee to more evolved forms of interaction, where

[82] ibid 269.

[83] Details of the programme available at <http://sites.uclouvain.be/cpdr-refgov/>

[84] O De Schutter and J Lenoble, 'Introduction: Institutions Equipped to Learn in O De Schutter, and J Lenoble (eds), *Redefining the Public Interest in a Pluralistic World* (Hart Publishing 2010) xxiv.

[85] C Scott (n 29).

[86] N Gunningham, 'Regulatory Reform and Reflexive Regulation: Beyond Command and Control' in E Brousseau, T Dedeurwaerdere, and B Siebenhner (eds), *Reflexive Governance and Global Public Goods* (MIT Press 2009) 87.

‘regulation is achieved through mechanisms that systematically further the development of reflexion structures within other social subsystems’.[87]

4.4.3 The Need and Opportunity for Self-Reflexion within the Law

It is evident that the advent of cryptocurrency and other technology-based phenomena calls for a change in the way the law positions itself. As noted by Teubner, ‘substantive legal rationality attempts to regulate social structures by legal norms, even though these structures do not always or easily bend to legal regulation’,[88] and it is clear that cryptocurrencies in particular do not easily fit into existing substantive legal definitions and regulations. This necessary change in the law will require a process of internal self-reflexion within the legal system. By providing an understanding of the cognitive openness of systems and how these can learn from each other, the reflexive regulation of cryptocurrencies will allow for the internal evolution of the legal system. This is because, as noted by Rogowski, ‘reflexive processes can be used to change structures and to overcome rituals’[89] where the internal self-awareness that takes place through reflexive mechanisms would allow for the consideration of second-order norms in law, leading to outcomes such as ‘the introduction of legislation that regulates legislation … decisions about how to decide … and solving conflicts that arise from conflict resolution’.[90]

Teubner’s theory on reflexive law provides a basis for understanding the need and ability for such an evolution, by establishing the ‘self-reference of legal structures’, through autopoiesis, that allows legal structures to ‘reinterpret themselves … in the light of external needs and demands’ and, in so doing, enabling them to retain their distinctively legal character, without losing a

[87] Teubner (n 8) 275.
[88] ibid 274.
[89] R Rogowski (n 5) 35.
[90] ibid 35.

broader social sciences-based perspective, leading to a ‘rematerialisation of the law’ into a new form.[91]

This view is largely echoed by Tunney who, on considering the reflexive role of law in regulating cyberspace, argues that the development of legal system, and the development of communications technology are reflexively related, and that failure to consider the general, individual and cumulative effects of communications technology on law, and of law on communications technology, will inevitably lead to ‘flawed anticipations’.[92] This assertion is based on the opinion that the current legal system and legal establishment is plagued by systemic problems, including

> *relative dysfunctionality, the recurrences of miscarriages of justice, the redundancy of and irrelevancy of legal concepts, the persistence of legal exclusion, discontent in the mirror of the zeitgeist, the failure of enforceability and the crisis in the legal profession…*[93]

and that ‘the advent of Communications Technology promises to address and correct some of these issues’—both as a threat and as an opportunity. Tunney’s conclusion is that reflexive paradigms in which communications technology is incorporated bi-directionally in a new ‘Tao of Law’ will lead to, amongst an extensive list of benefits, the minimisation and prevention of the occurrence of systems failures, through ‘utilising the optimum synthesis of interdisciplinary knowledge’.[94]

Whilst a reflexive approach to the regulation of cryptocurrencies might not immediately produce a new Tao of Law, it does present an opportunity to consider the seemingly paradoxically expansion of the remit of the law through considered self-restraint. The law is cognitively open to this change, because as

[91] Teubner (n 8) 279.

[92] J Tunney, ‘Notes on the Reflexive Role of Cyberspace’ [2000] *International Review of Law Computers and Technology* Volume 14, No 2, 243.

[93] ibid 244.

[94] ibid 253.

noted by Moloney et al, ‘change and innovation have encompassed regulation in action (in particular supervision and enforcement) as well as rule design’[95] and that the institution of law—like that of the state, the market, and finance—is a ‘complex system with adaptive properties’.[96]

4.5 Conclusion

With the view of presenting an alternative approach to cryptocurrency regulation in mind, this chapter has introduced the theory of reflexive law and regulation as posited by Teubner. The chapter commenced by providing an overview of reflexive regulation, explaining its basis in systems theory and autopoiesis, socially adequate complexity and proceduralisation. Here, it was shown that by drawing on these three concepts in the formulation of a theory of reflexive law, not only can practical considerations around avoiding the regulatory trilemma be addressed using proceduralisation, the metatheoretical issues concerning the role and function of law and the legal system in a complex society can be contended with.

With this understanding in mind, the chapter proceeded to position reflexive regulation vis-à-vis other established regulatory theories and strategies. Here is was shown how regulatory theory has moved beyond the simple dichotomous categories of command-and-control and self-regulation. By considering the differences between reflexive regulation and other self-regulation-based approaches, it was seen that reflexive regulation falls under theories that advocate some form of self-regulation and is further away from theories that are about imposing substantive rules.

However, the main contribution of reflexive regulation lies in providing an understanding of the limitations of the law, and how it influences and is

[95] N Moloney, E Ferran and J Payne, ‘Introduction’ in N Moloney, E Ferran, and J Payne (eds), *Oxford Handbook of Financial Regulation* (OUP 2015) 2.

[96] S Deakin, ‘The Evolution of Theory and Method in Law and Finance’ in N Moloney, E Ferran and J Payne (eds) *Oxford Handbook of Financial Regulation* (OUP 2015) 15.

influenced by other systems, framing the shortcomings of each regulatory approach, including the new governance techniques, as natural ramifications of the operational closure of each system. Most tellingly, it solidifies the notion that regulatees should form the cornerstone of any effective regulatory strategy, because self-regulation is more than a context-specific option—it is presented as the only way through which the law can significantly influence and shape the direction of the evolution of other systems, including that of the regulatory target.

In this way, Teubner's theory of reflexive law allows for the realistic assessment of the role, position and influence of the law in relation to other systems, and calls for a process of self-reflexion within the law, combined with placing an onus on the law to attempt to understand the systems upon which it wishes to exert its influence, and, by so-doing, presents a holistic metatheory of regulation that provides an understanding of where the law stands, both instrumentally and normatively, in relation to regulatory targets. By allowing for learning over compliance and facilitating self-reflexion within the law, reflexive regulation offers a theory of regulation that is well-suited to addressing the regulatory challenges and opportunities presented by the advent of cryptocurrencies.

Chapter Five: Internal Self-Regulatory Mechanisms of the Cryptocurrency System

> *A reflexive orientation ... seeks to identify opportunity structures that allow legal regulation to cope with social problems without, at the same time, irreversibly destroying valued patterns of life*[1]

5.1 Introduction

This chapter is aimed at presenting the main mechanisms through which the cryptocurrency system self-regulates and self-governs. This is a necessary pre-cursor to the core component of reflexive regulation, which is to redirect internal self-regulatory mechanisms towards regulatory goals. With this in mind, the chapter identifies the two main internal governance mechanisms within cryptocurrency system as 'Code' and 'Consensus'. These mechanisms are described and analysed in turn, with a focus on their operational closure (functionality) and cognitive openness (regulability). This will be done with an emphasis on highlighting not only the avenues and means for legal intervention within these internal governance structures, but identifying the role of law and legal intervention in ameliorating these self-regulatory mechanisms, in order to address the issues of regulatory concern.

As has been discussed in the preceding chapter, Teubner's theory of reflexive law and regulation posits that it is impossible for the law to exert influence upon or to regulate another system without engaging with that system reflexively, and that failure to do so will present a regulatory trilemma.[2] The first logical step in reflexively engaging with a system, successfully implementing a reflexive regulation approach and arriving at a reflexive regulatory outcome is to initially seek to understand the internal regulatory structures and mechanisms of the

[1] G Teubner, 'Substantive and Reflexive Elements in Modern Law (1983) 17 Law & Soc Rev 239.

[2] G Teubner, 'Juridification: Concepts, Aspects, Limits, Solutions', in G Teubner (ed), *Juridification of Social Spheres: A Comparative Analysis of the Areas of Labour, Corporate, Antitrust and Social Welfare Law* (W de Gruyter 1987).

target system. This understanding is crucial to the success of the second, enforcement-orientated element of reflexive regulation—namely the redirection of these internal self-regulatory mechanisms towards wider issues of regulatory concern.[3]

In a study identifying lessons for self-enforcing online dispute resolution from Bitcoin, Ortolani argues that Bitcoin's internal dispute resolution mechanisms, with their capacity to enforce the outcome of procedures autonomously, signal the existence of an 'enforcement jurisdiction', with the power to enforce its own norms, which can 'rightly considered to be an indicator of the existence of an autonomous legal order'.[4] Linking this view of Bitcoin as an autonomous legal system to Legal Darwinism, Ortolani focuses on the ability of the Bitcoin system to self-enforce and conduct private adjudication in instances where there is a need to determine the final recipient of a disputed sum of money using multi-signature addresses.[5] By permitting the execution of a transaction only upon authorisation by two out of three locks involving the two contracting parties and an adjudicator, multi-signature wallets, along with the provision for escrow coding, provide internal dispute resolution mechanisms that can be seen to form part of the internal self-regulatory and self-governance mechanisms of cryptocurrency.

Expanding on these observations, this chapter will take a broader view based on an analysis of the functioning of the cryptocurrency system, which reveals that there exist two main overarching internal self-regulatory mechanisms and internal governance structures in cryptocurrencies, namely computer 'Code' and 'Consensus'. Here, it is evident that cryptocurrencies are code-governed by the rules embedded in their design, and that these rules are, in turn, modified and moderated by consensus-based distributive governance mechanisms. The former conceptualisation is primarily based on the understanding of code as law,

[3] Teubner (n 1).
[4] P Ortolani, 'Self-Enforcing Online Dispute Resolution: Lessons from Bitcoin' (2016) 36 (3) OJLS 595, 615.
[5] ibid.

first introduced by Lawrence Lessig,[6] and the latter assertion is supported by observations on the internal governance structures open source software, as canvassed by the Oxford-based OSS Watch.[7]

What follows is a discussion of the internal self-regulation and self-governance of cryptocurrency system through Code and Consensus through the lexicon of autopoeisis, namely the operational closure, or uniquely self-contained rationality of the system, and cognitive openness, or the extent to which the system is open to influence by and from other systems.[8] More specifically, in this chapter, operational closure will describe the functionality or modus operandus through which code and consensus govern cryptocurrency, whilst cognitive openness will consider two things: (a) regulability of code and consensus, examining whether or not it is possible for the law to influence this system, whether or not there are any avenues through which the law can influence this system, and whether or not there is an openness or willingness in this system to be influenced by the legal system; (b) whether or not there is a *need* for legal intervention in the internal governance structure and the consideration of the role of law in this system.

5.2 Code

5.2.1 Introduction

Simply put, computer code is a set of rules or instructions made up of words and numbers, which, when ordered correctly, will instruct a computer to perform a function.[9] The process of writing and developing computer code ('programming') has near ubiquitous functionality, in the creation of everything from video games to rocket launches, and the financial services sector is not exempt from the

[6] L Lessig, *Code 2.0* (2nd edn, Basic Books 2006).

[7] R Gardler and G Hanganu, 'Governance Models' (OSS Watch, 2010) <http://oss-watch.ac.uk/resources/governancemodels> Accessed 15 May 2017.

[8] Teubner (n 2).

[9] BBC Bitesize, 'What is Code?' (*BBC* 2017) <http://www.bbc.co.uk/guides/zykx6sg> Accessed 15 May 2017.

influence of code. Algorithms—the sequence of rules underpinning computer code[10]—have been a part of the global financial system since the onset of digitisation, decades before the development of cryptocurrencies. Even simple activities, such as the electronic transfer of a specified amount of money from one bank account to another, are pre-programmed and executed by computer code, and maintained by computer algorithms;[11] it has been noted that the modern financial system is 'heavily reliant' on computer code, which 'governs the creation and amendment of the digital records of the legal obligations between institutions'.[12]

However, the introduction of cryptocurrencies presented an elevated role for computer code in financial services, beyond just a task-based functionality. In cryptocurrencies, the code not only specifies *how* the cryptocurrency works, but also *creates* the currency. Unlike fiat or everyday currency, where physical bank notes are printed out by the reserve or central bank, cryptocurrencies are generated autonomously online by the running of code. This means that computer code is the bedrock of cryptocurrency, and is the fundamental internal governance mechanism of this system. Here, it is the code that determines and enforces the rules that each participant in the cryptocurrency network must follow, and controls what types of transactions are possible or permissible. In its generative capacity, in addition to governing what the users who have downloaded the software code can or cannot do, cryptocurrency code also regulates the rules surrounding the creation of cryptocurrency where, for example in the case of Bitcoin, a cap is put on the size of the money pool.[13] In this instance, it is code that governs and regulates, as 'there are no bylaws or other

[10] ibid.

[11] V Lehdonvirta and R Ali, 'Governance and Regulation' in M Walport, 'Distributed Ledger Technology: Beyond Blockchain' (Report by Sir Mark Walport, UK Government Chief Scientific Adviser, Government Office for Science 2016) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf> Accessed 20 May 2016.

[12] ibid 41.

[13] S Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (*Unpublished Manuscript* 2008).

legal documents stating these rules, and no humans to enforce them—distributed ledger systems are government by their own software code only'.[14]

In this way, as has been prominently observed by Lawrence Lessig, the conceptualisation of cyberspace or internet-based systems (such as that of cryptocurrencies) as ungoverned and ungovernable, or as unregulated and unregulatable is erroneous, because cyberspace regulation is conducted by and through code. Here, 'important rules are imposed, not through social sanctions, and not by the state, but by the very architecture of the particular space. A rule is defined, not through statute, but through the code that governs the space'.[15] To re-emphasise, the paramountcy of code in the self-regulation of the cryptocurrency system is doubly significant in the dual role of code, as both the generator of value and the maintainer of system functionality.

5.2.2 Code Operational Closure (Functionality)

As has been described in Chapter 1, the first and original cryptocurrency, Bitcoin, was developed by Satoshi Nakamoto who, in 2008, published a white paper explaining the functionality of Bitcoin and the rationale for its development. In addition to the white paper, freely downloadable open-source software (Bitcoin Core) was made available online. Downloading and running Bitcoin Core not only deploys the Bitcoin system, 'implement[ing] all aspects of the Bitcoin system, including wallets, a transaction verification engine with a full copy of the entire transaction ledger (blockchain), and a full network node in the peer-to-peer Bitcoin network',[16] it also allows for and calls on software developers from anywhere in the world to contribute to further development of the software, and participate in testing and sharing results with the developer community on a dedicated forum.[17] Primarily, Bitcoin Core activates through code the various

[14] V Lehdonvirta and R Ali (n 11) 42.

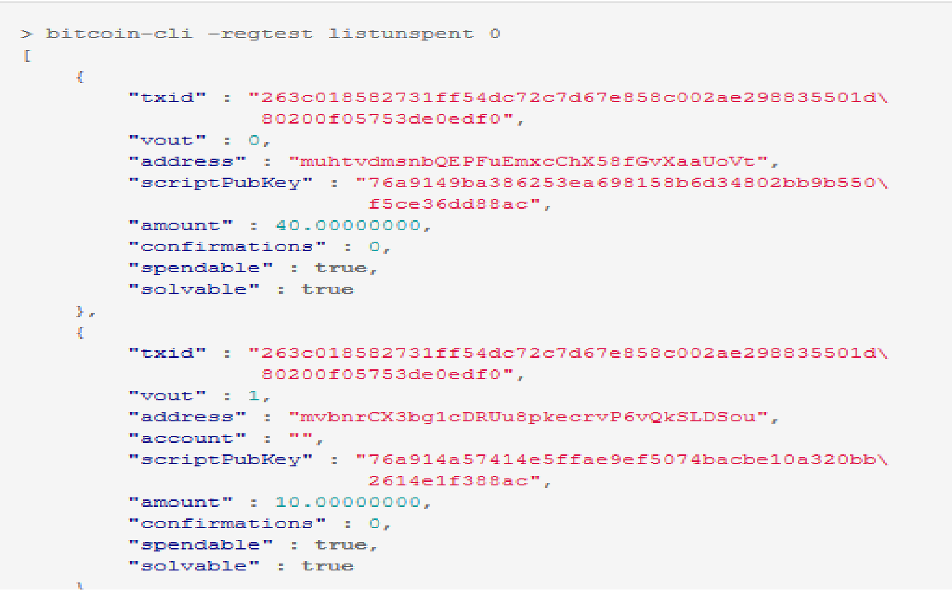
[15] L Lessig (n 6) 24.

[16] A Antonopoulos, 'Mastering Bitcoin: Unlocking Digital Cryptocurrencies' (O'Reilly Media Inc, 2014) 31.

[17] Github, 'Bitcoin Core Integration' (*Github* 2017) <https://github.com/Bitcoin/Bitcoin> Accessed 24 July 2017.

components of the functioning of Bitcoin, as described in Nakamoto's white paper. For example, the white paper defines a Bitcoin 'electronic coin' as a 'chain of digital signatures'.[18] These digital signatures allow each owner to transfer the coin to the next by digitally signing a 'hash' (an encrypted and abbreviated version of the string of text describing the previous transaction), and by also digitally signing the public key of the next owner, and adding these to the end of the coin and, in this way, allowing for the verification of the chain of ownership.[19] This first and basic component of Bitcoin is coded into Bitcoin Core through a series of letters and numbers instructing the computer or device running the software, step by step, as to the rules by which a transaction is generated and executed. Viewed in programming language, this process operationalising the first component of a Bitcoin transaction as described in Nakamoto's white paper and run using the Bitcoin Core software, would create responses to software queries similar to that depicted in Figure below, which shows the confirmation of transactions belonging to one particular wallet.

Figure 6: Bitcoin Transaction Confirmation



```
> bitcoin-cli -regtest listunspent 0
[
    {
        "txid" : "263c018582731ff54dc72c7d67e858c002ae298835501d\
                  80200f05753de0edf0",
        "vout" : 0,
        "address" : "muhtvdmsnbQEPFuEmxcChX58fGvXaaUoVt",
        "scriptPubKey" : "76a9149ba386253ea698158b6d34802bb9b550\
                          f5ce36dd88ac",
        "amount" : 40.00000000,
        "confirmations" : 0,
        "spendable" : true,
        "solvable" : true
    },
    {
        "txid" : "263c018582731ff54dc72c7d67e858c002ae298835501d\
                  80200f05753de0edf0",
        "vout" : 1,
        "address" : "mvbnrCX3bg1cDRUu8pkecrvP6vQkSLDSou",
        "account" : "",
        "scriptPubKey" : "76a914a57414e5ffae9ef5074bacbe10a320bb\
                          2614e1f388ac",
        "amount" : 10.00000000,
        "confirmations" : 0,
        "spendable" : true,
        "solvable" : true
    }
```

Source: bitcoin.org[20]

[18] Nakamoto (n 13) 2.
[19] ibid.
[20] Bitcoin.org, 'Bitcoin Developer Examples' (*Bitcoin.org* 2017) <https://Bitcoin.org/en/developer-examples#testing-applications> Accessed 24 July 2017.

In this way, programming language is used to give instructions and set parameters for the Bitcoin Core software on all aspects of the Bitcoin system. The open source nature of the Bitcoin software means that anyone can download and modify it through programming. These modifications range from suggested improvements to Bitcoin Core itself, to the development of a completely new cryptocurrency with different features to Bitcoin, which are known as 'altcoins'. The first of these altcoins was Litecoin, developed by Google programmer Charles Lee in 2011 by using a different algorithm to Bitcoin, aimed at increasing the speed of transactions.[21] Another prolific altcoin is Ethereum, which was launched 2015 to move beyond Bitcoin by being more than just a payment system. Instead, Ethereum is 'a decentralised platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference'.[22] By deploying multiple different programming languages to Bitcoin, Ethereum allows for coding flexibility over the blockchain for more fully integrated and flexible applications beyond just peer-to-peer payments.

Other altcoins based on more subtle modifications and deviations from Bitcoin include Zcash and Dash. Launched in 2016, Zcash is based on a modification of the Bitcoin core code, to offer users the choice of 'shielded' transactions which use the more advanced cryptographic technique of zero-knowledge proof construction in order to mask details such as sender, recipient and amount, leaving only a record of transactions on the blockchain.[23] This differs from Bitcoin, which shows all these, albeit with public keys in lieu of sender and receiver names. Similarly, the cryptocurrency Dash, launched initially in 2014,

[21] Litecoin (*Litecoin.com* 2017) <https://litecoin.com/> Accessed 17 July 2017.
[22] Ethereum Foundation, 'Ethereum Homestead Release' (*Ethereum.org* 2016) <https://www.ethereum.org/> Accessed 25 July 2017.
[23] Zcash, 'What is Zcash?' (*Z.cash* 2016) <https://z.cash/> Accessed 25 July 2017.

uses features such as Darksend and InstantX to provide more anonymity than Bitcoin, making transactions near untraceable as was described in Chapter 1.[24]

Overall, there are over one thousand trading cryptocurrencies or altcoins, and growing.[25] Each of them were made possible by the open source nature of the original Bitcoin Core program and code, which allowed for modification and further development. The distinguishing features of each cryptocurrency is based on changes made to the rules embedded in the code. In this way, the operational closure of the cryptocurrency system is defined by the parameters set by computer code, as it is the code that determines what is possible and permissible and what is not. In sum, code governs and regulates the cryptocurrency system at its most fundamental level, both existentially and operationally.

5.2.3 Code Cognitive Openness (Regulability)

Having established the role of code in governing the cryptocurrency system and described its operational closure, the key question to be considered is whether or not, and to what extent computer code can be influenced by other systems—in this case, the legal system. Key to addressing this question is considering the possibility for the code (internal 'law') of the cryptocurrency system to incorporate the regulatory variables of the legal system (external law) in order to facilitate financial regulation.

The most obvious starting point in considering the intersection between the legal and the cryptocurrency systems is that of smart contracts, originally conceived by Nick Szabo.[26] The scripting language of Ethereum allows for the embedding of smart contract code within cryptocurrency transactions. Smart contracts use computer programming to automatically execute the terms of a contract by using 'if-then' statements that lead to the execution of a corresponding contractual

[24] Dash, 'Dash is Digital Cash' (*Dash.org* 2015) <https://www.dash.org/> Accessed 25 July 2017.
[25] Data from <https://coinmarketcap.com/all/views/all/> Accessed 25 July 2017.
[26] N Szabo, 'Smart Contracts' (*Unpublished Manuscript* 1994).

clause when a pre-programmed condition is triggered. Examples of smart contracts are 'send x amount of Bitcoins from person A to person B on 17 May 2018' or, more complexly, 'send x amount of Bitcoins to person C if their location, verified by GPS coordinates x, is reached and increase the amount by x amount per hourly rate' or an example given by Jamali et al, 'if person A passes away, verified by external data, transfer x Bitcoins to person B, and change the appropriate land title from person A to person B'.[27] This ability to write smart contracts into transactions is potentially particularly useful for regulatory compliance purposes in financial services.

More generally, there are several examples where computer code has been used for regulatory purposes. These innovations have led to a burgeoning industry centred on legal programming and regulation technology, or 'regtech', and supervisory technology, or 'suptech'. Legal programming involves the incorporation of legal criteria in software design, in order to—as proposed by Bain and Subirana in the case of e-commerce—'model legal constraints and dependencies within process models so that the relations and transactions between agents are compliant on all levels'.[28] Similarly, and more generally, regtech can be defined as 'any technological innovation that helps efficiency and transparency in regulation'[29] or alternatively defined as referring to 'a set of companies and solutions that address regulatory challenges across industries, including financial services, through innovative technology'.[30] Regtech is being used by financial institutions to lower compliance costs by harnessing financial technology, (fintech) in areas such as risk control and management, KYC identity verification compliance, AML regulatory reporting, and data management tools.

[27] R Jamali, and others, 'Cryptocurrency, Digital Asset Class of the Future—Bitcoin vs Ethereum' (*The Economist* 2016) <http://www.economist.com/sites/default/files/economist_case_comp_ivey.pdf> Accessed 6 June 2017.

[28] M Bain and B Subirana, 'E-commerce Oriented Software Agents' (2004) 20 CLSR 1, 201.

[29] Deloitte, 'RegTech is the New FinTech' (*Deloitte* 2016) <https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/FinancialServices/IE_2016_FS_RegTech_is_the_new_FinTech.pdf> Accessed 6 June 2017.

[30] M Cavallo, 'How RegTech Closes the Gap Between Technology and Financial Services' (*CIO* 2017) <http://www.cio.com/article/3190162/it-industry/how-regtech-closes-the-gap-between-technology-and-financial-services.html> Accessed 6 June 2017.

In this way, regtech allows firms to automate some of their more basic compliance tasks, and by so doing, makes it easier for them to use these elevated compliance functions to manage risk.

More advanced applications such as big data and machine learning platforms 'allow for large data sets to be analysed to reveal patterns, trends and association', and this can 'enable banks to monitor transactions in real time and improve the identification of unusual activity'.[31] Management consultancy firm Deloitte surmised that regtech provides companies with process and data agility, increased reporting speed, system integration, advanced analytic tools, and cloud-based solutions.[32] It has also been suggested that banks can save as much as £2.7billion per year by using regtech solutions, instead of antiquated anti-money laundering systems, whilst simultaneously 'reducing the ability of criminals to exploit financial networks for money laundering and terrorist financing around the globe'.[33] This technology is particularly pertinent to cryptocurrency markets, where the pseudonymous and distributed nature of transactions adds a high degree of complexity, such that only machine learning and other regtech tools can monitor and flag suspicious activity and out-of-the-norm behaviour 'that may not be caught by knowledge-based rules of human review'.[34] In this way, regtech can be seen as a code-based solution to the regulation of a code-based regulatory target like cryptocurrency.

This capability has been further enhanced by the development of regtech and legal programming solutions based on cryptocurrencies' own technology and software. An example of this is the blockchain-based solution to malware provided by Charles Noyes who developed BitAv.[35] This system allows for the decentralisation of software updates and maintenance mechanisms using a peer-to-peer network, instead of a central host, as is traditionally the case. Noyes'

[31] Deloitte (n 29).
[32] ibid.
[33] M Cavallo (n 30).
[34] ibid.
[35] C Noyes, 'BitAv: Fast Anti-Malware by Distributed Blockchain Consensus and Feedforward Scanning' (*Arxiv.org* 2016) <https://arxiv.org/pdf/1601.01405.pdf> Accessed 6 June 2017.

study showed how 'the peer to peer network maintenance mechanism lowered the average update propagation speed by 500 per cent and is far less susceptible to targeted denial-of-service attacks'.[36] This innovation is a reflexive solution to the regulatory challenges of malware attacks (usually demanding payment in Bitcoin),[37] and to the more recent denial-of-service attacks targeted at cryptocurrency exchanges.[38] In this way, it uses the cryptocurrency system's own internal logic and tools of code over a blockchain or distributed ledger, in order to address the shortcomings within the system itself. This example also demonstrates not only the possibility, but also the superior efficacy of using computer code and programming for regulatory purposes.

The BitAv initiative is in line with the existing application of the underlying DLT of cryptocurrencies to better achieve KYC and AML compliance. An example of this is the proof-of-concept launched by R3, a consortium of fifty of the world's top financial institutions, aimed at the formation of a KYC registry developed to 'catch identity theft, avoid fraud, prevent money laundering, and stop terrorist financing',[39] circumventing traditional mechanisms such as designated money-laundering officers, whilst acknowledging the fact that 'the transparency, and immutability of storing identification information in the blockchain seems like a logical choice for fighting illicit activities in the financial sector'.[40]

Additionally, as explained by Matonis, cryptographic proof of reserves can deliver responsible public audits of exchange assets, as Bitcoin's public ledger allows an organisation to prove control of Bitcoin assets, without revealing

[36] ibid 1.
[37] S Smith, and others, 'Huge Cyberattack Hits Nearly 100 Countries with 'Wanna Decryptor' Malware' (*NBC News* 13 May 2017) <http://www.nbcnews.com/news/world/national-health-service-cyberattack-hits-english-hospitals-hackers-demand-Bitcoin-n758516> Accessed 6 June 2017.
[38] The Merkle provides a list of denial-of-service attacks targeted at cryptocurrency exchanges at <https://themerkle.com/top-5-cryptocurrency-exchanges-hit-by-ddos-attacks/> Accessed 6 June 2017.
[39] J Manning, 'R3 Uses Blockchain to Streamline KYC for Banks Around the World' *RiskScreen* *<https://www.riskscreen.com/kyc360/news/24653/>* Accessed 21 February 2020.
[40] ibid. For further details about R3, see <http://www.r3cev.com/> Accessed 21 February 2020.

private information about customers or account holders.[41] These and other developing innovations will be able to make oversight of cryptocurrency activity easier. As previously alluded to in describing the work of Ortolani, consumers also have the ability to monitor and oversee their own assets using developments such as multisignature (multisig) wallets that allow for the introduction of additional parties to a transaction, authorised to act as a security and dispute resolution backstop.[42] In this way, from smart contracts to legal programming and regtech, the cognitive openness of cryptocurrency code, as displayed by regulability, is highly evident.

Further indicating cognitive openness is the observation that there is a clear and distinct role for the legal system to play in ameliorating and improving the functioning of code as a self-regulatory mechanism in the cryptocurrency system. This is primarily because 'as opposed to the law, computer code lacks the necessary flexibility to cover unforeseen situations that might emerge in a complex society'.[43] This is particularly true of smart contracts, where it has been noted that these cannot operate fully autonomously, and that a smart contract cannot 'actively scan its environment and execute in response to changes accordingly'.[44] Instead, smart contracts are reactive, and cannot, for example, 'proactively quer[y] an external database and change its own state based on the outcome of the query'.[45] As such, there is scope for legal intervention in both the design and execution of smart contracts, as well as in the overall monitoring and modification of these algorithms. This fact came to the fore when Ethereum experienced a hack in 2016[46] that led to the observation that 'social organisations

[41] J Matonis, 'Why the OECD Needs to Do its Homework on Cryptocurrencies' (*Coindesk* 1 July 2014) <https://www.coindesk.com/oecd-needs-homework-Bitcoin/> Accessed 3 July 2018.

[42] ibid.

[43] P De Filippi, 'A $50M Hack Tests the Values of Communities Run by Code' (*Motherboard* 2016) <https://motherboard.vice.com/en_us/article/thedao> Accessed 15 May 2017.

[44] O Rikken, '3 Smart Contract Misconceptions' (*CoinDesk* 2017) <https://www.coindesk.com/3-common-smart-contract-misconceptions-explored/> Accessed 6 June 2017.

[45] ibid.

[46] I Allison, 'Ethereum Reinvents Companies With Launch of the DAO' (*International Business Times* 2016) <http://www.ibtimes.co.uk/ethereum-reinvents-companies-launch-dao-1557576> Accessed 15 May 2017.

cannot be ruled only and exclusively by code', and furthermore, that the need for a drastic reconfiguration of the Ethereum code in order to reverse transactions leading to the hack displayed 'a tension between the 'intention of the code' and the 'wording of the code'.[47]

Cryptocurrency was designed to be a 'trustless' system, but, as was noted by De Fillipi, this claim is only valid 'provided that the underlying technology can be trusted'[48]—meaning that the cryptocurrency system needs to look beyond its internal code-based governance structure, and consider legal direction from conception to implementation of the code.

This need for legal direction is further illustrated by the potential of code-based governance to clash with fundamental legally enshrined principles, such as privacy. Since a large number of the above-mentioned regtech solutions currently in the market are concerned with knowing who people are for AML and KYC purposes, this raises privacy concerns, as regtech and code would amplify the ability to reveal facts about individuals through certification. This is a legitimate legal issue, which takes on an extra level of significance, since as the certification architecture depends on who chooses the code, the choice depends upon what incentives they face, where 'if 'protecting privacy' is not an incentive then the code will not provide it and your privacy will not be protected'[49]. This means there is a danger in leaving exclusive control of regtech and other code-based governance development solely in the hands of the private sector, without a certain level of legal and regulatory oversight, as industry is driven by incentives that may not necessarily align with the public good.

Of note here is how, as described in the theory of autopoiesis, this system-to-system influence between code and law is bi-directional. The legal system has been engaging with the information technology system in which cryptocurrency

[47] De Filippi (n 43).
[48] ibid.
[49] Lessig (n 6) 103.

partly operates, and computer code or software, at an incremental rate. Recent developments include the international law firm Clifford Chance, announcing an extended relationship with Microsystems, an information technology firm that provides 'document authoring, editing, formatting, proofreading, and metadata scrubbing software serving the legal and life sciences industries', to implement and provide Contract Companion—proof-reading software designed to leverage 'Artificial Document Intelligence (ADI) to achieve unparalleled analysis speed, greater accuracy, and improved workflow'.[50] These, and other similar intersections, would be unsurprising to researchers highlighting the similarities in rules-driven writing seen in legal writing and computer programming, and those involved in Legal Rule Mark-up Language projects.[51]

A final indicator of cognitive openness is a display of willingness to comply with legal regulation.[52] The cryptocurrency system has displayed this, initially through intermediaries such as Coinbase and Gemini, pre-empting and then later surpassing licensing requirements motivated in part (particularly in the case of Gemini) by the need to attract institutional investors.[53] More recently, a new number of cryptocurrency market players, including Coinfirm.io, Elliptic and Chainanalysis have risen to compliance challenges, and provided a range of solutions (from blacklisting cryptocurrency addresses with potential involvement in money laundering, ransomware, and trafficking to providing technology aimed at identifying and tracking suspicious transactions).[54] In this way, the cognitive openness to the legal system of code-based governance structures within the cryptocurrency system is characterised by (a) being

[50] PRWeb, 'Clifford Chance Enhances Document Review With AI in Microsystems Contract Companion' (*PRWeb* 2017) <http://www.prweb.com/releases/2017/06/prweb14395641.htm> Accessed 15 June 2017.

[51] K Koch, 'A Multidisciplinary Comparison of Rules-Driven Writing: Similarities in Legal Writing, Biology Research Articles, and Computer Programming' (2005) 55 J Legal Educ 234.

[52] Consider also the instances where cryptocurrency exchanges have been calling for regulation in jurisdictions with 'no regulation', as highlighted in Chapter 2.

[53] D Roberts, 'With Gemini, Winklevoss Brothers Seek Respect in Bitcoin' (*Fortune* 2015) <http://fortune.com/2015/10/05/gemini-winklevoss-Bitcoin/> Accessed 25 July 2016.

[54] N Ayton, 'Bitcoin Community Cracking Down on Money Laundering and Fraud' (*Innovation Enterprises.com* 2016) <https://channels.theinnovationenterprise.com/articles/Bitcoin-community-cracking-down-on-money-laundering-and-fraud> Accessed 25 July 2016.

technically feasible, (b) having areas with a clear role for the law and for intervention by the legal system, and (c) displaying amenability to intervention by the legal system.

5.2.4 Code - Conclusion

Thus far, this chapter has shown how computer code is the key governance mechanism of the cryptocurrency system, as it both generates cryptocurrency and defines the parameters of its operation. The chapter has also shown how, as has been noted by Wu, 'code can be used to produce regulatory effects similar to laws'[55] and Lessig, 'there is regulation of behaviour on the Internet and in cyberspace, but that regulation is imposed primarily through code'.[56] A key consideration raised here is that if regulability depends on code, then 'some architectures are more regulable than others'.[57] This has been evident in the description of how changes and modifications in code create specific features and characteristics unique to each cryptocurrency, and as its 'architecture will affect whether behaviour can be controlled'.[58] It therefore follows that if regulability is determined by code, architectures can be coded for regulability.

The plethora of different cryptocurrencies or altcoins, each with a different coding structure, means that each has a different level regulability, and that this regulability is possible through code itself. As a regulatory tool, computer code provides ease of enforcement, because 'if its rules are broken then an error is returned and no activity occurs, so compliance is ensured through the operation of the code itself'.[59] However, this also means that there is absolute rigidity of compliance by code. As has been noted above, with code, once run, there is no room for interpretation, for the taking into account of unique or special circumstances, or for the application of the spirit of the intended regulation.

[55] T Wu, 'When Code Isn't Law' (2003) 89 Va L Rev 679, 681-82.
[56] Lessig (n 6) 24.
[57] ibid 24.
[58] ibid 24.
[59] Lehdonvirta and Ali (n 11) 41.

Further challenges to regulation by code can be noted. On considering regulation by software, Grimmelmann revisits the most basic principle in Lessig's *Code* by directing emphasis on how software has its own unique modality of regulation, characterised by being automated, immediate and plastic. More significantly, he provides some insight into recurring patterns where regulation by software is used. These are that software acts according to rules rather than standards, that software can regulate without transparency, that software rules cannot be ignored, and finally, that software is vulnerable to sudden failure, particularly through hacking.[60] Similarly, Ohm and Reid highlight further challenging areas in the regulation of software, particularly the inevitable conflict in policy goals such as privacy versus transparency, and freedom versus control.[61] These observations call for a critical consideration of the appropriateness of regulation by software or regulation by code on a case-by-case basis.

Furthermore, the notion that 'code is law', as initially articulated by Lessig, has been challenged by several scholars including Wu, who cites critical areas of non-compliance such as copyright. This leads to the questioning of 'notions that technological self-help can offer a substitute for legal systems'.[62] Here it has been argued that, whilst computer code can be seen as a regulatory mechanism, as described above, it can also work as 'an anti-regulatory mechanism: a tool to minimise the costs of law that certain groups will use to their advantage'.[63] Citing the example of peer-to-peer (P2P) file sharing, Wu illustrates how code design is used to 'undermine an existing legal system (copyright)'.[64]

Relating this argument to the computer code that governs cryptocurrencies, it can be argued that cryptocurrency was programmed, at the most extreme, to undermine—but more moderately viewed, to circumvent existing legal system governing financial markets. By introducing disintermediation and

[60] J Grimmelmann, 'Regulation by Software' (2004) 114 Yale L J 1719.
[61] P Ohm and B Reid, 'Regulating Software When Everything Has Software' (2006) 84 Geo Wash L Rev 1672.
[62] Wu (n 55) 682.
[63] ibid 682.
[64] ibid 683.

pseudonymity, cryptocurrency code facilitated and made easier the perpetration of tax evasion, money laundering, terrorist financing, ransomware, and the purchase of illegal goods and services on the dark web. However, as has been shown above, the cryptocurrency system displays a multi-level cognitive openness in the feasibility of the use of code to achieve regulatory ends, the evident areas where legal intervention is necessary, and significant and legitimate system participants' signalled willingness to comply.

A reflexive approach to the use of code in the regulation of cryptocurrency therefore places emphasis on the notion of law through code, and calls for regulatory intervention aimed at re-directing this internal self-governance tool (code) to work not against, but for the law, through the incorporation of compliance and regulation targeted code into existing transaction code. This is divergent to the approach proposed by Wagner, who presents the notion of 'software code as complimentary to law rather than its substitute', and the idea of 'code meets law' rather than 'code is law', based on the concern that 'the nature of cyberspace [is] particularly sensitive to emerging concerns about the tyranny of software'.[65] Providing a more co-regulatory solution to software regulation, Wagner's approach does not allow for the mutual bi-directional learning of a more reflexive approach necessary for the effective regulation of a new technology such as cryptocurrency. Moreover, it fails to appreciate the fact that system integrity or operational closure is still maintained in a reflexive approach, and that the regulatory trilemma challenge of lack of coherence is avoided through the process of separate but unidirectional co-evolution between the legal and code-based cryptocurrency systems.

Therefore, for the reflexive regulation of cryptocurrency, the notion to be espoused in the debate on the correct relation between code and the law is neither 'code meets law', nor the more universal 'code is law'—but 'law through code'. An understanding of law through code maintains the operational closure

[65] P Wagner, 'On Software Regulation' (2004) 78 S Cal L Rev 457, 458.

of the legal and the cryptocurrency systems respectively, whilst accounting for the cognitive openness that allows the legal system to influence the cryptocurrency system and vice versa.

5.3 Consensus

5.3.1 Introduction

The manner in which computer code acts as a self-governance mechanism for the cryptocurrency system has been shown through the operational closure of code as described above. In addition to code, consensus—based on the notion of distributed governance—is a complementary self-regulatory tool within the cryptocurrency system. As the word implies, consensus is about agreement, and the process through which multiple parties arrive at the same conclusion and agree upon the same outcome. More specific to the cryptocurrency system, consensus is the mechanism through which decisions are made on a distributed network involving multiple participants. At its most fundamental level, consensus in the cryptocurrency system manifests itself firstly by how cryptocurrency requires agreement about rules (criteria to determine which transactions are valid), consensus about state (agreement on the history and ownership of transactions), and consensus that cryptocurrencies are valuable (demonstrated by players being willing to accept them in payment).[66]

More specific to governance, consensus forms part of cryptocurrency's internal self-regulatory mechanism in two ways. Firstly, the technicalities of distributed ledger technology and blockchain technology call for the use of 'consensus algorithms' that allow for various nodes or computer systems that have downloaded the cryptocurrency software to firstly verify transactions and confirm and accept the legitimacy of each transaction, and secondly, secure the

[66] J Kroll, 'The Economics of Bitcoin Mining, or, Bitcoin in the Presence of Adversaries' (*Econinfosec* 2013).<http://www.econinfosec.org/archive/weis2013/papers/KrollDaveyFeltenWEIS2013.pdf> Accessed 20 May 2017.

network from attack. In this instance, the original Bitcoin Core software uses a 'proof-of-work' algorithm in order to verify transactions, but, as shall be further described below, other cryptocurrencies and altcoins use alternative consensus algorithms resulting in different implications for their regulation.

The second, related, aspect of consensus as a governance model for cryptocurrencies has to do with the manner in which decisions are arrived at regarding changes to the cryptocurrency code. Similar to consensus algorithms, this aspect of consensus concerns the assigning of rights and responsibilities to various actors in the cryptocurrency system. The initial code and rules that define the generation and functioning of cryptocurrency was written by software developers and, as such, can be changed or modified by software developers. This means that there is an additional layer of governance and regulatory intervention through the oversight of human rule-making, at the point of decisions about code creation and code modification.

Bitcoin's source code was programmed and provided open source by Satoshi Nakamoto, who passed on coding control to the Bitcoin 'core development' team led by Gavin Andresen.[67] This team does not, however, act autonomously. Instead, it operates based on a form of distributed governance, where 'the core developer's power is constrained by an informal self-imposed charter, which states that significant changes to the rules require broad consensus from the community'.[68] This consensus-based governance structure has additional decentralisation assurance, by providing an influential role for miners—who essentially ratify an update by it only being effective and operational once it is installed by the majority of miners. Likewise, cryptocurrency intermediaries, users, investors and merchants have a choice in which version of the software to install and run on their systems. In this way, 'cryptocurrency is built on the premises that a decentralised governance model, controlled by the community and all stakeholders, can manage money more efficiently than a centralised

[67] Lehdonvirta and Ali (n 11).
[68] ibid 51.

organisation'.[69] What follows is an examination of the operational closure (functionality) and cognitive openness (regulability) of consensus as a self-regulatory and self-governance mechanism within the cryptocurrency system, and a discussion on the implications of these findings for cryptocurrency regulation.

5.3.2 Consensus Operational Closure (Functionality)

The first form of consensus in the cryptocurrency system has to do with how the code assigns, by algorithms and programming, decision-making roles on mainly transaction verification and network security to the various participants in the cryptocurrency system. Here, the consensus model used by Bitcoin, proof-of-work, 'ensures that the next block in a blockchain is the one and only version of the truth, and it keeps powerful adversaries from derailing the system'.[70] The Bitcoin proof-of-work algorithm relies on miners to verify transactions where the miner that solves the given complex mathematical code associated with a transaction first, verifies it, and receives a fee allowing for the network as a whole to confirm the legitimacy of a transaction, which then goes through and is sealed onto the blockchain, allowing for the next transaction to be verified above it.[71]

Different cryptocurrencies implement varying degrees of this consensus model, and by so doing, (re)allocate the balance of power, primarily between developers and miners, in a configuration that suits their purposes. As has been previously described, the first altcoin or new form of cryptocurrency to fork, or break away from the initial Bitcoin source code was Litecoin, which uses the same mining and proof-of-work as Bitcoin, but with a different algorithm that allows for faster transaction verification.[72] Subsequent altcoins have developed different consensus models to Bitcoin's proof-of-work model in their governance. These

[69] R Jamali (n 27) 12.
[70] A Castor, 'A (Short) Guide to Blockchain Consensus Protocols' (*CoinDesk* 4 March 2017) <https://www.coindesk.com/short-guide-blockchain-consensus-protocols> Accessed 6 June 2017.
[71] Nakamoto (n 13).
[72] Litecoin (n21).

include proof-of-stake (eg, Peercoin), proof-of-importance (eg, NEM), proof-of-burn (eg, Slimcoin), proof-of-disk-capacity (eg, Burst), and proof-of-time-connected (eg, Timecoin).[73] In the proof-of-stake consensus algorithm, validation of blocks is not conducted by miners as it is in Bitcoin's proof-of-work model—the right to create the next block is awarded based on the percentage of coins in the system owned. Similarly deviating from the Bitcoin proof-of-work consensus algorithm, are proof-of-capacity, where hard drive space determines the probability of block verification, and proof-of-time, where a trusted execution environment (TEE) is used to randomly select blocks for production without the required work in Bitcoin.[74]

However, different these consensus models are, they are all rooted in the notions of decentralised governance, where 'consensus about the rules is a social process' and 'participants come to a common understanding of what is allowed, so that the rules can be encoded into the software that each participant uses'.[75] With these consensus algorithms, while a significant amount of power and influence lies with the software developers, decentralisation is intrinsic to their development as open source projects. This means that developers' influence is curbed by the ability of anyone to fork (separately copy and change) the current version of the software, with the key factor determining distributed or decentralised governance being that 'a fork will survive [only] if it has enough support from the community', ensuring that governance of the software is mostly 'consistent with the desires of the community'.[76] This dynamic is best illustrated by comparing how consensus operates in Bitcoin and Ethereum respectively, and by presenting the newer, alternative proposals of Tezos, Decred and Cosmos.

[73] D5000, 'A Cryptocurrency with Many Consensus Methods to Avoid Centralisation' (*Bitcoin Forum* 1 May 2016) <https://Bitcointalk.org/index.php?topic=1456484.0> Accessed 17 July 2017.

[74] Castor (n 70).

[75] Kroll (n 66) 7.

[76] ibid 17.

5.3.2.1 Bitcoin

Bitcoin applies a distributed governance model, where all stakeholders have to agree in order for change to be implemented. This means that no one has unilateral control over the currency. Although the core development team of volunteer programmers play a key role in maintaining the code and making updates when needed, anyone else can propose changes to the protocol, which are voted for and vetted by the community as whole, and only implemented by the development team when consensus about the proposed changed is reached. Proposals for the improvement of Bitcoin are known as Bitcoin Improvement Proposals, or BIPs.[77]

The 199 BIPs that have been submitted since the first one on 2011 can be divided into three types, namely Standards Track proposals (which introduce changes to the Bitcoin network protocol, blocks or transaction validation), information BIPs (which recommend changes in design issues rather than propose new features), and Process BIPS (which propose process changes outside of the Bitcoin protocol itself).[78] As has been previously mentioned, although there is a crucial role of the Bitcoin development team in the vetting and implementation of proposals, BIPs require the mutual consent and consensus of the Bitcoin community in order to become active. The functionality of this consensus process amongst the Bitcoin community was tested by the BIPs in terms of the implementation of forks (changes) in the Bitcoin protocol. In this instance, the increased use and adoption of Bitcoin led to a slowing down of the network, due to continually increasing transaction volumes, which then resulted in delays in the processing and confirmation of transactions.

In addition to the disadvantage of inconvenience that potentially jeopardises e-commerce uses of Bitcoin, exchanges were charging more to clear Bitcoin

[77] J Buntix, 'What is a BIP?' (*The Merkle* 2017) <https://themerkle-com.cdn.ampproject.org/c/s/themerkle.com/what-is-a-bip/amp/> Accessed 6 June 2016.
[78] ibid.

transactions. With a median transaction confirmation time of 11 minutes[79] at the time of writing, there is agreement about the need for a change in the protocol, but in 2017 there an on-going debate, described as the Bitcoin 'civil war'[80] between those suggesting a hard fork (dramatic change in the code) and those advocating a soft fork (slight change in the code). The hard fork proposal, Blockchain Unlimited, would allow for an increase in block size, or number of transactions per tranche, as and when needed. Whilst this would increase capacity with no upper limit, it would entail splitting the original Bitcoin Core blockchain into two. Apprehension over the drastic nature of this change led to a soft fork or minor modification proposal, using Segregated Witness (Segwit) programming in order double the transactions per second, by increasing bandwidth. Detractors of this proposal argued that it would only be a temporary solution, as transaction volumes are likely to continue increasing, and that an increase in block size is inevitable.[81]

Of particular interest is how Bitcoin Unlimited developers stated that they would move ahead with implementation of changes when it reached an adoption rate of more than 51 per cent, whereas Segwit set an ambitious adoption-trigger threshold of 95 per cent of the network.[82] Both targets were set arbitrarily with no clearly stated rationale. The decision on which change to the Bitcoin protocol would be adopted was tracked by the number of computers of nodes that download the software for each option, as seen in Figure below, still using the existing protocol, but signaling their support for either option ready to start running it once activated.

[79] Median Confirmation Time as on 16/06/17 from Blockchain.Info chart <https://blockchain.info/charts/median-confirmation-time> Accessed 16 June 2017.

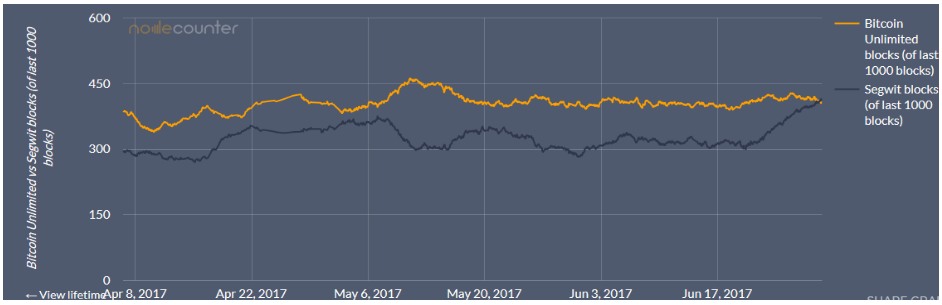
[80] O Williams-Grut and R Price, 'A Bitcoin Civil War is Threating to Tear the Digital Currency in 2' (*Business Insider* 2017) <http://uk.businessinsider.com/Bitcoins-hard-fork-Bitcoin-unlimited-segregated-witness-explained-2017-3> Accessed 16 June 2017.

[81] ibid.

[82] A Quentson, 'Price Shoots Up as Bitcoin Unlimited Surpasses Segwit' (*CryptocoinNews* 2017) <https://www.cryptocoinsnews.com/price-shoots-Bitcoin-unlimited-surpasses-segwit/> Accessed 6 June 2017.

The debate in 2017 culminated in Bitcoin being forked (or split into two), creating Bitcoin Cash (BCH). Bitcoin Cash subsequently also split into two in 2018, creating Bitcoin Cash and Bitcoin SV.[83] Whilst there are varying opinions about the effects and implications of the development of Bitcoin Cash, what is pertinent to this analysis is the observation that the cryptocurrency system has an internal consensus-driven process, through which decisions regarding the evolution of cryptocurrency are made through 'voting by download'.

Figure 7: Bitcoin Unlimited vs Segwit Support



Source: Node Counter[84]

5.3.2.2 Ethereum

Presenting a distinctly different consensus model to Bitcoin, Ethereum has a more recognisable corporate structure, where the development team has taken a more structured approach to solve critical issues, such as the hard fork following the 2016 hack of its Distributed Autonomous Organisation (DAO). This has left two chains of Ethereum currently in operation, and it is left to the community to decide which version or chain to follow. In this way, Ethereum operates based on what has been described as 'central control with democratic processes.[85] Of regulatory significance here is that, unlike Bitcoin, where the creator and founder, Satoshi Nakamoto, is unknown, Ethereum has an

[83] Cointelegraph, 'Difference between Bitcoin and Bitcoin Cash' (*Cointelegraph* 2020) <https://cointelegraph.com/Bitcoin-cash-for-beginners/btc-bch-differences> Accessed 27 January 2020.
[84] Data from Node Counter <http://nodecounter.com/#Bitcoin_classic_blocks> Accessed 27 January 2020.
[85] Jamali (n 27).

established leadership structure, and the ability to be more responsive and agile to prompts for change than Bitcoin.

Ethereum additionally incorporates the use of smart contracts. In this case, these are used in order to facilitate transactions within a virtual Distributed Autonomous Organisation (DAO). The DAO works as a decentralised blockchain company where individuals that have 'bought in' to the organisation through the purchase of ether (ETH), initially through a crowd-funding initiative, 'stay in control of its funds, vote on its future and get rewarded when it succeeds'.[86] The DAO community decides on which submitted proposals to collectively invest in, based on votes (which are in turn proportional to the amount of ether tokens held). Once a proposed project, submitted by a 'contractor', is approved, the DAO community cedes day-to-day operational control of the project to the contractor, whilst receiving pre-determined scheduled payments, enforced through smart contract coding, where DAO token holders keep control over their ETH holdings at all times. In this way, as stated in its manifesto, the DAO seeks to 'blaze a new path in business organisation for the betterment of its members, existing simultaneously nowhere and everywhere and operating solely with the steadfast iron will of immutable code'.[87] The DAO aims to invest in proposals that not only provide returns on investment to the venture fund, but also promote the 'sharing community' and distributed economy.[88]

The DAO's 2006 hack led to a hard fork, which resulted in the existence of two separate strands of Ethereum. This allowed for a reversal of the transactions after a hacker had taken advantage of a loophole in the DAO smart contract code. The fork was proposed in order to allow for miners to switch to a more secure code, and for investors to safely withdraw their funds.[89] Significantly, this decision was arrived at democratically, where the developers within and outside the Ethereum

[86] Allison (n 46).

[87] ibid.

[88] ibid.

[89] K Breitman, 'Op Ed: Why Ethereum's Hard Fork will cause problems in the coming year' (*BitcoinMagazine* 2017) <https://Bitcoinmagazine.com/articles/op-ed-why-ethereums-hard-fork-will-cause-problems-coming-year/> Accessed 15 May 2017.

foundation wrote the software necessary to activate the fork, but remained 'neutral stewards' in order to allow the fork to be a 'community decision'.[90] This community decision was arrived in a faster, more convenient and more organised manner than occurred within Bitcoin, largely due to the fact that there is a higher degree of structured governance within Ethereum, as a result of a clearer defined chain of command and a more accountable and visible leadership team. In this way, Ethereum's governance mechanism—although similar to that of Bitcoin and other cryptocurrencies in its use of distributive governance—circumvents some of the challenges inherent in Bitcoin's structure, by virtue of possessing more formal governance structures with a known and active founder and leader.

5.3.2.3 Tezos, Decred and Cosmos

Recognising the likely governance conundrum that comes with the inevitable updates and changes to open source cryptocurrency projects, a new generation of cryptocurrencies with in-built governance structures have emerged. The first of these is Tezos, which opened up a funding round in July 2017. Incorporating the smart contract capabilities of Ethereum, Tezos takes this concept one step further, by letting participants directly control the rules of the network. It does this by 'creating governance rules for stakeholders to approve of protocol upgrades that are then automatically deployed on the network'.[91] In this way, Tezos describes itself as enforcing 'new types of constitutionalism', where its tokens not only fuel smart contracts but also allow votes on protocol amendments. This is done through attaching an invoice to every proposed change, which creates not just financial incentive for contributing to development, but also allows for participants to coordinate on-chain and arrive at collective decision-making by voting with their tokens. Similarly, Decred, founded in 2015, offers a 'layered governance organisation that extends beyond

[90] I Allison, 'Ethereum's Vitalik Buterin' (*IBTimes* 2016) <http://www.ibtimes.co.uk/ethereums-vitalik-buterin-democratic-hard-fork-proves-mining-oligopoly-cannot-engage-censorship-1569079> Accessed 15 May 2017.

[91] Tezos, 'Governance' (*Tezos* 2017) <https://www.tezos.com/governance> Accessed 15 July 2017.

the miners and users to bring forward and represent insider and outsider voices in the community'.[92] This is achieved by combining the proof-of-work used in Bitcoin with proof-of-stake, in which Decred funds are used to purchase voting networks on the network and, by so doing, allow users to vote on suggested network changes.[93]

A final notable solution to cryptocurrency governance mechanisms is presented by Cosmos. This proposal is a direct response to the governance issues of Bitcoin, Ethereum and other cryptocurrencies, through the development of a blockchain network architecture that allows for multiple parallel blockchains to interoperate using Cosmos Hub, 'a multi-asset proof-of-stake cryptocurrency with a simple governance mechanism which enables the network to adapt and upgrade'.[94] Cosmos' white paper details the functioning of a constitution and a governance system in which validators and delegators 'can vote on proposals that can change preset parameters of the system automatically, coordinate upgrades, as well as vote on amendments to the human-readable constitution that govern the policies of the Cosmos Hub'.[95] According to Cosmos, this constitution 'allows for cohesion among the stakeholders on issues such as theft and bugs, allowing for quicker and cleaner resolution'.[96] In this way, Tezos, Decred and Cosmos are at the vanguard of a new generation of cryptocurrencies incorporating internal consensus-based distributed governance structures, aimed at resolving the governance issues evident in established cryptocurrencies and paving the way for greater regulability of cryptocurrencies.

[92] Decred, 'About' (*Decred* 2017) <https://www.decred.org/> Accessed 15 July 2017.

[93] Bitcoin Exchange Guide, 'Decred—Cryptocurrency Governance Consensus System & Wallet?' (*BitcoinExchangeGuide* 2017) <https://Bitcoinexchangeguide.com/decred/> Accessed 15 July 2017.

[94] J Kwon and E Buchman, 'Cosmos: A Network of Distributed Ledgers' (*Github* 2017) <https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md#governance> Accessed 14 August 2017.

[95] ibid.

[96] ibid.

5.3.3 Consensus Cognitive Openness (Regulability)

The first component in assessing cognitive openness and regulability is considering whether or not it is feasible and possible for this consensus-based governance model to be influenced by the legal system. It has been argued that the practice of consensus-based governance establishes, prima facie, regulability. As noted by Kroll, 'contrary to claims that Bitcoin is ungovernable and relies on fixed rules laid down at its founding, the rules can be and have been changed by consensus' means that 'Bitcoin is more amenable to government regulation than advocates claim'.[97]

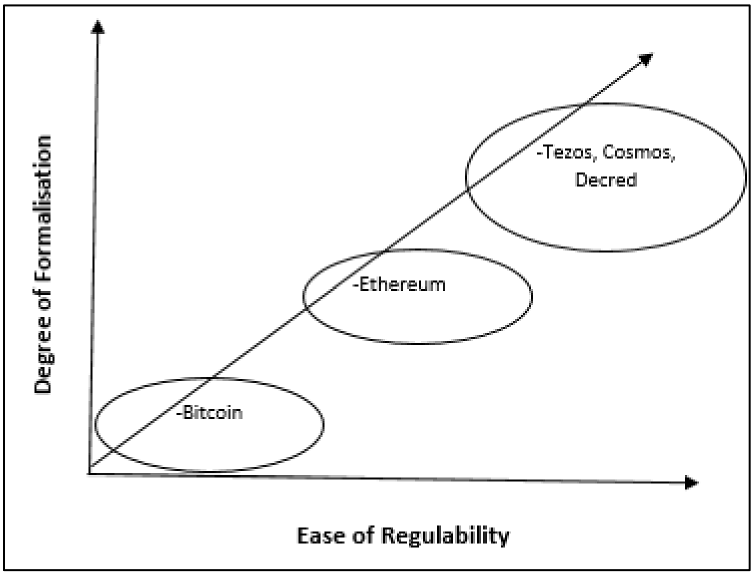
However, this study has shown how Bitcoin's consensus process leads to a lesser degree of governability than Ethereum. In fact, Ethereum's governability goes beyond any other established cryptocurrency, by virtue of having an identifiable corporate structure which presents the possibility of Ethereum being subject to existing law. For example, a common law equitable remedy solution was proposed for the DAO hack, as the DAO itself could be interpreted, in US law, as a 'general partnership' and as such, is subject to corporate governance rules and obligations, in which 'those within this profit-orientated organisation have a duty to behave fairly with their partners and not in his or her 'adverse interest'.[98] This shows that, with regards to the ability of external law to influence internal self-regulatory structures, it is highly evident that there is a positive relationship between the ease of regulability and the degree of formalisation of the cryptocurrency's governance structure.

In other words, the more formalised the consensus model and official the governance structure, the greater the ease of regulability and higher the degree of cognitive openness. As depicted in Figure below, this view would place Bitcoin as the least regulable cryptocurrency of those observed, with other cryptocurrencies falling somewhere along this axis, depending on their own

[97] Kroll (n 66) 18.
[98] Allison (n 90).

governance structures, and where Tezos, Decred and Cosmos displaying the most potential regulability.

Figure 8: Cryptocurrency Cognitive Openness Scale—Relationship between Regulability and Formalisation



This creates a trade-off between maintaining the more informal, looser, decentralised governance structures, technologically and philosophically inherent to the first generation of cryptocurrency projects that were based on anti-institutionalism, and allowing for the introduction of the efficiency gains of more formally recognisable legal governance structures.

The second element of cognitive openness has to do with questioning whether or not legal intervention in this system is needed or necessary. Several commentators have noted that legal intervention in cryptocurrency governance processes is inevitable, and the natural next step in the evolution of this technology. Most notably, Krall and others opine that

> *threats to the Bitcoin community, in the form of actual adversaries, protocol instabilities, and inevitable bugs and accidents, necessarily require mechanisms for governance … and that the emergence of formal governance structures will*

> *ultimately subject Bitcoin itself (and not merely particular players) to influence by government and regulators around the world.*[99]

This conclusion, reached in 2013, has been supported and made even more relevant by recent events around Bitcoin governance, where the decentralised consensus model in use is struggling to arrive at agreement about solutions for a crucial issue. The protracted debate on scaling Bitcoin saw a surge in transaction costs, and left the Bitcoin community in desperate need for a solution. Of further interest in this instance is how the data showed that 27 per cent of miners wanted the mining pool to decide for them, inferring that over a quarter of miners did not care either way.[100] This data questions the assumption that every member of a consensus-based system has an opinion that they need to be heard, and in so doing, raises some pertinent procedural questions in the development of the system.

Similarly, in highlighting some of the problems associated with Ethereum's hard fork, Breitman notes that soft forks and hard forks are becoming a way of life for blockchains, and that is dangerous because 'any fork has the potential to become controversial, and those controversies can weaken a network and stall future growth, just as with the post-DAO fork in Ethereum and the seemingly endless Bitcoin block size debate'.[101] Because of these issues, Breitman proposes that:

> *future blockchains need built-in governance systems. Whenever possible, decisions should happen on chain, not on Reddit or Twitter or some off-site polling tool. And, as part of that governance system, blockchains also need a testnet, so stakeholders can review protocol changes before implementing them.*[102]

[99] Kroll (n 66) 2.

[100] J Buntix, 'Slush Pool Simplifies Voting Process for Segwit and Bitcoin Unlimited' (*DashTimes* 2017) <http://thedashtimes.com/2017/03/06/slush-pool-simplifies-voting-process-segwit-Bitcoin-unlimited/> Accessed 15 May 2017.

[101] Breitman (n 89).

[102] ibid.

These views about the need for and, indeed, inevitability of legal intervention in cryptocurrency's distributed governance process gain credence when consensus is stripped down to its most basic principle—which is the allocation and distribution of power. In consensus algorithms, it has been noted that the proof-of-work algorithm benefits large mining pools, proof-of-stake benefits those with large amounts of currency, proof-of-importance benefits those who hold and actively transfer large amounts of currency, proof-of-burn benefits those with large amount of currency, proof-of-disk-capacity benefits those with a large amount of hardware, and proof-of-time connected benefits people who maintain a stable node with few interruptions.[103]

In this way, the choice of consensus algorithm by programmers represents a political decision concerned with the allocation and distribution of power, rights and responsibilities. Some have even gone as far as stating that cryptocurrency developers are getting close to acting as policymakers because, in the case of Bitcoin, the market has matured to the point where 'a technical decision has economic ramifications and picks winners and losers'.[104] Overall, the dynamics of consensus-based decision making in cryptocurrency markets can be described as 'emerging quasi-political systems' that are 'ill-defined in terms of them having self-consciousness of their political nature',[105] with the latter observation calling for more internal self-reflexion within this system, which a reflexive regulatory approach can aid in providing.

As we have seen, the newer generation of cryptocurrencies have started incorporating more formal, internal, in-built governance structures and mechanisms. This represents a logical evolution in cryptocurrencies, in a direct response to both the internal needs of the system, and external demands on the system. Calls for more formalisation of cryptocurrency governance systems have

[103] D5000 (n 73).

[104] L Shin, 'Why Bitcoin's Greatest Asset could also Spell its Doom' (Forbes 2017) <https://www.forbes.com/sites/laurashin/2017/04/20/why-bitcoins-greatest-asset-could-also-spell-its-doom/#f9ed8126adcd> > Accessed 17 July 2017.

[105] ibid.

come from various quarters,[106] from general to more specific recommendations—for example, that 'an IETF-like working group,[107] in public, with transparency, inclusive of all geographies'[108] be set up. This is in line with innovations such as the establishment of a reputation-based system of community arbitration, obligatory deposits for the duration of a trade, or face-to-face meetings between traders put in place by peer-to-peer exchanges as Local Bitcoins.[109]

These changes are crucial to note for the development of a regulatory approach to legal intervention in the governance of cryptocurrency systems. The problematic areas in consensus-based cryptocurrency governance structures highlight both a need and method for legal intervention—in short, both the justification and avenue for cognitive openness. This means that there is scope for interaction between the legal system and the cryptocurrency system in improving internal governance mechanisms with regulatory aims in mind. At the same time, the self-evolution and incorporation of technology to develop more sophisticated internal governance structures as seen in Tezos, Decred and Cosmos calls for a more nuanced, learning-orientated approached to be taken by the legal system, in order to allow for bi-directional growth and development in both systems.

5.3.4 Consensus – Conclusion

Reflexive regulation takes account of the internal self-regulatory mechanisms within each system. The lesson learnt from a study of consensus models is that cryptocurrency systems are decentralised by design. Decentralisation is not

[106] Lehdonvirta and Ali (n 11).

[107] The Internet Engineering Task Force (IETF) is an open standards organisation developing internet standards.

[108] J Garzik, 'Bitcoin Upgrade Governance, Hard Forks and Segregated Witness' (*Medium.com* 2017) <https://medium.com/@jgarzik/Bitcoin-upgrade-governance-hard-forks-and-segregated-witness-942885e0ce58> Accessed 15 May 2017.

[109] A Marshall, 'P2P Cryptocurrency Markets, Explained' (*Cointelegraph* 7 April 2007) <https://cointelegraph.com/explained/p2p-cryptocurrency-exchanges-explained> Accessed 19 June 2018.

purely functional, for example in ensuring the security of the network by having multiple, disparate nodes, as in the case of Bitcoin. Decentralisation in the DLT that underlies cryptocurrency is a community imperative and community values. It therefore follows that a reflexive regulatory approach to cryptocurrency needs to take into account the communities' ability to arrive at consensus over governance issues collectively, autonomously and democratically.

In order to avoid the regulatory trilemma, regulatory changes should be agreed to by consensus. Whilst this is either difficult and/or impossible to achieve in other regulatory environments, the cryptocurrency systems offers the potential for the application of regulation by consensus. This chapter has shown that there is a need for legal intervention, in order to improve how consensus works within cryptocurrency systems, in order to redirect it towards achieving regulatory goals. As seminally noted by De Filippi,

> *[M]embers of the blockchain community have a lot of power, and are socially accountable for how they choose to exercise, or not exercise this power … if there is no central authority capable of applying the law, the blockchain community is under a moral duty or responsibility to intervene in order to enforce the intention of the law (or of the code, for that matter) so as to preserve public order and morality. This is what 'distributive governance' is about.*[110]

De Filippi's observation is in line with thought on reflexive regulation, where the regulated system or community is called upon to exercise and deploy its internal self-regulatory mechanisms in order to uphold the values of society as a whole, and address issues of regulatory concern where the 'limits on the scope of legality' are apparent.

5.4 Discussion

As explained by Teubner, reflexive regulation calls for a new form of 'legal self-restraint', where 'instead of taking over regulatory responsibility for the outcome

[110] P De Filippi (n43).

of social processes, reflexive law restricts itself to the installation, correction and redefinition of democratic self-regulatory mechanisms'.[111] With this reflexive approach in mind, this chapter has considered computer code and consensus-based distributive governance mechanisms as the two main internal self-governance mechanisms within cryptocurrency systems, and has noted the strengths and areas in need of improvement and support within both code and consensus.

A reflexive approach directed towards computer code would not be to prescribe or dictate what cryptocurrency code should look like, but instead, will be directed towards guiding and improving the internal mechanisms that determine how the final code is arrived at, to incorporate issues of regulatory concern within the code and the code-generation processes through proceduralisation, standardisation and institutionalisation. This is because 'the task of the legal system is neither to develop its own purposive program nor to decide goal conflicts between competing policies. It is to guarantee coordination processes and to compel agreement'.[112]

Similarly, reflexive regulatory interventions targeted at consensus-based distributed governance mechanisms within the cryptocurrency system would be aimed at enhancing and re-directing these, rather than dictating their processes and outcomes, because 'the role of reflexive law is to structure and restructure semi-autonomous social systems by shaping both their procedures of internal discourse and their methods of coordination with other social systems'.[113] Failure to do so would result in ineffectiveness, because despite their regulability or cognitive openness, it has been noted that,

> *still, a regulator's power will be limited by the participants' ability to fork the Bitcoin rules. Even if a regulator forces the developers to incorporate changes into the Bitcoin rules and reference software, the rest of the Bitcoin community*

[111] Teubner (n 1) 239.
[112] ibid 277.
[113] ibid 255.

> *will be able to fork the rules and carry on under the rule set of its choice. Bitcoin is not immune to regulation, but it is not like traditional currencies either … it is an open-source currency.*[114]

It is essentially this open-source nature of cryptocurrencies that not only calls for, but allows for the deployment of reflexive solutions in their regulation. This chapter has shown both potential for code and consensus to be redirected to achieve regulatory goals through their displayed cognitive openness. However, this potential is marred by a myriad of functional challenges that can be significantly improved by legal intervention in this system. Teubner describes how reflexive law can deal with the deficiencies in a system by creating legal structures aimed at systematically strengthening 'reflexion mechanisms' within the system. Linking this to the 'democratisation of social institutions', Teubner asserts that this process is 'the design of organisational structures which makes the institution … sensitive to the outside effects of their attempts to maximise internal rationality'.[115]

Here, it must be noted that, unlike other regulatory approaches and theories, the function of reflexive regulation is to substitute for outside interventionist control an 'effective internal control structure'.[116] The shortcomings and challenges of code and consensus mean that there is a distinct role for the law, where 'law must act at the sub-system-specific level to install, correct, and redefine democratic self-regulatory mechanisms'.[117] The concluding chapter of this thesis will explore the means through which a reflexive regulatory approach might be arrived within the cryptocurrency system, through legal intervention in the development of code and consensus.

[114] Kroll (n 66) 19.
[115] Teubner (n 1) 269.
[116] ibid 278.
[117] ibid 275.

5.6 Conclusion

This chapter has presented the main mechanisms through which cryptocurrency systems self-regulate and self-govern as a necessary pre-cursor to the core component of reflexive regulation, which is to redirect internal self-regulatory mechanisms towards regulatory goals. Here, the two main internal governance mechanisms within cryptocurrency system were identified as 'Code' and 'Consensus' and were analysed in turn with a focus on their operational closure (functionality) and cognitive openness (regulability). The discussion on code presented an understanding of 'law through code' as a means of maintaining the operational closure of the legal and the cryptocurrency systems respectively, whilst accounting for the cognitive openness that allows the legal system to influence the cryptocurrency system and vice versa. Concurrently, observations relating to the notion of consensus concluded that whilst the cryptocurrency systems offers the potential for the application of regulation by consensus, there is a need for legal intervention, in order to improve how consensus works within cryptocurrency systems, in order to redirect it towards achieving regulatory goals.

In this way, this chapter highlighted not only the avenues and means for legal intervention within these internal governance structures of cryptocurrencies, but identified the role of law and legal intervention in ameliorating these self-regulatory mechanisms, in order to address the issues of regulatory concern. What follows is the presentation of reflexive strategies for enhancing and supporting internal self-regulatory mechanisms of cryptocurrencies in a manner that is consistent to a reflexive law approach.

Chapter Six: Reflexive Strategies for Enhancing and Supporting Internal Self-Regulatory Mechanisms

> *Law realises its own reflexive orientation insofar as it provides the structural premises for reflexive processes in other social subsystems … Thus law must act at the subsystem-specific level to install, correct, and redefine democratic self-regulatory mechanisms. Law's role is to decide about decisions, regulate regulations, and establish structural premises for future decisions in terms of organisation, procedure and competences.*[1]

6.1 Introduction

This chapter will provide strategies for the reflexive regulation of cryptocurrencies, based on observations on the structure and self-regulatory mechanisms of the cryptocurrency system made in the preceding chapters. Here, the focus will be on five key recommendations, stemming from the use of code and consensus as internal self-regulatory mechanisms within the cryptocurrency system. Further expanding on previous chapters, these recommendations are made in light of the identified issues of regulatory concern, and in recognition of the highlighted 'limits in the scope of legality', and regulatory gaps and fissures present in current off-chain cryptocurrency regulation. Most importantly, these recommendations are embedded within a reflexive law orientation, characterised by the primacy of proceduralisation.

According to Teubner, proceduralisation is the process through which the legal system concerns itself with providing the structural premises for self-regulation within other social systems.[2] It is a process through which the law restricts itself, in recognition of its limited capacity to directly influence other social systems,

[1] G Teubner, 'Substantive and Reflexive Elements in Modern Law (1983) 17 Law & Soc Rev 239, 275.

[2] ibid 274.

‘making decisions about decisions’ in a manner that has been described as ‘social gardening’ rather than ‘social engineering’.[3]

More specifically, as described by Julia Black,

> *Procedural law is the adoption of indirect mechanisms for regulating social behaviour, the regulation of organisation and procedures, the redistribution of power and competences. It is the replacement of state control with effective internal control; the creation of structural conditions for an ‘organisational conscience’ that would reflect the balance between the system's relation with other systems and its relationship with itself. Procedural law is a shift to more indirect and abstract guidance mechanisms, but ones which are, like material law, purposive in their orientation. It is the recognition of a heterarchical and not hierarchical relationship between politics, law and other social systems; its central characteristic is decentral, context regulation. It attempts to affect (irritate) the system in such a way that it moves from its current state to that which is required.*[4]

The prerequisite for adopting a procedural approach to regulation is an examination and understanding of the strategic structures of the target system, in order to ascertain ‘what makes them tick’.[5] To reiterate, the strategic structures of the cryptocurrency system have been identified as being based on the interplay between code and consensus mechanisms in the delivery of financial services operating within a social system. What follows are procedural and reflexive regulatory recommendations designed to ‘irritate’ (in Black’s terminology) the cryptocurrency system towards the development of a ‘organisational conscience’, aimed at achieving regulatory goals in light of the code and consensus-based characteristics of this system.

[3] G Teubner, ‘Regulatory Law: Chronicle of Death Foretold’ (1992) 1 *Social and Legal Studies* 451, 463, quoting F Scharpf, ‘Grenzen der institutionellen Reform’ (1987) *Jahrbuch zur Staats und Verwaltungswissenschaft* 111.

[4] J Black, ‘Proceduralizing Regulation: Part 1’ (2000) 20 *OJLS* 597, 603.

[5] ibid.

6.2 Strategies for the Reflexive Regulation of a Cryptocurrency as Code-Based System

In Chapter 5, computer code was identified as the first main internal self-regulatory mechanism of the cryptocurrency system, as it performs the dual function of generating and governing cryptocurrency functionality. Here, it was concluded that a reflexive approach to the use of code in the regulation of cryptocurrency should place emphasis on the notion of law through code, and calls for regulatory intervention aimed at re-directing this internal self-governance tool to work for law—and not against it—through the incorporation of compliance and regulation-targeted code into existing transaction code. Following up on this train of thought, we can recommend that considerations from the regulation of algorithms should be applied to cryptocurrency, that legal programming and regtech should be regularised through proceduralisation and that competition within cryptocurrency markets should be promoted.

6.2.1 Recommendation 1: Regulate Algorithms

The consideration of areas where insight can be gained from existing regulation of algorithms is reflexive in its direct link to an internal self-regulatory mechanism of the cryptocurrency system. In this way, the regulation of algorithms, if reflexively applied, could be seen as a complementary regulatory tool that could be used irritate the internal mechanisms of the cryptocurrency system towards achieving regulatory goals in a manner that avoids the regulatory trilemma.

Since the advent of algorithmic trading in securities markets, various regulatory initiatives have been put in place, aimed at overseeing their use in trading, in order to ensure financial market stability and investor protection. Whilst having led to timelier executed trades based on pre-determined criterion, the use of algorithms—particularly more advanced, intuitive models powered by Artificial Intelligence (AI) and Machine Learning (ML)—has also resulted in a new suite of regulatory concerns. These have to do with the challenges of determining liability between traders and computer systems in the event of the execution of bad trades, as well as determining the causal links between algorithm use and market integrity and financial stability. The use of algorithms in the global financial system has also risen to the attention of regulators, where these have been involved in making consumer-related decisions, such as the determination of credit-worthiness by banks, and prudential decisions around the calculation and monitoring of capital adequacy. These considerations have led regulators to start considering oversight mechanisms for algorithms in the financial system. In the UK, the FCA has highlighted five key compliance areas around the use of algorithms, namely:

> *a full understanding and management of algorithms across the business; robust development and testing processes for algorithms; pre and post trade risk controls; an effective governance and oversight framework; and the ability to monitor for potential conduct issues and thereby reduce market abuse risks.*[6]

More generically, the regulation of algorithms has focused on the opening up of 'black boxes', in order to explain to regulators, in layman terms, the underlying code-bases and parameters of each algorithm deployed by financial institutions. The key insights to be gleaned from these regulatory issues and initiatives for the purposes of the reflexive regulation of cryptocurrencies has to do with the need for the regulator to have a better understanding of the underlying proofs and protocols of each cryptocurrency.

Using standardisation and proceduralisation tools, regulators will be able to edge out of the market regulatory undesirable cryptocurrencies, such as privacy coins, by putting in place code-based criterion for market participation. The same principles of disclosure and evaluation can be applied to address security concerns on cryptocurrency exchanges and platforms to ascertain their robustness. These measures might be more effective than existing substantive

[6] FCA, 'Algorithmic Trading Compliance in Wholesale Markets' (*Financial Conduct Authority* February 2018) <https://www.fca.org.uk/publication/multi-firm-reviews/algorithmic-trading-compliance-wholesale-markets.pdf> Accessed 1 June 2018.

off-chain regulations and requirements around capital adequacy and cybersecurity, as they are aimed at addressing the shortcomings of the code itself rather than the institutions using the code. However, it must be noted that regulating algorithms in this way should be based on regulatory goals and objectives and not excessive prescription, in order to be coherent with the reflexive framework.

6.2.2 Recommendation 2: Support the Development of Legal Programming, Regtech and Regulatory Smart Contracts

As alluded to in Chapter 5, the code-based nature of cryptocurrencies allows for the development of in-build regulatory compliance mechanisms through the use of programming. Legal programming involves the incorporation of legal criteria in software design, in order to 'model legal constraints and dependencies within process models so that the relations and transactions between agents are compliant on all levels'.[7] Similarly, and more generally, regtech can be defined as 'any technological innovation that helps efficiency and transparency in regulation',[8] or alternatively defined as referring to 'a set of companies and solutions that address regulatory challenges across industries, including financial services, through innovative technology'.[9]

The instances of the applications, strengths and weaknesses of the use of regtech and legal programming in the regulation of cryptocurrencies have been discussed at length in Chapter 5, illustrating the cognitive openness of the cryptocurrency system. A key finding of Chapter 5 was the recognition of the need and scope for intervention of the legal system in the use of code as a governance mechanisms. This is primarily due to the fact that with code, once run, there is no room for interpretation, for the taking into account of unique or

[7] M Bain and B Subirana, 'E-commerce Oriented Software Agents' (2004) 20 CLSR 1.

[8] Deloitte, 'RegTech is the New FinTech' (Deloitte 2016) <https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/FinancialServices/IE_2016_FS_RegTech_is_the_new_FinTech.pdf> Accessed 6 June 2017.

[9] M Cavallo, 'How RegTech Closes the Gap Between Technology and Financial Services' (CIO 2017) <http://www.cio.com/article/3190162/it-industry/how-regtech-closes-the-gap-between-technology-and-financial-services.html> Accessed 6 June 2017.

special circumstances, or for the application of the spirit of the intended regulation—as has been shown by the numerous cited instances where code and legal programming has failed to achieve the desired regulatory outcomes.

In this instance, a reflexive area of intervention would involve procedures aimed at assessing and monitoring the quality of regtech and legal programming solutions and outputs. This indirect oversight can potentially be achieved by considering the applicability of regulations around data reporting services. In the UK, entities intending to provide a data reporting service (DRS) need to be authorised (or verified, in the case of trading venue operators) by their national competent authority before they may provide the service.[10] The regulatory functions of regtech and legal programming companies fall within the scope of data reporting services providers (DRSPs) such as Approved Reporting Mechanisms (ARMs), Approved Publication Arrangements (APAs) and Consolidated Tape Providers (CTPs),[11] each with specific requirements and conditions as stipulated by the Data Reporting Services Regulation 2017.[12]

By putting in place procedures and structures that allow regtech and legal programming providers to develop solutions for in-built cryptocurrency compliance around AML and KYC, regulators can have effective control over the quality of the regulatory outputs of these tools—which will, in turn, lead to the enhancement of these internal self-regulatory mechanism through reflexivity**.**

6.2.3 Recommendation 3: Promote Competition

The third recommendation for a reflexive regulation approach, based on cryptocurrency as a code-based system, has to do with the promotion of competition in the cryptocurrency industry. An understanding of what makes the

[10] FCA, 'Data Reporting Service Providers' (*Financial Conduct Authority*, 13 January 2017) <https://www.fca.org.uk/markets/data-reporting-services-providers-drsps> Accessed 2 June 2018.

[11] ibid.

[12] Data Reporting Services Regulation 2017 <http://www.legislation.gov.uk/uksi/2017/699/contents/made> Accessed 2 June 2018.

cryptocurrency system 'tick' leads to the realisation that when participants can avoid regulation and obligations by shifting their operations exclusively online, reflexivity in regulation needs to be targeted at incentivising compliance, with strategies on how to align these incentives with regulatory goals.

A key strategy in incentivising positive behaviour, when cryptocurrency participants and service providers are operating exclusively online, is through supporting and enhancing competition. According to Cave, in internet regulation,

> *[C]ompetition and consumer protection must be seen as complements: effective competition forces firms to identify and serve consumer needs and desires while consumer protection enables users to seek out better offers from rival suppliers.*[13]

The existence of a competitive market in cryptocurrency is already acting as an incentive to comply with regulation. This is illustrated by the case of the cryptocurrency exchange Gemini. Gemini was one of the first exchanges to successfully apply for and obtain the New York Bitlicense in 2015.[14] The founders of Gemini stated their goal to become market leaders in this space by assuring potential investors that they were safe and compliant, at a time when other cryptocurrency companies were leaving the jurisdiction.[15] Gemini put in place measures such as ensuring that all fiat currency transferred to them was deposited in an FDIC-insured New York state chartered bank, and meeting requirements including adherence to robust AML regulations, internal controls and procedures, and comprehensive security programs. In this way, a bridge was

[13] J Cave, 'Policy and Regulatory Requirements for a Future Internet' in Ian Brown (ed) *Research Handbook on Governance of the Internet* (Edward Elgar 2013) 143, 147.

[14] H Lombardo, 'Winklevoss Gemini Exchange Gets BitLicense for Oct 8th Official Launch' (*Allcoinsnews,* 6 October 2015) <http://allcoinsnews.com/2015/10/06/winklevoss-gemini-exchange-gets-bitlicense-for-oct-8th-official-launch/> Accessed 27 May 2018

[15] For an overview of cryptocurrency regulatory arbitrage across jurisdictions, see Gregory Klumov, 'How Various Countries Benefit and Suffer from Regulation Arbitrage Today' (*Bitcoinist.com,* April 21, 2018)<http://bitcoinist.com/countries-benefit-suffer-regulation-arbitrage/> Accessed 27 May 2018.

built between Gemini's market-driven incentives and the regulator's compliance goals around consumer and investor protection.

Always aiming to stay ahead of the competition, in April 2018, Gemini launched a block-trading product aimed at retaining and attracting institutional investors, by allowing them to buy and sell large volumes of digital assets outside the exchange's continuous order books.[16] This competitive drive inadvertently addressed the regulatory concerns around the volatility of cryptocurrency markets. Here, the relative immaturity of the cryptocurrency market means that when institutional investors were trading in the usual Gemini platform, they created significant price swings each time they placed their large orders. With the high liquidity block-trading facility, it is envisaged that the price volatility of cryptocurrencies such as Bitcoin and Ethereum will significantly reduce,[17] increasing market stability.

Similar alignment between incentives and regulatory goals, highlighting the link between competition and consumer protection, is the growing trend in cryptocurrency exchanges delisting trading pairs for privacy-centric cryptocurrencies such as Monero, Zcash and Dash. An example of this is the Japanese-based Coincheck, which announced the removal of less traceable cryptocurrencies from their platform after a $530 million hack.[18] This decision was not a response to any form of compulsion by regulators, but instead, was described as being motivated by the need to retain customers, in what has been described as an attempt to bring the platform back into Japan's Financial Services Agency (FSA)'s 'good graces'.[19] The first observation here is that Coincheck independently and organically addressed the regulatory concerns around compliance with AML and KYC regulation posed by privacy coins, in a bid to

[16] J Buntix, 'Gemini Launches Block Trading to Attract Institutional Investors' (*The Merkle* 12 April 2018) <https://themerkle.com/gemini-launches-block-trading-to-attract-institutional-investors/> Accessed 27 May 2018.

[17] ibid.

[18] J Wilmoth, 'Coincheck to Delist Privacy Coins Monero, Zcash and Dash' (*CCN.com* 19 May 2018) <https://www.ccn.com/coincheck-to-delist-privacy-coins-monero-zcash-and-dash/> Accessed 27 May 2018.

[19] ibid.

retain customers and stay competitive in the market. The second key observation is that the FSA placed itself in a position where its licencing regime acts as a 'carrot', linking directly with the market-driven incentives of the regulatory target.

Most significantly, these two examples illustrate the role of competition in promoting consumer protection in the cryptocurrency system, which, similar to the internet, is characterised by the need to incentivise positive behaviour due to the ability of market participants to easily move online in order to circumvent regulation and evade obligations. Based on the implications of the complex nature of the cryptocurrency system, therefore, a key recommendation for the reflexive regulation of cryptocurrencies would be to actively promote competition within cryptocurrency markets.

The role of competition in the cryptocurrency system has already started to be examined. An April 2018, an OECD study raised the possibility of several competition and anti-trust issues that might arise in blockchain and cryptocurrency markets.[20] These include the potential of intermediaries, such as firms that sell specialised cryptocurrency mining hardware, to exploit and exclude based on their market dominance, where the absence of alternatives leaves market participants vulnerable to excessive pricing in the absence of regulation[21]. Secondly, there is a concern that dominant cryptocurrencies might exploit their network effects[22] primacy to charge excessive transaction fees, which might in turn further entrench their position. Both instances can be illustrated by the case of Chinese cryptocurrency firm Bitmain, which has been

[20] OECD, 'Blockchain Technology and Competition Policy' (*OECD,* June 8, 2018) <https://one.oecd.org/document/DAF/COMP/WD(2018)47/en/pdf> Accessed 28 May 2018.

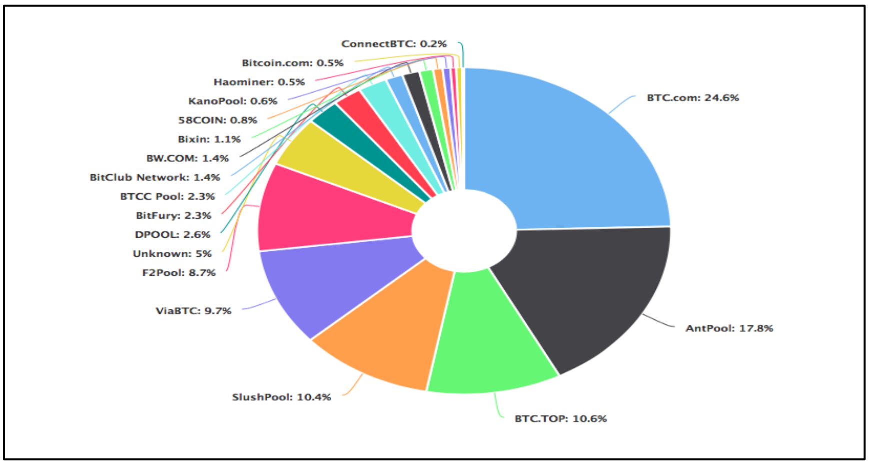
[21] ibid.

[22] 'Network effects' are the incremental, and exponential, benefit gained by users of a platform for each new user that joins the platform. Definition from *Investopedia* < https://www.investopedia.com/terms/n/network-effect.asp> Accessed 3 March 2020

described as having near-monopoly in Bitcoin hardware, whilst also having a market-dominant mining pool operation.[23]

Initially, Bitcoin was mined using software that could be found on the CPUs of normal computers. However, in 2013, a specialised software development exclusively for cryptocurrency mining, ASIC (Application Specific Integrated Circuits), catalysed the development of the industry. With one ASICs costing around $2,000,[24] a company such as Bitmain (the chief supplier of ACISs, being in possession of warehouses full of this hardware) becomes an even more dominant force in the cryptocurrency mining, when it starts mining itself.[25] Currently, Bitmain operates two of the largest Bitcoin mining operations in the world (AntPool and BTC.com), that together account for 42.4% of the entire network's mining power as shown in Figure below.

Figure 9*: Hashrate Distribution—Market Share of Largest Mining Pools*



Source: blockchain.com [26]

[23] D Oberhaus, 'What Happens When a Chinese Giant Swoops in on Your Tiny Cryptocurrency' (*Motherboard* January 22, 2018) <https://motherboard.vice.com/en_us/article/ev59dz/bitmain-siacoin-obelisk-asic-vorick> Accessed 1 June 2018.

[24] ibid.

[25] J Wong, 'China's Bitmain Dominates Bitcoin Mining', (*Quartz* August 20, 2017) <https://qz.com/1053799/chinas-bitmain-dominates-bitcoin-mining-now-it-wants-to-cash-in-on-artificial-intelligence/> Accessed 1 June 2018.

[26] Blockchain.com 'Hashrate Distribution' (*Blockchain.com* 2017) <https://www.blockchain.com/en/pools> Accessed 1 June 2018.

This dominance is particularly concerning in light of the 51% Attack problem for proof-of-work based cryptocurrencies such as Bitcoin, Ethereum, Litecoin, Monero and Dash—where any mining operation that controls 51% of the network can override and manipulate the network's transaction history.[27] Bitmain did, in fact, play a leading role in the Bitcoin hard fork that led to the cryptocurrency being split in two in 2017.[28]

Most recently flagged is the move by Bitmain to essentially take over the mining of the US-based Netflix-affiliated blockchain company Sia, which requires specialised hardware to mine its network cryptocurrency, Siacoin. Bitmain has begun to both produce and mine Siacoin, leaving Sia in a position where it is unable to compete with a firm of Bitmain's size. Whilst several other Chinese mining hardware suppliers have expressed interest in producing the ASIC hardware specific to Siacoin's code, thereby potentially reducing Bitmain's monopoly, there is still a concern that Bitmain may have already flooded the market before its competitors' deployment.[29] With the previous impediment of high cost preventing a 51% attack now significantly reduced,[30] the competition concern around consumer and investor protection is rising in significance.

Addressing the adequacy of competition policy in cryptocurrency markets, Østbye claims that traditional competition policy instruments, such as antitrust and regulation, are inadequate to address competition policy concerns around cryptocurrency.[31] This is due to the fact that competition and antitrust law is a reactive tool to foster competition, displaying shortcomings in fostering competition in the first place.[32] This is in line with the observations made in this

[27] SNakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (*Bitcoin.org* 2009) <https://bitcoin.org/bitcoin.pdf> Accessed 27 May 2018.

[28] Wong (n 25).

[29] Oberhaus (n 23).

[30] K Sedgwick, 'You Can Now 51% Attack a Coin for as Little as $500' (*Bitcoin.com* May 29, 2018) <https://news.bitcoin.com/you-can-now-51-attack-a-coin-for-as-little-as-500/> Accessed 1 June 2018.

[31] P Østbye, 'The Adequacy of Competition Policy for Cryptocurrency Markets' (*SSRN* 2017) <https://ssrn.com/abstract=3025732> Accessed 27 May 2018.

[32] ibid.

thesis about limits in the scope of legality and shortcomings of substantive legal rules in addressing cryptocurrency regulation. Providing an alternative to competition and antitrust law, Østbye proposes regulation and government participation in the cryptocurrency markets. Here, regulatory tools suitable to addressing competition in cryptocurrency markets (with the caveat of stated enforcement challenges and unintended consequences) are the capping of transaction fees similar to the EU payment services directive PSD2, the mandating exchanges and merchants to accept all cryptocurrencies, instruments such as the use of central counterparty clearing CCPs aimed at preventing wallets and exchanges becoming dominant, and the reduction of barriers to entry imposed by AML/KYC and capital requirements.[33]

In terms of government participation, Østbye states that 'as an alternative to regulation … governments may prevent exploitation of market power in the cryptocurrency markets by augmenting their national currencies to be better substitutes to private cryptocurrencies'.[34] This proposal supports recent government exploration into central bank issued digital currency (CBDC),[35] characterised by an augmentation of blockchain technology to allow for the execution of monetary policy.

With enforcement challenges around these proposals in mind, a reflexive law approach to fostering competition within cryptocurrency markets could, instead, draw from soft law application of competition law. For example, the European Commission-issued competition guidelines and notices put in place, in order to add legal consistency to decentralised national enforcement systems through Article 101 and Article 102 of the TFEU.[36] Whilst there have been varying degrees

[33] ibid.

[34] ibid 32.

[35] Governments experimenting with central bank digital currencies include Sweden, China, Venezuala and Estonia; also see M Orcutt, 'Governments Are Testing Their Own Cryptocurrencies' (*MIT Technology Review* September 25, 2017) <https://www.technologyreview.com/s/608910/governments-are-testing-their-own-cryptocurrencies/> Accessed 1 June 2018.

[36] European Commission, 'Competition' (*European Commission* 2014) <http://ec.europa.eu/competition/antitrust/overview_en.html> Accessed 1 June 2018.

of success with this regime,[37] the overarching prohibition of agreements between two or more independent market operators which restrict competition (such as cartels) in Article 101, and the prohibition of firms that hold a dominant position on a given market to abuse that position (for example, by charging unfair prices) in Article 102, with appended rules on procedures for anticompetitive prices cases, procedures for abuse of dominance cases and key actors and checks and balances proceeding for the application of Articles 101 and 102 of the TFEU[38] present the possibility for application within the reflexive regulation of competition in cryptocurrency markets, with a view to indirectly foster consumer and investor protection. However such procedural guidelines for cryptocurrency markets may require structural institutional support as shall be further discussed below.

6.3 Strategies for the Reflexive Regulation of Cryptocurrency as a Consensus-Based System

The second set of recommendations around a reflexive approach to the regulation of cryptocurrencies is based on the use of consensus mechanisms as an internal self-regulatory mechanism of the cryptocurrency system. As described in Chapter 5, consensus is the mechanism through which decisions on a distributed network involving multiple participants are made. In the cryptocurrency system, this involves the use of code-based consensus models (such as proof-of-work and proof-of-stake) that decide cryptographically which market participants have the authority to verify transactions, as well as human rule-making regarding decisions on changes to cryptocurrency code and functionality. In this instance, three recommendations can be considered, aimed at enhancing and supporting consensus within the cryptocurrency system, with the aim of achieving regulatory goals. These are the facilitation of discursive

[37] Z Georgieva, 'Competition Soft Law in French and German Courts: A Challenge For Online Sales Bans Only?' (2017) 24 Maastricht Journal of European and Comparative Law 2, 175; Z Georgieva, 'The Judicial Reception of Competition Soft Law in the Netherlands and the UK' (2016), 12 European Competition Journal 54.
[38] European Commission (n 36).

participatory democracy, the establishment of fiduciary duties, and the development of standardisation and Codes of Conduct.

6.3.1 Recommendation 4: Facilitate Discursive Participatory Democracy in Rule Formulation

Having already established the need to reduce information asymmetries in order to enhance competition (for consumer protection) and add predictability (and therefor regulability) to cryptocurrency markets), it is also evident that the ability for cryptocurrency market participants to decide on changes to code is an effective way to ensure market integrity. According to Cave,

> *the retention by internet users of a range of powers—eg to collect and share information about internet stakeholders' activities, to negotiate and agree to abide by standards, etc—can thus help to preserve the self-correcting capabilities of the internet. This may be preferable to more formally-constituted and legally-backed forms of regulation, if only because such regulatory bodies … may tend to view changes in light of existing rules and thus to miss emergent opportunities.*[39]

In this way, empowering cryptocurrency market participants through access to information and through the ability to more effectively participate in decision-making processes is key. As shown in Chapter 5, the process through which decisions are made about changes to cryptocurrency code is fraught with complications and inadequacies, which often lead to the development of inefficiencies within cryptocurrency markets, and the deployment of solutions by core developers that may not be in the best interest consumers. This can be illustrated by responses to the 51% attack problem which has had inconsistent levels of success. In 2014, bitcoin miners around the world decided to leave the Ghash.io mining pool after the bitcoin community became aware that Ghash.io

[39] Cave (n 13) 159.

had started to account for more than 42% of bitcoin mining power. As reported by Hajdarbegovic,

> *The fact that a single pool has such a high share has prompted some bitcoin miners to voice their concerns on social media and the mining community is starting to take notice. If a single entity ends up controlling more than 50% of the network's computing power, it could – theoretically – wreak havoc on the whole network.*[40]

These concerns were shared and addressed on social medial, which led to the organic and spontaneous provision of a solution. However, a more recent example on how a 51% attack was handled highlights the weaknesses of this current system. In this instance, tweets by Cryptoconomy Podcast host Guy Swann in May 2019 were the sole source of information explaining that a 51% attack on bitcoin cash (BCH) carried out by two mining pools was not malicious, as was initially assumed, but instead the mining pools were trying to prevent a theft in BCH resulting from vulnerabilities presented by a code update.[41] Having a social media outlet as the primary source of information and as the sole mechanism for debate and discussion amongst the cryptocurrency community is precarious as it leads to confusion and uncertainty around the accuracy of unverified reports. Whilst social media and other informal, decentralised digital platforms will always have a vital role to play in the cryptocurrency ecosystem, having more structured and better defined processes and mechanisms to arrive at infrastructure-critical decisions will be essential in improving and and redirecting consensus mechanisms within this system towards regulatory goals.

Delving further into reflexive law theory provides more insight into the potential form and features of a procedural law approach to enhancing and supporting

[40] N Hajdarbegovic, 'Bitcoin miners ditch Ghash.io pool over fears of 51% attack' (*Coindesk* 9 January 2014) <https://www.coindesk.com/bitcoin-miners-ditch-ghash-io-pool-51-attack> Accessed 1 June 2018.

[41] M Boddy, 'Two Miners Purportedly Execute 51% Attack on Bitcoin Cash Blockchain' (*Cointelegraph*, 25 May 2019) < https://cointelegraph.com/news/two-miners-purportedly-execute-51-attack-on-bitcoin-cash-blockchain> Accessed 8 September 2020.

consensus mechanisms towards achieving regulatory goals. Drawing from the work of Habermas, Teubner presents a view of law as an external constitution that can promote 'discursive decision processes and consensus-orientated procedures of negotiation and decision', by 'providing norms of procedure, organisation, and competencies that aid other social systems in achieving the democratic self-organisation and self-regulation which … are the heart of procedural legitimacy'.[42]

Commenting on the same line of enquiry around procedures, participant and institutional design, Julia Black states that proceduralisation, as advocated by Teubner, is based on the design of the decision processes of organisations so as to ensure internal democratisation and external responsiveness, where 'the substantive content of regulatory norms should be determined by a particular mode of decision making, that is participation and deliberation'[43]. In this way, Black places emphasis on the inextricability of participation from proceduralisation. Here, she makes the distinction between a 'thin' concept of proceduralisation, where procedures have to do with bargains and compromises, and 'thick' proceduralisation, which is a more deliberative form of proceduralisation, orientated towards the 'mutuality, consensus and inter-subjective understanding of deliberative democracy'.[44] It is the latter approach that will be used in the consideration of procedural strategies in cryptocurrency regulation.

Whilst the cryptocurrency system is built on consensus, it faces challenges within decision-making processes, around who makes changes and improvements to cryptocurrency code, and what these changes should consist of — in other words, procedures for internal democratisation. Facilitating internal democratisation in cryptocurrency code and consensus mechanisms will entail considering procedures aimed at facilitating discursive stakeholder participation, and as shall

[42] Teubner (n 1) 275.
[43] Black (n 4) 589.
[44] ibid 599.

be further elaborated on below, the development of institutional infrastructure to facilitate and organise decision making within the cryptocurrency system. However, in order to achieve regulatory outcomes, the reflexive role of law in the regulation of cryptocurrency should extend beyond supporting the democratisation of internal self-regulatory mechanism, to include procedures aimed at re-directing these mechanisms towards addressing issues of regulatory concern. In other words, internal democratisation through participation and institutional infrastructure should be aimed at ensuring external responsiveness towards achieving regulatory goals.

In this instance, overlaying external responsiveness to participatory and institution-based procedures entails adding substantive considerations targeted at addressing issues of regulatory concern. Here, the discussion will focus on including the regulator in the participatory framework, through the amplification of the regulatory sandbox model, as shall be further elaborated on below. It also entails considering the 'ideal speech situation'[45] as the ideal format for deliberation. The ideal speech situation provides a benchmark for discursive procedures around the generation and modification of code in cryptocurrency systems. In an ideal speech situation, the requirements of public reason mean that each participant has to put forward reasons that others could reasonably accept their point of view, and reject proposals on the basis that insufficiently good reasons have been offered for them. In other words, the only influence exercised in an ideal speech situation is the force of the better argument.[46]

This ideal speech requirement can translate into 'the best code wins' as a way for market participants to exercise quality control. In this case, standards and procedures around the vetting process of code appended to an internal voting mechanism can be put in place. Indeed, as explained in the preceding chapter,

[45] J Habermas, *Theory and Practice*, J Viertel (tr), (Heineman 1974); J Habermas, *The Theory of Communicative Action* (Beacon Press 1984); J Habermas, 'Three Normative Models of Democracy' in S Benhabib (ed), *Democracy and Difference: Contesting the Boundaries of the Political* (Princeton UP 1996).
[46] ibid.

there are already cryptocurrencies that have developed in-build voting mechanisms to facilitate smoother decision making around alteration and improvement to code. Similarly, having developers present an overview and test-run to their proposed changes, such as BIPs and EIPs, will prove to be a key strategy in the democratisation and transparency of decision making within the cryptocurrency system.

6.3.2 Recommendation 5: Develop Appropriate Institutional Infrastructure

In order for the procedural recommendations proposed above to be operationalised, there is a need to develop an institutional framework from which to transmit the development of these procedures on a global scale. In other words, proceduralisation needs institutional infrastructure and a supranational approach to cryptocurrency regulation, coordinating and framing the recommendations of organisations such as the FATF, IMF, CFTC on cryptocurrencies, as well as the recommendations proposed in this thesis.

Here, discussions on competition showed how the EU is able to coordinate the national implementation of competition policy through the recommendations and guidelines issues by the EC. A proposal may be appropriate for a similar list of guidelines from a sui generis cryptocurrency oversight body, perhaps with similar powers to issue fines and conduct investigations. Similarly, institutional support for the development of standards and codes of conduct might be both necessary and appropriate. As stated by Cave, one of the recommendations of the governance of the future internet is the development of:

> *competitiveness-enhancing infrastructural change by strategic engagement in inter and multi-national fora, involved with internet architectures and governance by supporting research and standardisation endeavours that will drive the frontiers of internet development.*[47]

[47] Cave (n 13) 163.

There is also a need for institutional infrastructure to promote discursive processes. In order for rights to be enforced, according to Habermas, in an 'ideal speech' situation, the community has need of the institutions of an organised legal system and the sanctioning power of an organisation that can make collectively binding decisions.[48] Institutions are key in thick proceduralisation, as they provide a platform from which deliberative, democratic self-governance can take place. As has been previously noted, cryptocurrency debates need to move out of Reddit, Github and Twitter, into a more organised space.

6.3.3.1 Regulatory Sandboxes

A pre-existing model that can be expanded upon to play this institutional role in the cryptocurrency system is that of regulatory sandboxes, which can be enhanced to serve as a locus for discursive procedures that support participatory democracy. Initiated by the FCA, the regulatory sandbox model was developed to allow businesses to test innovative products, services, business models and delivery mechanisms in the real market, on real consumers, with few or no restrictions. The sandbox also offers tools such as restricted authorisation, individual guidance, informal steers, waivers, and no enforcement action letters, and has already had cohorts consisting of several cryptocurrency firms.[49] In this way, the use of a regulatory sandbox addresses the issue of 'governance problems aris[ing] when regulators do not know what the stakeholders know (and thus cannot integrate their knowledge and/or cannot (cost-effectively) observe (let alone compel) their actions'.[50]

The regulatory sandbox can be conceptualised as a procedural law technique or 'institution', due to the fact that it is discursive and facilitative, and presents a bi-

[48] J Habermas, *Facts and Norms* paraphrased by J Black, 'Proceduralizing Regulation' (2001) 21 *OJLS* 1.
[49] Financial Conduct Authority, 'Regulatory Sandbox Lessons Learnt Report' (2017) <https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf> Accessed 14 May 2018.
[50] Cave (n 13).

directional learning opportunity between the regulatory and the regulatory target. In this case,

> *The sandbox provides access to regulatory expertise and a set of regulatory tools to facilitate testing. Sandbox firms are assigned a dedicated case officer who supports the design and implementation of the test. This close contact enables case officers to help firms understand how their innovative business models fit within the regulatory framework. It also ensures that appropriate safeguards are built into innovative products and services during and after testing.*[51]

With more and more countries beginning to implement regulatory sandboxes to address the regulation of cryptocurrency and other nascent financial technology,[52] and the proposal to put in place a global regulatory sandbox already being tabled,[53] regulatory sandboxes may present an institutional base for putting in place procedural mechanisms aimed at re-directing the internal self-regulatory mechanisms of the cryptocurrency system towards achieving regulatory goals. The call for flexibility in internet regulation raised by Cave is also pertinent here. In order for the potential of regulatory sandboxes to be fully realised, there must be regulatory flexibility 'to construct and continuously to monitor multi-stakeholder discourse platforms and to support appropriate regulatory innovation and regulatory withdrawal where possible'.[54] This is a call to internal reflexivity within the legal system itself, as it would entail critical self-evaluation and reflection of the role, positioning and functioning of the law vis-à-vis the regulatory target. In this case, the regulator would become a node and a participant within the regulatory process, and not merely an observer, in order to better understand and influence developments within the target system.

[51] Financial Conduct Authority (n 66).

[52] Lithuania's new blockchain sandbox as an example of this; see <https://fintechbaltic.com/2018/04/19/lithuania-to-introduce-blockchain-sandbox-in-2019/> Accessed 14 May 2018.

[53] G Conheady, 'Is Fintech Ready for a Global Regulatory Sandbox?' (*A&LGoodbody* 27 November 2018) <https://www.algoodbody.com/insights-publications/is-fintech-ready-for-a-global-regulatory-sandbox> Accessed 17 February 2020.

[54] Cave (n 13) 162.

6.4 Conclusion

This chapter has provided recommendations to arrive at a reflexive approach to the regulation of cryptocurrencies. These recommendations have been based on the manner in which cryptocurrencies operate based on the use of code and consensus as internal self-governance mechanisms within cryptocurrency systems. Aimed at evading the regulatory trilemma, whilst addressing issues of regulatory concern posed by cryptocurrencies, the reflexive dimensions of these recommendations have been directed by a procedural orientation, which requires an institutional basis for its realisation.

More specifically, the recommendations based on code as an internal self-regulatory mechanism of the cryptocurrency system are targeted at addressing the regulatory challenges posed by the potential for on-chain and online money laundering, terrorist financing and tax evasion. The application of algorithmic regulation, legal programming and regtech will be able to go beyond existing AML and CFT regulations, by deploying algorithms with the technological sophistication and capability to track and trace online cryptocurrency transactions occurring over P2P and DEX. In addition to addressing this regulatory challenge, regulating algorithms, legal programming and regtech, combined with the promotion of competition, will be able to promote consumer and investor protection by reducing information asymmetries and increasing accountability of all cryptocurrency intermediaries, as well as addressing some of the challenges associated with establishing jurisdiction and liability in cryptocurrency transactions. Recommendations based on consensus as an internal self-regulatory mechanism for the cryptocurrency system are additionally geared towards enhanced consumer and investor protection, as the facilitation of discursive participatory democracy in rule formulation, and the development of appropriate institutional infrastructure are both aimed at providing transparency and consistency around how decisions are arrived at within cryptocurrency systems. The link between recommendations and the target regulatory goals is illustrated in Table 2, below.

Table 2: Overview of System Features, Recommendations and Target Regulatory Goal

System Features	**Recommendation**	**Target Regulatory Goal**
Code as internal self-regulatory mechanism of cryptocurrency system	1. Apply regulation of algorithms	On-chain AML/CTF and tax evasion; consumer and investor protection
	2. Support the development of legal programming, regtech and smart contracts	On-Chain AML/CTF and tax evasion; consumer and investor protection
	3. Promote competition	Consumer and investor protection
Consensus as internal self-regulatory mechanism of cryptocurrency system	4. Facilitate discursive participatory democracy in rule formulation	Consumer and investor protection; market integrity
	5. Develop appropriate institutional infrastructure	Consumer and investor protection; market integrity; address jurisdictional limitations

Conclusion

This thesis has presented a reflexive law approach to cryptocurrency regulation, structured against layered responses to six questions, namely:

1) What are cryptocurrencies and why do they need to be regulated?
2) What is the current approach to cryptocurrency regulation?
3) Why is there a need for an alternative approach to cryptocurrencies?
4) What is reflexive regulation?
5) How can reflexive regulation be applied to cryptocurrencies?
6) What are the strategies for reflexively regulating cryptocurrencies?

Key Conclusions

The key conclusions of the discussions around each of these questions shall be discussed in turn.

What are cryptocurrencies and why do they need to be regulated?

Using an evolutionary perspective on the advent of cryptocurrencies, this thesis has shown how cryptocurrencies developed from DC and VC, combined with traditional notions of ledgers, incorporating blockchain and DLT to create a unique means of generating, storing and transmitting value. This description highlighted the use of DLT and blockchain, cryptographic protocols, and P2P networking as the features that make cryptocurrencies novel, distinct and unique. This understanding of the development of cryptocurrency placed the technical components and functionality of cryptocurrencies at the forefront, giving them primacy as the main defining features of cryptocurrency. This understanding of the fundamental role of the underlying technology to the conceptualising of cryptocurrency laid the contextual and conceptual foundation for the thesis.

The need for cryptocurrency regulation was identified, based on the issues of concerns they pose to regulators. These concerns have to do with the potential use of cryptocurrencies for the purposes of cybercrime, money laundering, financing of terrorism and tax evasion, consumer and investor protection, and finally, prudential and systemic risk. This analysis showed that, whilst there are legitimate uses for cryptocurrencies, and there is considerable interest in their innovative potential in the financial sector and beyond, their use in facilitating illegal activities, combined with the risks they pose to consumers and investors warrants their regulation. However, this thesis highlighted how the discussions surrounding cryptocurrency crime are often anecdotal, with available data showing the scale and impact of the use of cryptocurrency to be relatively low, in comparison to illicit activity occurring through conventional channels.

What is the current approach to cryptocurrency regulation?

The thesis provided a holistic overview of current approaches to cryptocurrency regulation in Chapter 2, by considering both international and national responses to their regulation. The international regulatory environment for cryptocurrencies was analysed based on the recommendations, warnings, opinions, and statements of international organisations, whose mandates and purview include and intersect with the issues of regulatory concern raised by cryptocurrencies. Here it was shown that:

a) There is a concerted call for a global approach to the regulation of cryptocurrencies, in line with a recognition of the need for combined supra-jurisdictional oversight, to ensure regulatory effectiveness and the role of these institutions in standards-setting.
b) International organisations predominantly identify cryptocurrency intermediaries (exchange and wallet providers) as the sole regulatory targets, advocating for like-for-like regulation, based on the functions performed by these intermediaries.
c) There is an increasing awareness of the potential use of the technology itself as a regulatory tool and mechanism, as stated by both the IMF and the BIS, and, as observable in the enforcement-oriented initiatives of the TITANIUM project, the UNDOC and Interpol.

Regarding national regulatory approaches to cryptocurrencies, this thesis has shown how these can be broadly categorised into jurisdictions with (a) no regulation, (b) restrictive regulations, (c) neutral regulation, and (d) promotive regulations. With regards to jurisdictions with no regulation, it has been found that these have issued statements providing warnings around the use of cryptocurrencies. Also in this category are jurisdictions that have adopted a wait-and-see approach, in light of the emerging nature of the cryptocurrency industry. The second classification used in this thesis is that of restrictive jurisdictions. This category includes jurisdictions that have issued bans making cryptocurrency use illegal, as well as jurisdictions that have put in place relatively restrictive regulations towards the cryptocurrency market. In the third category of jurisdictions, it has been noted how neutrality in cryptocurrency regulation consists of the application of like-for-like rules and regulations, without distinguishing cryptocurrency financial products, services and institutions from similar products, service and institutions. The final category of national regulatory approaches identified is that of promotive jurisdictions. These are areas where the use of cryptocurrencies is actively encouraged and supported through regulation. Through this analysis, this thesis has provided a summary of the regulated financial products, regulated activities and regulated institutions related to cryptocurrencies.

Why is there a need for an alternative approach to cryptocurrencies?

In Chapter 3, there is an examination and evaluation of both the international and national approaches to the regulation of cryptocurrencies, with a focus on enforcement and compliance challenges, conducted in order to highlight the need for an alternative regulatory response. Here it was shown how current cryptocurrency regulation is faced with enforcement and compliance challenges and limitations. Enforcement challenges have to do with P2P and DEX, pseudonymity, and the challenges of jurisdiction and arbitrage. Compliance challenges relate to financial and non-financial compliance costs, regulatory exclusions and oversights, the uncertainties that arise from multiple legal definitions for cryptocurrency regulation, and the lack of a harmonised global approach. This highlighted the need for an alternative approach to cryptocurrency regulation, punctuated by the ineffectiveness of having no regulation, and the emphasis of the technical roots to the regulatory challenges presented by cryptocurrencies.

The key conclusion here is that current cryptocurrency regulation is unenforceable using substantive legal rules and the traditional tools of financial regulation, due to cryptocurrency's technical features. In addition to presenting challenges to regulation, the technical features of cryptocurrencies also present unique regulatory opportunities currently un- or under-explored by regulators.

What is reflexive regulation?

Following on from highlighting the need for an alternative regulatory response to cryptocurrencies, this thesis presented an overview reflexive of regulation theory in Chapter 4. In this approach,

> *[l]aw realises its own reflexive orientation insofar as it provides the structural premises for reflexive processes in other social subsystems … Thus law must act at the subsystem-specific level to install, correct, and redefine democratic self-regulatory mechanisms. Law's role is to decide about decisions, regulate regulations, and establish structural premises for future decisions in terms of organization, procedure and competences.*[1]

This thesis has placed emphasis on the manner in which a reflexive regulation approach facilitates learning. Here, learning is shown to be a natural by-product of the reflexive process, because, as Teubner asserts, when law serves as an institution that facilitates self-regulatory processes of communication and learning, it plays a role that is 'congruent with emergent forms of discursive rationality', and because of its procedural orientation, is 'well-suited to the legitimation problems of post-modern society'.[2] Embedded in an understanding

[1] G Teubner, 'Substantive and Reflexive Elements in Modern Law (1983) 17 Law & Soc Rev 239.
[2] ibid.

of autopoiesis and facilitated by communication, this learning process is bi-directional, and propels both the regulated and the regulatee to more evolved forms of interaction. Such a line of thought was developed in this thesis, with emphasis being placed on the need and opportunity for self-reflexion within the legal system, developing structures to reinterpret themselves in the light of external needs and demands presented to it by the cryptocurrency system, leading to a 'rematerialisation of the law'[3] into a new form.

How can reflexive regulation be applied to cryptocurrency?

In Chapter 5, this thesis has shown how identifying and understanding the internal self-regulatory mechanisms or the regulatory target system is a pre-requisite to the application of a reflexive regulation approach. With regards to cryptocurrency, this thesis identified and considered computer code, and consensus-based distributive governance mechanisms as the two main internal self-governance mechanisms within cryptocurrency systems, by highlighting their respective cognitive openness and operational closure. Here, the strengths and areas in need of improvement and support within both code and consensus were highlighted. These shortcomings and challenges of code and consensus show that there is a distinct role for the law, where 'law must act at the sub-system-specific level to install, correct, and redefine democratic self-regulatory mechanisms',[4] in order to re-direct these internal self-regulatory mechanisms towards achieving regulatory goals.

What are the strategies for reflexively regulating cryptocurrencies?

Reflexive regulation strategies for cryptocurrencies have been provided in Chapter 6 through recommendations based on the code and consensus-based internal self-governance structures and processes of the cryptocurrency system.

[3] Teubner (n 1) 279.
[4] ibid 275.

Here, the recommendations based on code as an internal self-regulatory mechanism are:

a) Regulate algorithms
b) Support the development of legal programming, regtech and smart contracts
c) Promote competition

Complementing these are recommendations based on consensus as an internal self-regulatory mechanism, which are:

d) Facilitate discursive participatory democracy in rule formulation
e) Develop appropriate institutional infrastructure

The manner in which each of these recommendations target addressing cryptocurrency-specific regulatory challenges are highlighted in this thesis. In addition to evading the regulatory trilemma, the reflexive dimensions of these recommendations are based on their being informed by a procedural orientation, supported by calls for an institutional basis for their realisation. In this way, by taking into account the code and consensus-based internal self-regulatory structures and processes of the cryptocurrency system, this thesis has shown how the limitations of current regulation can be overcome through the redirection of these structures and processes towards regulatory goals. The task of creating a social conscience within the regulatee is essential to enhancing, supporting, and indirectly diverting internal self-regulatory mechanisms towards addressing issues of regulatory concern.

Bibliography

Case Law

Ang v Reliantco Investments Ltd [2019] Queen's Bench Division (Commercial Court) EWHC 879 (Comm).

Eckerle v Wickeder Westfalenstahl GmbH [2013] EWHC 68 (Ch) [2014] Ch 196.

Federal Trade Commission v BF Labs Inc et al 201No 4:14-cv00815- BCW (WD Mo Apr 16).

Hashfast Technologies LLC v Lowe [2016] California North Bankruptcy Court 14-30725-DM (Bankr ND Cal Feb 22, 2016).

R v Assaf and others [2019] EWCA Crim 1057 Court of Appeal, Criminal Division.

Secure Capital SA v Credit Suisse AG EWHC 388 (Comm) 25 Feb 2015.

SEC v Shavers and Bitcoin Savings and Trust No 4: 13 –CV – 416 2014 WL 4652121.

Skatteverket v David Hedqvist (C-264/14) [2015].

State of Florida v Michell Abner Espinoza Criminal Division Case No F14-2923 (Fla 11th Cir Ct 2016).

United States of America v Alexandre Cazes Case No 1:17 CR-00144 2017.

United States of America v Ali Shukri Amin 1:15-cr-65 2015; 5.

United States v BTC-e a/k/a Canton Business Corp and Alexander Vinnik, United States District Court, Northern District of California, San Francisco Division, No 3:19-CV-04281 (ND Cal Jul 25, 2019).

United States v Lebedev, No 17-3691 (2d Cir 2019).

United States v Murgio, No 15-CR-769 (AJN) (SDNY 21 April 2016).

United States of America v Ulbricht 31 F Supp 3d 540-Dist (Court, SD New York, 2014).

Books

Adam N, *Regulating Global Financial Markets* (Economist Intelligence Unit 1992).

Ahrne G, and Brunsson N, *Meta-Organizations*, (Edward Elgar Publishing 2008).

Alexander K, Dhumale R, and Eatwell J, *Global Governance of Financial Systems: The International Regulation of Systemic Risk* (OUP 2006).

Andenas M, and Chiu H, *The Foundations and Future of Financial Regulation: Governance for Responsibility* (Routledge 2014).

Antonopoulos A, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* (O'Reilly Media Inc, 2014).

Appelbaum R, Felstiner W, and Gessner V, *Rules and Networks: The Legal Culture of Global Business Transactions* (Hart 2001).

Ayres I, and Braithwaite J, *Responsive Regulation: Transcending the Deregulation Debate* (OUP 1992) 21.

Baldwin R, Cave M, and Lodge M, (eds.) *The Oxford Handbook of Regulation*. (OUP 2010).

Baldwin R, Cave M, and Lodge M, *Understanding Regulation: Theory, Strategy and Practice.* (OUP 2012).

Benjamin J, Financial Law (OUP 2007).

Black J, *Rules and Regulators* (OUP 1997).

––, Lodge M, and Thatcher M, *Regulatory Innovation a Comparative Analysis* (Edward Elgar Publishing 2005)

Boyle J, *Shamans, Software and Spleens. Law and the Construction of the Information Society* (Harvard UP 1996).

Braithwaite J, *Regulatory Capitalism: How it Works, Ideas for Making it Work Better* (Edward Elgar 2008).

Bratton W, McCahery J, Picciotto S, and Scott S, (eds) *International Regulatory Competition and Coordination* (Clarendon Press 1996).

Brütsch C, and Lehmkuhl D, (eds) *Law and Legalization in Transnational Relations* (Routledge 2007).

Busch A, *Banking Regulation and Globalization* (OUP 2009).

Brownsword R, Scotford E, Yeung K, (eds.) *The Oxford Handbook of Law, Regulation and Technology* (OUP 2017).

Bronwen M, and Yeung K, *An Introduction to Law and Regulation: Text and Materials* (CUP 2007).

Carmichael J, Flemming A, and Llewellyn D, (eds), *Aligning Financial Supervisory Structures with Country Needs* (World Bank Institute 2004).

Castells M, *The Rise of the Network Society* (Blackwell Publishers 1996).

Chui H, *Regulating (From) The Inside: The Legal Framework for Internal Control in Banks and Financial Institutions* (Hart Publishing 2015).

Dale R, *Risk and Regulation in Global Securities Markets* (John Wiley 1996).

Davies H, and Green D, *Global Financial Regulation* (Polity Press 2008).

Delimatsis P, (ed), *The Law, Economics and Politics of International Standardisation* (CUP 2015).

Epstein D, and O'Halloran S, *Delegating Powers: A Transaction Cost Politics Approach to Policy Making under Separate Powers* (CUP 1999).

Faulhaber G, Madden G, and Petchey J, *The Regulation and Performance of Communication and Information Networks* (Edward Elgar 2012).

Feest J, and Nelken D, (eds), *Adapting Legal Cultures* (Hart 2001).

Ferran E, and others, *The Regulatory Aftermath of the Global Financial Crisis* (CUP 2012).

Finck M, *Blockchain Regulation and Governance in Europe* (CUP 2019).

Golumbia D, *The Politics of Bitcoin: Software as Right-Wing Extremism* (U of Minnesota Press 2016).

Goodhart C and others, *Financial Regulation: Why, How and Where Now?* (Routledge 1998).

Gorton G, *Slapped by the Invisible Hand: Banking and the Panic of 2007* (OUP 2010).

Gray J, and Hamilton J, *Implementing Financial Regulation: Theory and Practice* (Wiley 2006).

Gray J, and Akseli O, *Financial Regulation in Crisis? The Role of Law and the Failure of Northern Rock* (Edward Elgar 2011).

Gunningham N, and Grabovsky P, *Smart Regulation: Designing Environmental Policy* (Clarendon Press 1998).

Habermas J, *Theory and Practice* J Viertel (tr), (Heineman 1974).

––, *The Theory of Communicative Action* (Beacon Press 1984).

Hawkins K, and Thomas J, *Enforcing Regulation* (Boston, Kluwer Nijhoff 1984).

Herring R, and Litan R, *Financial Regulation in a Global Economy* (Brookings Institution 1994).

Herian R, *Regulating Blockchain: Critical Perspectives in Law and Technology* (Routledge 2018).

Jeunemaître, A (ed) *Financial Markets Regulation: A Practitioner's Perspective (*Macmillan 1997).

Joerges C, and Falke J, *Karl Polanyi, Globalisation and Potential of Law in Transnational Markets* (Hart 2011).

Johnston D, (ed) *Towards World Constitutionalism: Issues in the Legal Ordering of the World Community* (M. Nijhoff Publishers 2014).

Kindleberger C, *Manias, Panics, and Crashes: A History of Financial Crises* (John Wiley & Sons 2005).

Lacovino L, *Recordkeeping, Ethics and Law: Regulatory Models, Participant Relationships and Rights and Responsibilities in the Online World* (Springer 2006).

Lee R, *What is an Exchange? The Automation, Management, and Regulation of Financial Markets* (OUP 1998).

Lessig L, *Code 2.0* (2nd edn, Basic Books 2006).

Luhmann N, *A Sociological Theory of Law* (Routledge and Kegan Paul 1985).

Macdonald R, and Johnston D, *Towards World Constitutionalism: Issues in the Legal Ordering of the World Community* (M Nijhoff Publishers 2004).

Mayes D, and Wood G, *The Structure of Financial Regulation* (Routledge 2007).

Mason P, *Meltdown: The End of the Age of Greed* (Verso 2010).

Morgan B, and Yeung K, *An Introduction to Law and Regulation* (CUP 2017).

Muir Watt H, and Fernandez Arroyo D, (eds), *Private International Law and Global Governance* (OUP 2014).

Mullan P, *The Digital Currency Challenge: Shaping Online Payment Systems through US Financial Regulations* (Palgrave Macmillan 2014).

Ogus A, *Regulation: Legal Form and Economic Theory* (Hart Publishing).

Pauwelyn J, Wessel R, and Wouters J, (eds), *Informal International Lawmaking* (OUP 2012).

Picciotto S, *Regulating Global Corporate Capitalism*, *International Corporate Law and Financial Market* (CUP 2011).

Popper N, *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money* (Harper 2015).

Quade E, *Analysis of Public Decisions* (3rd edn, Prentice Hall 1989).

Reinhart C, and Rogoff K, *This Time is Different: Eight Centuries of Financial Folly* (Princeton UP 2009).

Rhodes R, (ed.) *Understanding Governance: Policy Networks, Governance, Reflexivity, Accountability* (Open UP 1997).

Rogowski R, *Reflexive Labour Law in the World Society* (Edward Elgar 2013).

Santos B, *Toward a New Common Sense*: *Law, Science and Politics in the Paradigmatic Transition* (Routledge 1995).

Schooner H, *Bank Regulation: Principles and Policies* (Academic Press 2010).

Scott H, *International Finance: Law and Regulation* (Sweet & Maxwell 2009).

Shelton D, (ed) *Commitment and Compliance: The Role of Non-Binding Norms in the International Legal System* (OUP 2000).

Singh D, *Banking Regulation of UK and US Financial Markets* (Ashgate Publishing 2007).

Slaughter A, *A New World Order* (Princeton UP 2004).

Slager A, *'Banking Across Borders'* (Erasmus Research Institute for Management 2004).

Teubner G, (ed), *Juridification of Social Spheres: A Comparative Analysis of the Areas of Labor, Corporate, Antitrust and Social Welfare Law* (W de Gruyter 1987).

––, (ed), *Autopoietic Law: A New Approach to Law and Society* (W de Gruyter 1987).

––, (ed), *Global Law without a State* (Dartmouth 1997).

––, *Constitutional Fragments: Societal Constitutionalism and Globalization* (OUP 2012) .

Tushnet T, and Cane P, (eds), *The Oxford Handbook of Legal Studies* (OUP 2005).

Ugeux G, *International Financial Regulation: The Quest for Financial Stability* (Wiley 2014).

Watkins D, and Burton M, (eds), *Research Methods in Law* (Routledge 2013).

Wilson J, *The Politics of Regulation* (Basic Books 1980).

Wood P, *Law and Practice of International Finance* (Sweet & Maxwell 2008).

Book Chapters

Arthurs H, 'The Reconstitution of the Public Domain' in Drache D, (ed), *The Market or the Public Domain? Global Governance and the Asymmetry of Power* (Routledge 2001).

Bhaskar N, and Lee D, 'Bitcoin Exchanges' in D Lee, and C Kuo (eds), *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data* (Elsevier 2015).

Black J, 'Regulatory Styles and Supervisory Strategies' in N Moloney, E Ferran, and J Payne (eds), *Oxford Handbook of Financial Regulation* (OUP 2015).

Cave J, 'Policy and Regulatory Requirements for a Future Internet' in I Brown (ed), *Research Handbook on Governance of the Internet* (Edward Elgar 2013).

De Schutter O, and Lenoble J, 'Introduction: Institutions Equipped to Learn' in O De Schutter, and J Lenoble (eds), *Redefining the Public Interest in a Pluralistic World* (Hart Publishing 2010).

Deakin S, 'The Evolution of Theory and Method in Law and Finance' in N Moloney, E Ferran, and J Payne, (eds), *Oxford Handbook of Financial Regulation* (OUP 2015).

Gunningham N, 'Regulatory Reform and Reflexive Regulation: Beyond Command and Control' in E Brousseau, T Dedeurwaerdere, and B Siebenhner (eds), *Reflexive Governance and Global Public Goods* (MIT Press 2009).

Habermas J, 'Three Normative Models of Democracy' in S Benhabib (ed), *Democracy and Difference: Contesting the Boundaries of the Political* (Princeton UP 1996).

Luhmann N, 'The Autopoiesis of Social Systems' in F Geyer and J Van d Zeuwen (eds), *Sociocybernetic Paradoxes: Observation, Control and Evolution of Self-Steering Systems* (Sage 1986).

Luhmann N, 'The World Society as a Social System' in N Luhmann, *Essays on Self-Reference* (CUP 1990).

Moloney N, Ferran E, and Payne J, 'Introduction' in N Moloney, E Ferran, and J Payne (eds), *Oxford Handbook of Financial Regulation* (OUP 2015).

Parker C, and Braithwaite J, 'Regulation' in M Tushnet and P Cane (eds), *Oxford Handbook of Legal Studies* (OUP 2005).

Patwardhan A, 'Financial Inclusion in the Digital Age' in D Chuen and R Deng (eds), *Handbook of Blockchain, Digital Finance, and Inclusion* (Elsevier 2017).

Schoenmaker D, and Oosterloo S, ‘Cross-Border Issues in European Financial Supervision’ in D Mayes, and G Wood, (eds), *The Structure of Financial Regulation* (Routledge 2007).

Scott C, ‘Reflexive Governance, Regulation and Meta-Regulation: Control or Learning?’ in O De Schutter, and J Lenoble, (eds), *Reflexive Governance: Redefining the Public Interest in a Pluralistic World* (Hart 2010).

Stiglitz J, ‘Regulation and Failure’ in D Moss, and J Cisternino, (eds), *New Perspectives on Regulation* (The Tobin Project 2009).

Teubner G, ‘Juridification: Concepts, Aspects, Limits, Solutions’ in G Teubner, (ed), *Juridification of Social Spheres: A Comparative Analysis of the Areas of Labour, Corporate, Antitrust and Social Welfare Law* (W de Gruyter 1987).

Walch A, ‘In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchain’ in P Hacker, and others (eds), *Regulating Blockchain: Techno-Social and Legal Challenges* (OUP 2019).

Official Publications

Ali R, Barrdear J, Clews R, and Southgate J, ‘Innovations in Payment Technologies and the Emergence of Digital Currencies’ (*Bank of England* 2014) <http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3digitalcurrenciesbitcoin1.pdf> Accessed 20 June 2018.

Australian Transaction and Analysis Centre (AUSTRAC), ‘Draft AML.CTF Rules’ (*AUSTRAC* 2 July 2018) <http://www.austrac.gov.au/draft-aml-ctf-rules> Accessed 6 July 2018.

Autorité des Marchés Financiers (AMF), ‘The AMF Considers that the Offer of Cryptocurrency Derivatives Requires Authorization and that it is Prohibited to Advertise such Offer via Electronic Means’ (*AMF* 22 February 2018) <https://www.amf-france.org/en_US/Actualites/Communiques-de-presse/AMF/annee-2018?docId=workspace://SpacesStore/a225bf1d-de35-4f58-89e3-f03cb7e9e551> Accessed 6 August 2018.

BaFin, ‘Initial Coin Offerings: High Risk for Consumers’ (*BaFin* 15 November 2017) <https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2017/fa_bj_1711_ICO_en.html;jsessionid=F880FC5388DF54C0EE1A65D0AC63407A.1_cid290> Accessed 2 December 2019.

Banco Central do Brasil (BACEN), ‘Virtual Currencies’ (*BACEN* Communiqué 31, 379 16 November 2017) <http://www.bcb.gov.br/ingles/norms/> Accessed 6 July 2018.

Bank for International Settlements, ‘About BIS’ (*Bank for International Settlements* 2018) <https://www.bis.org/about/index.htm?m=1%7C1> Accessed 3 July 2018.
––, ‘CPMI—Overview’ (*Bank for International Settlements* 2018) <https://www.bis.org/cpmi/about/overview.htm?m=3%7C16%7C691> Accessed 6 August 2018.

Bank of England, ‘Digital Currencies’ (*Bank of England* 22 August 2018) <https://www.bankofengland.co.uk/research/digital-currencies> Accessed 11 November 2018.

––, ‘What Are Cryptoassets (Cryptocurrencies)?’ (Bank of England 2019) <https://www.bankofengland.co.uk/knowledgebank/what-are-cryptocurrencies> Accessed 2 December 2019.

––, ‘Central Bank Group To Assess Potential Cases For Central Bank Digital Currencies’ (*Bank of England* News Release 21 January 2020)<https://www.bankofengland.co.uk/media/boe/files/news/2020/january/central-bank-group-to-assess-potential-cases-for-central-bank-digital-currencies.pdf?la=en&hash=F0F25B3FC0CB1F7A64B08797C3D124C171C0BF27> Accessed 15 January 2020.

Basel Committee on Banking Supervision, ‘Sound Practices: Implications of Fintech Developments for Banks and Bank Supervisors’ (*Bank of International Settlements* February 2018*)* < https://www.bis.org/bcbs/publ/d431.pdf> Accessed 3 December 2019.

––, ‘Sound Practices: Implications of Fintech Developments for Banks and Bank Supervisors’ (Bank of International Settlements August 2017) <https://www.bis.org/bcbs/publ/d415.pdf> Accessed 3 July 2018.

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 3 July 2018.

Carstens A, ‘Money in the Digital Age: What Role for Central Banks?’ (*Bank of International Settlements* 6 February 2018) <https://www.bis.org/speeches/sp180206.pdf> Accessed 2 December 2019.

Committee on Payments and Market Infrastructures (CPMI) ‘Digital Currencies’ (*Bank for International Settlements* November 2015) <https://www.bis.org/cpmi/publ/d137.pdf> Accessed 6 August 2018.

Council of the European Union, ‘Council Conclusions on the Fight Against the Financing of Terrorism’ (Press Release 50/16 2016) <http://www.consilium.europa.eu/en/press/press-releases/2016/02/12-conclusions-terrorism-financing/> Accessed 19 August 2016.

ESMA, ‘ESAs Warn Consumers of Risks in Buying Virtual Currencies’ (*ESMA* 12 February 2018) <https://www.esma.europa.eu/press-news/esma-news/esas-warn-consumers-risks-in-buying-virtual-currencies> Accessed 3 July 2018.

––, ‘Additional Information on the Agreed Product Intervention Measures Relating to Contracts for Differences and Binary Options’ (*ESMA* 27 March 2018) <https://www.esma.europa.eu/sites/default/files/library/esma35-43 1000_additional_information_on_the_agreed_product_intervention_measures_relating_to_contracts_for_differences_and_binary_options.pdf> Accessed 3 July 2018.

European Banking Authority ‘Opinion on ‘Virtual Currencies’ (*EBA* 2014) <http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf> Accessed 2 December 2019.

––, ‘Opinion of the European Banking Authority on the EU Commission’s proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849 (4AMLD)’ (*EBA* 11 August 2016) <https://www.eba.europa.eu/documents/10180/1547217/EBA+Opinion+on+the+Commission%E2%80%99s+proposal+to+bring+virtual+currency+entities+into+the+scope+of+4AMLD> Accessed 3 July 2018.

European Central Bank, ‘Virtual Currency Schemes’ (*ECB* 2012) <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> Accessed 7 June 2016.

European Commission, ‘Competition’ (*European Commission* 2014) <http://ec.europa.eu/competition/antitrust/overview_en.html> Accessed 1 June 2018.

––, ‘Communication from the Commission to the European Parliament and the Council on an Action Plan to for Strengthening the Fight against Terrorism Financing’ (*European Commission* COM 50/2 2016) <http://ec.europa.eu/justice/criminal/files/com_2016_50_en.pdf> Accessed 7 June 2016.

––, ‘Project to Prevent Criminal Use of the Dark Web and Virtual Currencies launched by International Consortium’ (*European Commission* 1 June 2017) <https://cordis.europa.eu/news/rcn/141335_en.html> Accessed 3 July 2018.

FATF, ‘Guidance for a Risk-Based Approach: Virtual Currencies’ (FATF June 2015) <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf> Accessed 7 June 2016.

––, ‘Who We Are’ (FATF 2018) <http://www.fatf-gafi.org/about/> Accessed 2 July 2018.

––, ‘FATF Report to the G20 Finance Ministers and Central Bank Governors’ (*FATF* March 2018) <http://www.fatf-gafi.org/media/fatf/documents/FATF-G20-FM-CBG-March-2018.pdf> Accessed 19 June 2018.

––, ‘Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers’ (*FATF* 2019) <www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html> Accessed 2 December 2019.

Federal Election Commission, ‘Political Committee May Accept Bitcoin as Contribution’ (*FEC* Advisory Opinion 2014-02 2014) <http://saos.fec.gov/aodocs/2014-02.pdf> Accessed 6 June 2016.

Financial Conduct Authority, ‘Initial Coin Offerings’ (*Financial Conduct Authority* 12 September 2017) <https://www.fca.org.uk/news/statements/initial-coin-offerings> Accessed 6 July 2017.

––, ‘Regulatory Sandbox Lessons Learnt Report’ (*Financial Conduct Authority* 2017) <https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf> Accessed 14 May 2018.

––, ‘Data Reporting Service Providers’ (*Financial Conduct Authority* 13 January 2017) <https://www.fca.org.uk/markets/data-reporting-services-providers-drsps> Accessed 2 June 2018.

––, ‘Innovation Hub’ (*Financial Conduct Authority* 2018) <https://innovate.fca.org.uk/innovation-hub/objectives-innovation-hub> Accessed 6 July 2018.

––, ‘Algorithmic Trading Compliance in Wholesale Markets’ (*Financial Conduct Authority* February 2018)<https://www.fca.org.uk/publication/multi-firm-reviews/algorithmic-trading-compliance-wholesale-markets.pdf> Accessed 1 June 2018.

––, 'Cryptoassets: Our Work' (*Financial Conduct Authority* 23 January 2019) <https://www.fca.org.uk/firms/cryptoassets> Accessed 3 December 2019.

Financial Consumer Agency of Canada, 'Digital Currency' (*Financial Consumer Agency of Canada* 19 January 2018) <https://www.canada.ca/en/financial-consumeragency/services/payment/digital-currency.html> Accessed 6 July 2018.

Financial Policy Committee, 'Financial Policy Committee statement from its meeting - 12 March 2018' (*Bank of England* 16 March 2018) <https://www.bankofengland.co.uk/statement/fpc/2018/financial-policy-committee-statement-march-2018> Accessed 2 December 2019.

Financial Transactions Reports and Analysis Centre of Canada, 'FINTRAC Advisory Regarding Money Services Businesses Dealing in Virtual Currency (*FINTRAC* July 2014) <http://www.canafe-fintrac.gc.ca/new-neuf/avs/2014-07-30-eng.asp> Accessed 7 June 2016.

FinCEN, 'Guidance: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies' (*FinCEN* 2013) <https://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html> Accessed 23 August 2016.

––, 'FinCEN Fines Ripple Labs Inc in First Civil Enforcement Action against a Virtual Currency Exchange (*FinCEN* 5 May 2015) <https://www.fincen.gov/news_room/nr/html/20150505.html> Accessed 7 June 2016.

Fournier O, and Lennard J, 'Rebooting Money: The Canadian Tax Treatment of Bitcoin and Other Cryptocurrencies' Canadian Tax Foundation (2014) Conference Report, 11.

FSA, A New Regulator for a New Millennium (2000) <https://www.fca.org.uk/old-fsa-website> Accessed 3 May 2015.

––, Principles-based Regulation: Focusing on the Outcomes that Matter (2007) <https://www.fca.org.uk/old-fsa-website> Accessed 3 May 2015.

G20, 'Communiqué of the First G20 Meeting of Finance Ministers and Central Bank Governors of 2018' (*G20* 20 March 2018) <https://back-g20.argentina.gob.ar/sites/default/files/media/communique_g20.pdf> Accessed 19 June 2018.

Greenspan A, Testimony before the House Committee on Oversight and Government Reform, 'The Financial Crisis and the role of Federal Regulators' (*US Government Printing Office* 2008) <https://www.govinfo.gov/content/pkg/CHRG-110hhrg55764/pdf/CHRG-110hhrg55764.pdf> Accessed 19 June 2018.

He D, 'Monetary Policy in the Digital Age' (2018) Finance and Development Vol 55.2 <http://www.imf.org/external/pubs/ft/fandd/2018/06/central-bank-monetary-policy-and-cryptocurrencies/he.pdf> Accessed 3 July 2018.

––, and others, 'Virtual Currencies and Beyond, Initial Considerations' (*IMF Staff Discussion Note* 2016) <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf> Accessed 18 June 2018.

HM Government, National Cybersecurity Strategy 2016 to 2021 (*HM Government Policy Paper* 1 November 2016) <https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021> Accessed 2 December 2019.

HM Treasury, 'Cryptoassets Taskforce: Final Report' (*HM Treasury Policy Paper* 30 July 2018) <https://www.gov.uk/government/publications/cryptoassets-taskforce> Accessed15 January 2020.

HMRC, 'Cryptoassets Tax for Individuals' (*HMRC Policy Paper* 1 November 2019) <https://www.gov.uk/government/publications/tax-on-cryptoassets/cryptoassets-for-individuals> Accessed 2 December 2019.

House of Commons Treasury Committee, 'Crypto-assets: Twenty-Second Report of Session 2017-19' (*House of Commons* 2018) <https://publications.parliament.uk/pa/cm201719/cmselect/cmtreasy/910/910.pdf> Accessed 19 February 2019.

Internal Revenue Service, 'Internal Revenue Bulletin: 2014-16' (*IRS* 14 April 2014) <https://www.irs.gov/irb/2014-16_IRB#NOT-2014-21> Accessed 6 July 2018.

International Monetary Fund, 'About' *(IMF* 2018) <https://www.imf.org/en/About> Accessed 19 June 2018.

––, 'Virtual Currencies and Beyond: Initial Considerations' (*IMF Staff Discussion Note* 3 2016) <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf> Accessed 20 June 2018.

Interpol, 'Interpol Holds First DarkNet and Cryptocurrencies Working Group' (*Interpol* 3 April 2018) <https://www.interpol.int/News-and-media/News/2018/N2018-022> Accessed 3 July 2018.

IOSCO, 'Securities Markets Risk Outlook' (*IOSCO* 2016) <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD527.pdf> Accessed 19 June 2018.

––, 'About IOSCO' (*IOSCO* 2018) <https://www.iosco.org/about/?subsection=about_iosco> Accessed 19 June 2018.

––, 'IOSCO Board Communication on Concerns Related to Initial Coin Offerings (ICOs) (*IOSCO*/MR/01/2018 18 January 2018) <http://www.iosco.org/news/pdf/IOSCONEWS485.pdf> Accessed 2 December 2019.

––, 'IOSCO Annual Conference Focuses on Key Challenges Facing Securities Regulators' (*IOSCO*/MR/13/2018 10 May 2018) <https://www.iosco.org/news/pdf/IOSCONEWS497.pdf> Accessed 19 June 2018.

Lagarde C, 'Addressing the Dark Side of the Cryptoworld' (*IMF Blog*, 13 March 2018) <https://blogs.imf.org/2018/03/13/addressing-the-dark-side-of-the-crypto-world/> Accessed 3 July 2018.

––, 'An Even-Handed Approach to Cryptoassets' (*IMF Blog*, 16 April 2018) <https://blogs.imf.org/2018/04/16/an-even-handed-approach-to-crypto-assets/> Accessed 3 July 2018.

––, 'Winds of Change: The Case for New Digital Currency' (*IMF* 13 November 2018) Singapore Fintech Festival Speech <https://www.imf.org/en/News/Articles/2018/11/13/sp111418-winds-of-change-the-case-for-new-digital-currency> Accessed 14 January 2020.

Lautenschläger S, 'Is Small Beautiful? Supervision, Regulation and the Size of Banks' (Speech at IMF seminar, Washington DC, 14 October 2017) <https://www.ecb.europa.eu/press/key/date/2017/html/ecb.sp171014.en.html> Accessed 3 December 2019.

Lehdonvirta V and Ali R, 'Governance and Regulation' in M Walport, 'Distributed Ledger Technology: Beyond Blockchain' in Report by Sir Mark Walport, UK Government Chief Scientific Adviser (*Government Office for Science* 2016) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf> Accessed 20 May 2016.

Malta Financial Services Authority (MFSA), 'Discussion Paper on Initial Coin Offerings, Virtual Currencies and Related Service Providers' (*MFSA* 11 January 2018) <https://www.mfsa.com.mt/pages/readfile.aspx?f=/files/Announcements/.../2017/> Accessed 11 November 2018.

Medcraft G, 'The OECD and the Blockchain Revolution' (*OECD* Presentation at the OECD Friends of Going Digital Meeting, Paris 29 March 2018) <http://www.oecd.org/parliamentarians/meetings/meeting-on-the-road-london-april-2018/The-OECD-and-the-Blockchain-Revolution-Presentation-by-Greg-Medcraft-delivered-on-29-March-2018.pdf> Accessed 30 June 2018.

New York Department of Financial Services (*NYDFS* 2015) 'BitLicense Regulatory Framework' <https://dfs.ny.gov/legal/regulations/bitlicense_reg_framework.htm> Accessed 2 December 2019,

OECD, 'OECD Secretary General Report to G20 Financial Ministers and Central Bank Governors' (*OECD* March 2018) <https://www.oecd.org/tax/OECD-Secretary-General-tax-report-G20-Finance-Ministers-Argentina-March-2018.pdf> Accessed 2 July 2018.

––, 'Blockchain Technology and Competition Policy' (*OECD* 8 June 2018) <https://one.oecd.org/document/DAF/COMP/WD (2018)47/en/pdf> Accessed 28 May 2018.

––, 'Our Mission' (*OECD* 2018) <http://www.oecd.org/about/> Accessed 19 June 2018.

Parliamentary Office of Science and Technology, 'Alternative Currencies' (*POSTnote* Number 475 August 2014) <http://researchbriefings.files.parliament.uk/documents/POST-PN-475/POST-PN-475.pdf> Accessed 7 June 2016.

Reserve Bank of Australia (RBA), 'Submission to the Enquiry into Digital Currency' (*Reserve Bank of Australia* September 2014) <https://www.rba.gov.au/publications/submissions/financial-sector/pdf/inquiry-digital-currency-2014-11.pdf> Accessed 6 July 2018.

Securities and Exchange Commission, 'SEC Charges Bitcoin Entrepreneur with Offering Unregistered Securities' (*SEC* 3 June 2014) <https://www.sec.gov/news/press-release/2014-111#.U49HUPldV8G> Accessed 6 July 2018.

––, 'SEC Sanctions Operator of Bitcoin-Related Stock Exchange for Registration Violations' (*SEC* 8 December 2014) <https://www.sec.gov/news/press-release/2014-273> Accessed 6 July 2018.

South African Revenue Service (SARS), 'SARS' Stance on the Tax Treatment of Cryptocurrencies' (*South African Revenue Service* 6 April 2018) <http://www.sars.gov.za/Media/MediaReleases/Pages/6-April-2018---SARS-stance-on-the-tax-treatment-of-cryptocurrencies-.aspx> Accessed 6 July 2018.

State Bank of Pakistan, 'Prohibition of Dealing in Virtual Currency/Tokens' (*State Bank of Pakistan* BPRD Circular No 03 of 2018 6 April 2018 <http://www.sbp.org.pk/bprd/2018/C3.htm> Accessed 17 July 2018.

UNDOC, 'UNDOC Delivers the First Cryptocurrency Investigation Training Course in Latin America' (*UNDOC* 19 January 2018) <https://www.undoc.org/unodc/en/drug-trafficking/crimjust/news/unodc-delivers-the-first-cryptocurrency-investigation-training-course-in-latin-america.html> Accessed 3 July 2018.

Velde F, 'Bitcoin: A Primer' (*Chicago Fed Letter* No 317 2013) <https://www.chicagofed.org/publications/chicago-fed-letter/2013/december-317> Accessed 2 December 2019.

Walport M, 'Distributed Ledger Technology: Beyond Blockchain' (*Government Office for Science* 2016) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf> Accessed 20 June 2018.

World Bank, 'Blockchain and Distributed Ledger Technology' (*World Bank* 2018) <https://www.worldbank.org/en/topic/financialsector/brief/blockchain-dlt> Accessed 20 June 2018.

Journal Articles

Bain M, and Subirana B, 'E-Commerce Oriented Software Agents' (2004) 20 CLSR 1.

Baldwin R, and Black J, 'Really Responsive Regulation' [2008] 71(1) MLR 59–94.

Black J, 'Proceduralizing Regulation: Part 1' [2000] 20 OJLS 597.

––, 'Enrolling Actors in Regulatory Systems: Examples from UK Financial Services' [2003] PL 63.

––, 'Tensions in the Regulatory State' [2007] PL 58.

––, 'Paradoxes and Failures: 'New Governance' Techniques and the Financial Crisis' [2012] 75(6) MLR 1037.

Boring N, 'France' in 'Regulation of Cryptocurrencies in Selected Jurisdictions' (*The Law Library of Congress* June 2018) <http://www.loc.gov/law/help/cryptocurrency/regulation-of-cryptocurrency.pdf> Accessed 6 July 2018.

Buchanan K, 'Australia' in 'Regulation of Cryptocurrencies in Selected Jurisdictions' (*The Law Library of Congress* June 2018) <http://www.loc.gov/law/help/cryptocurrency/regulation-of-cryptocurrency.pdf> Accessed 6 July 2018.

Burge M, 'Apple Pay, Bitcoin and Consumers: The ABC's of Future Public Payments Law' [2016] Hastings Law Journal 67(5).

Chiu H, 'Pathways to European Policy and Regulation in the Crypto-Economy' [2019] European Journal of Risk Regulation 10.

Coase R, 'The Problem of Social Cost' [1960] Journal of Law and Economics 3.

De Filippi P, 'Bitcoin: A Regulatory Nightmare to a Libertarian Dream' [2014] Internet Policy Review 3 (20).

Dow S, 'Central Banking in the Twenty-First Century' [2017] Cambridge Journal of Economics 41.

Georgieva Z, 'Competition Soft Law in French and German Courts: A Challenge for Online Sales Bans Only?' [2017] Maastricht Journal of European and Comparative Law 24.

––, 'The Judicial Reception of Competition Soft Law in the Netherlands and the UK' [2015] European Competition Journal 12.

Gray J, 'Is it Time to Highlight the Limits of Risk-Based Financial Regulation?' [2009] Capital Markets Law Journal 4(1).

Grimmelmann J, ‘Regulation by Software’ [2004] Yale L J 114.

Hughes S, and Middlebrook S, ‘Advancing a Framework for Regulating Cryptocurrency Payments Intermediaries’ [2015] Yale J on Reg 32.

Isajanyan N, ‘Belarus’ in ‘Regulation of Cryptocurrencies in Selected Jurisdictions’ (*The Law Library of Congress* June 2018) <http://www.loc.gov/law/help/cryptocurrency/regulation-of-cryptocurrency.pdf> Accessed 6 July 2018.

Kiviat T, ‘Beyond Bitcoin: Issues in Regulating Blockchain Transactions’ (2015) 65 Duke Law Journal 570, 577.

Koch K, ‘A Multidisciplinary Comparison of Rules-Driven Writing: Similarities in Legal Writing, Biology Research Articles, and Computer Programming’ [2005] J Legal Educ 55.

Library of Congress, ‘Regulation of Cryptocurrency around the World’ (*Library of Congress* 2019) <https://www.loc.gov/law/help/cryptocurrency/world-survey.php> Accessed 8 November 2019.

McBarnet D, and Whelan C, ‘The Elusive Spirit of the Law: Formalism and the Struggle for Legal Control’ [1991] MLR 54.

Moore T, and Christin N, ‘Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk’ International Conference on Financial Cryptography and Data Security (Berlin Heidelberg 2016).

Ohm P, and Reid B, ‘Regulating Software When Everything Has Software’ [2006] Geo Wash L Rev 84.

Ortolani P, ‘Self-Enforcing Online Dispute Resolution: Lessons from Bitcoin’ [2016] OJLS 36.

Rawlings P, Georgosouli A, and Russo C, ‘Regulation of Financial Services: Aims and Methods’ (Queen Mary University of London, Centre for Commercial Law Studies 2014).

Roderiquez-Ferrand G, ‘Argentina’ in ‘Regulation of Cryptocurrencies in Selected Jurisdictions’ (*The Law Library of Congress* June 2018) <http://www.loc.gov/law/help/cryptocurrency/regulation-of-cryptocurrency.pdf> Accessed 6 July 2018.

Stigler G, ‘The Theory of Economic Regulation’ [1971] Bell Journal of Economics and Management Science 2.

Terry L, ‘Combating Threat to the International Financial System’ [2014] NYL Sch L Rev 59.

Teubner G, ‘Substantive and Reflexive Elements in Modern Law [1983] Law & Soc Rev 17.

––, ‘Regulatory Law: Chronicle of Death Foretold’ [1992] Social and Legal Studies 1.

Tunney J, ‘Notes on the Reflexive Role of Cyberspace’ [2000] International Review of Law Computers and Technology 14(2).

Tziakouris G, ‘Cryptocurrencies—A Forensic Challenge or Opportunity for Law Enforcement? An Interpol Perspective’ [2018] IEEE Security and Privacy 13(4).

Wagner P, ‘On Software Regulation’ [2004] S Cal L Rev 78.

Walch A, ‘The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk’ [2015] NYU Journal of Legislation and Public Policy 18 (4).

Wu T, ‘When Code Isn’t Law’ [2003] Va L Rev 89.

Yeung K, ‘Regulation by Blockchain: The Emerging Battle for Supremacy between the Code *of* Law and Code *as* Law [2019] MLR 82.

--, ‘ 'Algorithmic Regulation: A Critical Interrogation' [2018] Regulation & Governance 4.

Zhang L, ‘China’ in ‘Regulation of Cryptocurrencies in Selected Jurisdictions’ (*The Law Library of Congress* June 2018) <http://www.loc.gov/law/help/cryptocurrency/regulation-of-cryptocurrency.pdf> Accessed 6 July 2018.

Internet Sources

Adriano A, and Monroe H, 'The Internet of Trust' (2016) 53 (2) IMF Finance and Development <https://www.imf.org/external/pubs/ft/fandd/2016/06/adriano.htm> Accessed 2 December 2019.

Agrawal H, '7 Best Bitcoin Payment Gateways for Merchant Account & Services' (*Coinsutra* 15 November 2019) <https://coinsutra.com/bitcoin-payment-gateways-merchants/> Accessed 2 December 2019.

Alexandre A, 'CryptoUK Trade Association Calls on MPs to Regulate Cryptocurrency Sector in UK' (*Cointelegraph* 2 May 2018) <https://cointelegraph.com/news/cryptouk-trade-association-calls-on-mps-to-regulate-cryptocurrency-sector-in-uk> Accessed 16 January 2019.

Alkhalisi Z, 'IMF Chief: Cryptocurrency Regulation is Inevitable' (*CNNMoney* 11 February 2018) <http://money.cnn.com/2018/02/11/investing/lagarde-bitcoin-regulation/index.html> Accessed 20 June 2016.

Allison I, 'Bitcoin Graduate Circle Launches Free Social Payment App in UK with Barclays', (*International Business Times* 6 April 2016) <http://www.ibtimes.co.uk/bitcoin-graduate-circle-launches-free-social-payment-app-uk-barclays-1553353> Accessed 2 December 2019.

––, 'Ethereum Reinvents Companies with Launch of the DAO' (*International Business Times* 30 April 2016) <http://www.ibtimes.co.uk/ethereum-reinvents-companies-launch-dao-1557576> Accessed 15 May 2017.

––, 'Ethereum's Vitalik Buterin' (*International Business Times* 8 July 2016) <http://www.ibtimes.co.uk/ethereums-vitalik-buterin-democratic-hard-fork-proves-mining-oligopoly-cannot-engage-censorship-1569079> Accessed 15 May 2017.

Auer R, and Claessens S, 'Regulating Cryptocurrencies: Assessing Market Reactions' (*BIS Quarterly Review* 23 September 2018), <https://www.bis.org/publ/qtrpdf/r_qt1809f.htm> Accessed 19 February 2019.

Ayton N, 'Bitcoin Community Cracking Down on Money Laundering and Fraud' (*Innovation Enterprises.com* 28 November 2016) <https://channels.theinnovationenterprise.com/articles/Bitcoin-community-cracking-down-on-money-laundering-and-fraud> Accessed 25 July 2017.

Back A, 'Hashback—A Denial of Service Counter-Measure' (*Hashcash* 2002) <http://www.hashcash.org/hashcash.pdf> Accessed 20 June 2018.

Bajpai P, 'Countries Where Bitcoin is Legal and Illegal' (*Investopedia* 11 October 2018) <https://ww.investopedia.com/articles/forex/041515/countries-where-bitcoin-legal-illegal.asp> Accessed 18 October 2018.

Batabyal A, ‘10 Best Privacy Coins in 2019’ (*Coinswitch* 7 June 2019) <https://coinswitch.co/news/10-best-privacy-coins-in-2019-latest-review> Accessed 8 November 2019.

BBC Bitesize, ‘What is Code?’ (*BBC* 2017) <http://www.bbc.co.uk/guides/zykx6sg> Accessed 15 May 2017.

Beedham M, ‘Report: Cryptocurrency Ransomware Payments up 90%, Thanks to Ryuk’ (*The Next Web* 18 April 2019) <https://thenextweb.com/hardfork/2019/04/18/cryptocurrency-ransom-increase-ryuk/> Accessed 2 December 2019.

––, ‘There Are Now over 5,000 Cryptocurrency ATMs around the World’ (*The Next Web* 26 June 2019) <https://thenextweb.com/hardfork/2019/06/26/5000-bitcoin-cryptocurrency-atms-coinatmradar/> Accessed 2 December 2019.

Beigel O, ‘Bitcoin Wallet Guide, Reviews and Comparison’ (*99bitcoins* 12 November 2019) <https://99bitcoins.com/bitcoin-wallet/> Accessed 2 December 2019.

Berta M, and Noonan W, ‘The Property-Contract Duality of Bitcoin’ (*Financier Worldwide Expert Briefing* June 2015) <https://www.financierworldwide.com/the-property-contract-duality-of-bitcoin#.XeUdyNXgqUk> Accessed 7 June 2016.

Bisq, ‘Bisq Network’ (*Bisq* 2019) <https://bisq.network/> Accessed 8 November 2019.

Bitcoin Core, ‘About Us’ (*Bitcoin Core* 2019) <https://bitcoincore.org/en/about/> Accessed 2 December 2019.

Bitcoin Exchange Guide, ‘Decred—Cryptocurrency Governance Consensus System & Wallet?’ (*BitcoinExchangeGuide* 2017) <https://Bitcoinexchangeguide.com/decred/> Accessed 15 July 2017.

Bitcoin.Org, ‘How Are Bitcoin Created?’ (*Bitcoin.org* 2014) <https://bitcoin.org/en/faq#how-are-bitcoins-created> Accessed 20 June 2018.

––, ‘Bitcoin Developer Examples’ (*Bitcoin.org* 2017) <https://Bitcoin.org/en/developer-examples#testing-applications> Accessed 24 July 2017.

Bitlegal, ‘Interactive Map’ (*Bitlegal* 2017) <http://bitlegal.io/> Accessed 3 July 2017.

Blockchain.com ‘Hashrate Distribution’ (*Blockchain.com* 2017) <https://www.blockchain.com/en/pools> Accessed 1 June 2018.

Bloomberg, ‘Why the Cryptocurrency World is Watching South Korea’ (*Bloomberg* 2 February 2018)

<https://www.bloomberg.com/news/articles/2018-02-04/why-the-cryptocurrency-world-is-watching-south-korea-quicktake> Accessed 3 July 2018.

––, 'Making Sense of the World's Cryptocurrency rules' (*Bloomberg* 19 March 2018) <https://www.bloomberg.com/news/articles/2018-03-19/is-this-legal-making-sense-of-the-world-s-cryptocurrency-rules> Accessed 3 November 2018.

––, 'What the World's Governments Are Saying about Cryptocurrencies' (*Bloomberg* 26 March 2018) <https://www.bloomberg.com/news/articles/2018-03-26/what-the-world-s-governments-are-saying-about-cryptocurrencies> Accessed 3 July 2018.

Boddy M, 'Two Miners Purportedly Execute 51% Attack on Bitcoin Cash Blockchain' (*Cointelegraph*, 25 May 2019) < https://cointelegraph.com/news/two-miners-purportedly-execute-51-attack-on-bitcoin-cash-blockchain> Accessed 8 September 2020.

Breitman K, 'Op Ed: Why Ethereum's Hard Fork Will Cause Problems in the Coming Year' (*BitcoinMagazine* 2017) <https://Bitcoinmagazine.com/articles/op-ed-why-ethereums-hard-fork-will-cause-problems-coming-year/> Accessed 15 May 2017.

Browning L and Davison L, 'Crypto Tax Avoiders Face IRS Roulette: Fess Up or Try Hiding' (*Bloomberg* 1 August 2019) <https://www.bloomberg.com/news/articles/2019-08-01/crypto-tax-avoiders-face-irs-roulette-fess-up-or-try-to-hide> Accessed 15 January 2020.

Buntix J, 'Slush Pool Simplifies Voting Process for Segwit and Bitcoin Unlimited' (*DashTimes* 2017) <http://thedashtimes.com/2017/03/06/slush-pool-simplifies-voting-process-segwit-Bitcoin-unlimited/> Accessed 15 May 2017.

––, 'What is a BIP?' (The Merkle 2017) <https://themerkle-com.cdn.ampproject.org/c/s/themerkle.com/what-is-a-bip/amp/> Accessed 6 June 2016.

––, 'Gemini Launches Block Trading to Attract Institutional Investors' (*The Merkle* 12 April 2018) <https://themerkle.com/gemini-launches-block-trading-to-attract-institutional-investors/> Accessed 27 May 2018.

Burgonye M, 'Canadian Provincial Bitcoin Law: It's All about Protecting the Consumer' (*Coindesk* 23 December 2013) <https://www.coindesk.com/canadian-bitcoin-law-consumer-protection> Accessed 7 June 2016.

Castor A, 'A (Short) Guide to Blockchain Consensus Protocols' (*CoinDesk* 4 March 2017) <https://www.coindesk.com/short-guide-blockchain-consensus-protocols> Accessed 6 June 2017.

Cavallo M, 'How RegTech Closes the Gap Between Technology and Financial Services' (*CIO* 2017) <http://www.cio.com/article/3190162/it-industry/how-

regtech-closes-the-gap-between-technology-and-financial-services.html> Accessed 6 June 2017.

Chainanalysis, ‘The Chainanalysis 2020 Crypto Crime Report’ (*Chainanalysis* January 2020) <https://go.chainalysis.com/2020-Crypto-Crime-Report-Demo.html?aliId=eyJpIjoiQkxPMEcwRk1uXC9zSGRrbTAiLCJ0IjoiN3JUcUNtNWxaUlc2QnhOc2JJOXhqdz09In0%253D> Accessed 15 January 2020.

Chelyshava I, ‘Belarus Cryptocurrency Experiment: Why the World Should Take Notice’ (*Jurist Academic Commentary* 10 January 2018) <http://jurist.org/forum/2018/01/Iryna-Chelyshava-Belarus-cryptocurrency.php> Accessed 6 July 2018.

Circle.com, ‘About’ (*Circle* 2016) <https://www.circle.com/en-gb/about> Accessed 2 December 2019.

Coindesk, ‘How Bitcoin Mining Works’ (*Coindesk* 20 August 2013)<http://www.coindesk.com/information/how-bitcoin-mining-works/> Accessed 2 December 2019.

––, ‘How Can I Buy Bitcoins? (*Coindesk* 2015) <http://www.coindesk.com/information/how-can-i-buy-bitcoins/> Accessed 2 December 2019.

Coinjournal, ‘Bitcoin Usage in the UK’ (*Coinjournal* 2015) <http://coinjournal.net/bitcoin-usage-in-the-uk/> Accessed 8 November 2019.

Coinsutra, ‘What is Cold Storage in Cryptocurrency?’ (*Coinsutra* 12 August 2019) <https://coinsutra.com/cold-storage-cryptocurrency/> Accessed 2 December 2019.

Cointelegraph, ‘Difference between Bitcoin and Bitcoin Cash’ (*Cointelegraph* 2020) <https://cointelegraph.com/Bitcoin-cash-for-beginners/btc-bch-differences> Accessed 27 January 2020.

Coleman L, ‘Bitfinex ‘Bail-In’—New Financial System Offers Laboratory for Handling Unexpected Losses’ (*Cryptocoin News* 12 August 2016) <https://www.cryptocoinsnews.com/bitfinex-bail-new-financial-system-offers-laboratory-handling-unexpected-losses/> Accessed 22 August 2016.

Collins B, ‘Whatever Happened to Second Life?’ (*Alphr* 4 January 2010) <http://www.alphr.com/features/354457/whatever-happened-to-second-life> Accessed 7 June 2016.

Conheady G, ‘Is Fintech Ready for a Global Regulatory Sandbox?’ (*A&LGoodbody* 27 November 2018) <https://www.algoodbody.com/insights-publications/is-fintech-ready-for-a-global-regulatory-sandbox> Accessed 17 February 2020.

Cryptalker, ‘9 Best Bitcoin Tumbler (Mixer) Services’ (*Cryptalker* 2009) <https://cryptalker.com/best-bitcoin-tumbler/> Accessed 8 November 2019.

Cuthbertson A, 'Bitcoin Market Opens to 1.6 Million Muslims as Cryptocurrency Declared Halal under Islamic Law' (*Independent* 13 April 2018) <https://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-islamic-law-muslims-cryptocurrency-market-permissible-sharia-news-price-surge-a8302761.html> Accessed 18 October 2018.

Cutts T, 'Bitcoin Ownership and its Impact on Fungibility' (*Coindesk* 14 June 2015) <http://www.coindesk.com/bitcoin-ownership-impact-fungibility/> Accessed 16 June 2016.

D5000, 'A Cryptocurrency with Many Consensus Methods to Avoid Centralisation' (*Bitcoin Forum* 1 May 2016) <https://Bitcointalk.org/index.php?topic=1456484.0> Accessed 17 July 2017.

Dai W, 'B-Money' (*Weidai.com* 1998) <http://www.weidai.com/bmoney.txt> Accessed 7 June 2016.

Dash, 'Dash is Digital Cash' (*Dash.org* 2015) <https://www.dash.org/> Accessed 25 July 2017.

De Filippi P, 'A $50M Hack Tests the Values of Communities Run by Code' (*Motherboard* 2016) <https://motherboard.vice.com/en_us/article/thedao> Accessed 15 May 2017.

De N, 'World Leaders are Talking Crypto at Davos' (*Coindesk* 25 January 2018) <https://www.coindesk.com/may-lagarde-mnuching-davos-bitcoin-roundup/> Accessed 20 June 2018.

––, 'Quadriga Creditor Protection Filing' (*Coindesk* 1 February 2019) <https://www.coindesk.com/quadriga-creditor-protection-filing> Accessed 2 December 2019.

––, and Baydakova A, 'The Collapse of QuadrigaCX: What We Know (And What We Don't)' (*Coindesk* 6 February 2019) <https://www.coindesk.com/quadrigacx-explainer> Accessed 2 December 2019.

Decred, 'About' (*Decred* 2017) <https://www.decred.org/> Accessed 15 July 2017.

Deloitte, 'RegTech is the New FinTech' (*Deloitte* 2016) <https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/FinancialServices/IE_2016_FS_RegTech_is_the_new_FinTech.pdf> Accessed 6 June 2017.

––, 'Six Control Principles for Financial Services Blockchains' (*Deloitte* October 2017) <https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/financial-services/deloitte-cn-fs-six-principles-for-blockchains-report-en-171121.pdf> Accessed 1 June 2018.

Deshpande A, and others, 'Understanding the Landscape of Distributed Ledger Technologies/Blockchain: Challenges, Opportunities and Prospects for

Standards' (*Rand Corporation* 18 October 2017) <https://www.rand.org/randeurope/research/projects/blockchain-standards.html> Accessed 1 June 2018.

Di Salvo M, 'Report: Use of Cryptocurrencies for Remittances is Growing in Popularity' (*Bitcoin.com* 25 December 2018) <https://news.bitcoin.com/report-use-of-cryptocurrencies-for-remittance-is-growing-in-popularity/> Accessed 2 December 2019.

Dion-Schwarz C, Manheim D, and Johnston P, 'Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats' (*Rand Corporation* 2019) <https://www.rand.org/pubs/research_reports/RR3026.html> Accessed 15 January 2020.

Electric Capital, 'Electric Capital Developer Report H1 2019' (*Medium* 12 August 2019) <https://medium.com/@ElectricCapital/electric-capital-developer-report-h1-2019-7d836d68fecb> Accessed 3 December 2019.

Elliptic, 'Cryptocurrencies: Money Laundering & Terrorist Financing Trends [Infographic]' (*Elliptic* 29 March 2019) <https://www.elliptic.co/our-thinking/cryptocurrencies-money-laundering-terrorist-financing-trends-infographic> Accessed 8 December 2019.

––, 'Bitcoin Money Laundering: How Criminals Use Crypto (And How MSBs Can Clean up Their Act)' (*Elliptic* 18 September 2019) <https://www.elliptic.co/our-thinking/bitcoin-money-laundering> Accessed 8 December 2019.

Ethereum Foundation, 'Ethereum Homestead Release' (*Ethereum.org* 2016) <https://www.ethereum.org/> Accessed 25 July 2017.

FinExtra, 'The Role of Regulator Sandboxes in Fintech Innovation' (*FinExtra* 10 September 2018) <https://www.finextra.com/blogposting/15759/the-role-of-regulatory-sandboxes-in-fintech-innovation> Accessed 11 November 2019.

Frauenfreder M, 'I Forgot My PIN': An Epic Tale of Losing $30,000 in Bitcoin' (Wired 29 October 2017) <https://www.wired.com/story/i-forgot-my-pin-an-epic-tale-of-losing-dollar30000-in-bitcoin/> Accessed 19 February 2019.

Gardler R, and Hanganu G, 'Governance Models' (*OSS Watch* 2010) <http://oss-watch.ac.uk/resources/governancemodels> Accessed 2 December 2019.

Garzik J, 'Bitcoin Upgrade Governance, Hard Forks and Segregated Witness' (*Medium.com* 2017) <https://medium.com/@jgarzik/Bitcoin-upgrade-governance-hard-forks-and-segregated-witness-942885e0ce58> Accessed 15 May 2017.

Gautham, 'Bitcoin Exchange OKCoin Fined in Money Laundering Case' (*Newsbtc* 15 August 2016) <https://www.newsbtc.com/2016/08/15/china-okcoin-exchange-fined> Accessed 15 January 2020.

Github, 'Bitcoin Core Integration' (*Github* 2017) <https://github.com/Bitcoin/Bitcoin> Accessed 24 July 2017.

Gross P, 'A History of Virtual Currency: Why Bitcoins Shouldn't Surprise You' (*CFA Institute* I October 2014) <https://annual.cfainstitute.org/2014/01/10/a-history-of-virtual-currency-why-bitcoins-shouldnt-surprise-you/> Accessed 7 June 2016.

Hacker P, 'Corporate Governance for Complex Cryptocurrencies? A Framework for Stability and Decision Making in Blockchain-Based Organizations' (*SSRN* 22 November 2017) <https://ssrn.com/abstract=2998830> Accessed 27 May 2018.

Hajdarbegovic N, 'Bitcoin miners ditch Ghash.io pool over fears of 51% attack' (*Coindesk* 9 January 2014) <https://www.coindesk.com/bitcoin-miners-ditch-ghash-io-pool-51-attack> Accessed 1 June 2018.

Hagan S, and Mayeda A, 'IMF Calls for Global Talks on Cryptocurrencies' (*Bloomberg* 18 January 2018) <https://www.bloomberg.com/news/articles/2018-01-18/imf-calls-for-global-talks-on-digital-fx-as-bitcoin-whipsaws> Accessed 20 June 2018.

Haig S, 'Chinese Investors Use Wechat Brokers to Bypass ICO Ban' (*Bitcoin.com* 30 March 2018) <https://news.bitcoin.com/chinese-investors-use-wechat-brokers-bypass-ico-ban/> Accessed 3 July 2018.

Hanif U, 'As Pakistan Bans Cryptocurrencies, People May Find Alternative Means' (*Tribune* 13 May 2018) <https://tribune.com.pk/story/1708782/2-pakistan-bans-cryptocurrencies-people-may-find-alternative-means/> Accessed 3 July 2018.

Helms K, 'South Korea to Follow G20 Unified Cryptocurrency Regulation' (*Bitcoin.com* 17 May 2018) <https://news.bitcoin.com/south-korea-g20s-unified-cryptocurrency-regulations/> Accessed 19 June 2018.

Higgins S, 'Silk Road Operator Ross Ulbricht Sentenced to in Life in Prison' (*Coindesk* 29 May 2015) <http://www.coindesk.com/ross-ulbricht-sentenced/> Accessed 20 June 2018.

Higgins S, 'CFTC Fines Bitcoin Exchange Bitfinex $75,000 Over Trading Violations' (*Coindesk* 3 June 2016) < https://www.coindesk.com/cftc-bitcoin-exchange-bitfinex-trading-violations> Accessed 2 December 2019.

Hileman G, and Rauchs M, 'Global cryptocurrency benchmarking study' (*Cambridge Centre for Alternative Finance* 2017) <https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf> Accessed 2 December 2019.

Hinmah W, 'Digital Asset Transactions: When Howey Met Gary (Plastic)' (*SEC* 14 June 2018) <https://www.sec.gov/news/speech/speech-hinman-061418> Accessed 11 November 2018.

Hobday L, 'More Than 1,200 People Complain to ACCC about Bitcoin Scams' (*ABC News* 19 February 2018) <http://www.abc.net.au/news/2018-02-19/more-than-1200-people-complain-to-accc-about-bitcoin-scams/9462240> Accessed 2 December 2019.

Hody S, 'Ownership Does Not Require Possession' (*Medium* 2016) <https://medium.com/@SHodyEsq/ownership-doesnt-require-possession-5eac8e29e460#.itw4rw4f7> Accessed 19 August 2016.

Howmuch.net, 'Comparing Cryptocurrency Against the Entire World's Wealth in One Graph' (*Howmuch.net* 2018) <https://howmuch.net/articles/worlds-money-in-perspective-2018> Accessed 3 December 2019.

Jamali R, and others, 'Cryptocurrency, Digital Asset Class of the Future—Bitcoin vs Ethereum' (*The Economist* 2016) <http://www.economist.com/sites/default/files/economist_case_comp_ivey.pdf> Accessed 6 June 2017.

Jones H, 'G20 Watchdog Focuses on Rules Review, Hold Fire on Cryptocurrencies' (*Reuters* 18 March 2018) <https://www.reuters.com/article/us-g20-regulations-carney/g20-watchdog-focuses-on-rules-review-holds-fire-on-cryptocurrencies-idUSKBN1GU0SF> Accessed 19 June 2018.

JP Morgan, 'Decrypting Cryptocurrencies: Technology, Application and Challenges' (*JP Morgan Perspectives* 9 February 2018) <http://forum.gipsyteam.ru/index.php?act=attach&type=post&id=566108> Accessed 20 June 2018.

Jury A, 'Is the Regulation That Threatens the Free-Spirited Nature of Cryptocurrency Actually the Key to its Future?' (*Bureau Van Dijk* 14 August 2019) <https://www.bvdinfo.com/en-gb/blog/compliance-and-financial-crime/regulation-of-cryptocurrency-actually-the-key-to-its-future> Accessed 3 December 2019.

Kaminska I, 'Time to Re-Evaluate Blockhain Hype' (*FTAphaville* 3 August 2016) <http://ftalphaville.ft.com/2016/08/03/2171799/time-to-reevaluate-blockchain-hype/> Accessed 2 December 2019.

Khatwani S, '2019's Best Cryptocurrency Lending (Crypto Loans) Platforms To Use' (*The Money Mongers* 22 October 2019) Accessed 2 December 2019.

Kroll J, 'The Economics of Bitcoin Mining, or, Bitcoin in the Presence of Adversaries' (*Econinfosec* 2013) <http://www.econinfosec.org/archive/weis2013/papers/KrollDaveyFeltenWEIS2013.pdf> Accessed 20 May 2017.

Kwon J, and Buchman E, 'Cosmos: A Network of Distributed Ledgers' (*Github* 2017) <https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md#governance> Accessed 14 August 2017.

Lee Y, 'Penalties Imposed on 8 Cryptocurrency Exchanges… Violation of 'Not Enough Privacy Measures' (*Byline Network* 24 January 2018) <https://byline.network/2018/01/1-997/> Accessed 8 November 2019.

Litecoin, (*Litecoin.com* 2017) <https://litecoin.com/> Accessed 17 July 2017.

LocalBitcoins, 'About LocalBitcoins.com' (*LocalBitcoins* 2019) <https://localbitcoins.com/about> Accessed 8 November 2019.

Lombardo H, 'Winklevoss Gemini Exchange Gets BitLicense for Oct 8th Official Launch' (*Allcoinsnews* 6 October 2015) <http://allcoinsnews.com/2015/10/06/winklevoss-gemini-exchange-gets-bitlicense-for-oct-8th-official-launch/> Accessed 27 May 2018.

Makhovsky A, 'Belarus Adopts Crypto-Currency Law to Woo Foreign Investors' (*Reuters* 22 December 2017) Accessed 6 July 2018.

Manning J, 'R3 Uses Blockchain to Streamline KYC for Banks around the World' (*RiskScreen* 2018) <https://www.riskscreen.com/kyc360/news> Accessed 21 February 2020.

Marshall A, 'P2P Cryptocurrency Markets, Explained' (*Cointelegraph* 7 April 2007) <https://cointelegraph.com/explained/p2p-cryptocurrency-exchanges-explained> Accessed 19 June 2018.

Matonis J, 'Why the OECD Needs to do its Homework on Cryptocurrencies' (*Coindesk* 1 July 2014) <https://www.coindesk.com/oecd-needs-homework-bitcoin/> Accessed 3 July 2018.

McKendry I, 'ISIL May Be Using Bitcoin, Fincen's Calvery Says', (*American Banker* 16 November 2015) <https://www.americanbanker.com/news/isil-may-be-using-bitcoin-fincens-calvery-says> Accessed 15 January 2020.

McMillan R, 'The Inside Story of Mt Gox, Bitcoins $460million Disaster' (*Wired.com* 3 March 2014) <http://www.wired.com/2014/03/bitcoin-exchange/> Accessed 2 December 2019.

Mersch Y, 'Virtual or Virtueless? The Evolution of Money in the Digital Age' (*ECB* 8 February 2018) <https://www.ecb.europa.eu/press/key/date/2018/html/ecb.sp180208.en.html> Accessed 3 July 2018.

Miles C, 'Blockchain Security: What Keeps Your Transaction Data Safe?' (*IBM* 12 December 2017) <https://www.ibm.com/blogs/blockchain/2017/12/blockchain-security-what-keeps-your-transaction-data-safe/> Accessed 2 December 2019.

Motiani P, 'Your Bank Will Not Allow You to Buy Bitcoin Anymore' (*The Economis*t 6 April 2018) <https://economictimes.indiatimes.com/wealth/personal-finance-news/your-bank-will-not-allow-you-to-buy-bitcoins-anymore/articleshow/63627123.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst> Accessed 6 July 2018.

Murphy H, ''Wild West' Crypto-Asset Markets Need UK Regulation, say MPs' (*The Financial Times* 19 September 2018) <https://www.ft.com/content/dbea3cac-bb3c-11e8-8274-55b72926558f> Accessed 11 November 2018.

Nakamoto S, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (*Bitcoin.org* 2009) <https://bitcoin.org/bitcoin.pdf> Accessed 27 May 2018.

Nakamura Y, 'The World's Biggest Cryptocurrency Exchange Heading to Malta' (*Bloomberg* 23 March 2018) <https://www.bloomberg.com/news/articles/2018-03-23/the-world-s-biggest-cryptocurrency-exchange-is-moving-to-malta> Accessed 18 June 2018.

Nasseri L, 'Iran's Central Bank Imposes Ban on Cryptocurrency Transactions' (*Bloomberg* 23 April 2018) <https://www.bloomberg.com/news/articles/2018-04-23/ban-on-cryptocurrency-transactions-imposed-by-iran-central-bank> Accessed 6 July 2018.

Noyes C, 'BitAv: Fast Anti-Malware by Distributed Blockchain Consensus and Feedforward Scanning' (*Arxiv.org* 2016) <https://arxiv.org/pdf/1601.01405.pdf> Accessed 6 June 2017.

Oberhaus D, 'What Happens When a Chinese Giant Swoops in on Your Tiny Cryptocurrency' (*Motherboard* January 22, 2018) <https://motherboard.vice.com/en_us/article/ev59dz/bitmain-siacoin-obelisk-asic-vorick> Accessed 1 June 2018.

Østbye P, 'The Adequacy of Competition Policy for Cryptocurrency Markets' (*SSRN* 2017) <https://ssrn.com/abstract=3025732> Accessed 27 May 2018.

Paech P, 'Integrating Global Blockchain Securities Settlement with the Law—Policy Considerations and Draft Principles' (*SSRN* 7 August 2016) <https://ssrn.com/abstract=2792639> Accessed 18 June 2018.

Panorama Crypto, '8 Cryptocurrency Lending Platforms' (*Panorama* Crypto 3 October 2019) <https://panoramacrypto.com/8-cryptocurrency-lending-platforms/> Accessed 2 December 2019.

Poster A, 'Cryptoassets Regulatory Arbitrage—A Clear and Present Danger' (*Forbes* 9 December 2019) <https://www.forbes.com/sites/amyposter/2019/12/09/crypto-assets-regulatory-arbitragea-clear-and-present-danger/#395730477438> Accessed 10 December 2019.

PRWeb, 'Clifford Chance Enhances Document Review with AI in Microsystems Contract Companion' (*PRWeb* 2017) <http://www.prweb.com/releases/2017/06/prweb14395641.htm> Accessed 15 June 2017.

Quentson A, 'Price Shoots Up as Bitcoin Unlimited Surpasses Segwit' (*CryptocoinNews* 2017) <https://www.cryptocoinsnews.com/price-shoots-Bitcoin-unlimited-surpasses-segwit/> Accessed 6 June 2017.

Ramasastry A, 'Is Bitcoin Money? Lawmakers, Regulators and Judges Don't Agree' (*Justia* 9 September 2014) <https://verdict.justia.com/2014/09/09/bitcoin-money> Accessed 7 June 2016.

Rapoza K, 'Cryptocurrency Exchanges Officially Dead in China' (*Forbes* 2 November 2017) <https://www.forbes.com/sites/kenrapoza/2017/11/02/cryptocurrency-exchanges-officially-dead-in-china/#3631935d2a83> Accessed 3 July 2018.

Rauchs M, and others, '2nd Global Cryptoasset Benchmarking Study' (*Cambridge Centre for Alternative Finance* December 2018) <https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2019-09-ccaf-2nd-global-cryptoasset-benchmarking.pdf> Accessed 2 December 2019.

Rikken O, '3 Smart Contract Misconceptions' (*CoinDesk* 2017) <https://www.coindesk.com/3-common-smart-contract-misconceptions-explored/> Accessed 6 June 2017.

Roberts D, 'With Gemini, Winklevoss Brothers Seek Respect in Bitcoin' (*Fortune* 2015). <http://fortune.com/2015/10/05/gemini-winklevoss-Bitcoin/> Accessed 25 July 2016.

Satran R, '6 Virtual Currencies That Went Bust' (*US News* 13 May 2013) <http://money.usnews.com/money/personal-finance/slideshows/6-virtual-currencies-that-went-bust/9> Accessed 7 June 2016.

Sedgwick K, 'You Can Now 51% Attack a Coin for as little as $500' (*Bitcoin.com* May 29, 2018) <https://news.bitcoin.com/you-can-now-51-attack-a-coin-for-as-little-as-500/> Accessed 1 June 2018.

Sharma R, 'Running a Full Bitcoin Node for Investors' (*Investopedia* 25 June 2019) <https://www.investopedia.com/news/running-full-bitcoin-node-investors/> Accessed 2 December 2019.

Shifflett S, and Jones C, 'Buyer Beware: Hundreds of Bitcoin Wannabes Show Hallmarks of Fraud' (*Wall Street Journal* 17 May 2018) <https://www.wsj.com/articles/buyer-beware-hundreds-of-bitcoin-wannabes-show-hallmarks-of-fraud-1526573115> Accessed 2 December 2019.

Shin L, 'Why Bitcoin's Greatest Asset could also Spell its Doom' (*Forbes* 20 April 2017) <https://www.forbes.com/sites/laurashin/2017/04/20/why-bitcoins-greatest-asset-could-also-spell-its-doom/#f9ed8126adcd>> Accessed 17 July 2017.

Shulze E, '"We Are about to See Massive Disruptions": IMF's Lagarde Says it's Time to Get Serious about Digital Currency' (*CNBC* 13 October 2017) <https://www.cnbc.com/2017/10/13/bitcoin-get-serious-about-digital-currency-imf-christine-lagarde-says.html> Accessed 19 June 2018.

Smith S, and others, 'Huge Cyberattack Hits Nearly 100 Countries with 'Wanna Decryptor' Malware' (*NBC News* 13 May 2017) <http://www.nbcnews.com/news/world/national-health-service-cyberattack-hits-english-hospitals-hackers-demand-Bitcoin-n758516> Accessed 6 June 2017.

Suberg W, 'Indonesia: $70 Million Capital Requirement for Bitcoin Futures Sparks Anger' (*Cointelegraph* 14 February 2019) <https://cointelegraph.com/news/indonesia-70-million-capital-requirement-for-bitcoin-futures-sparks-anger> Accessed 14 February 2019.

Tezos, 'Governance' (*Tezos* 2017) <https://www.tezos.com/governance> Accessed 15 July 2017.

Thomson P, 'Most Significant Hacks of 2019—New Record of Twelve in One Year' (*Cointelegraph* 20 January 2020) <https://cointelegraph.com/news/most-significant-hacks-of-2019-new-record-of-twelve-in-one-year> Accessed 15 January 2020.

Vaswani K, 'China Bans Initial Coin Offerings Calling Them 'Illegal Fundraising'' (*BBC News* 5 September 2017) <https://www.bbc.co.uk/news/business-41157249> Accessed 3 July 2018.

Vaziri A, 'Bitcoin Exchanges as Payment Institutions' (*Neopay* 2014) <http://neopay.co.uk/site/wp-content/uploads/Diacle-Bitcoin-Regulation.pdf> Accessed 3 July 2018.

Weiczner J, 'Inside New York's Bitlicense Bottleneck: An 'Absolute Failure'? (*Fortune* 25 May 2018) <http://fortune.com/2018/05/28/bitcoin-cryptocurrency-new-york-bitlicense/> Accessed 6 July 2018.

Weinstein J, Cohn A, and Parker C, 'Promoting Innovation through Learning' in J Dewey (ed) *Global Legal Insights—Blockchain and Cryptocurrency Regulation* (Global Legal Group 2019).

Williams-Grut O and Price R, 'A Bitcoin Civil War is Threating to Tear the Digital Currency in 2' (*Business Insider* 2017) <http://uk.businessinsider.com/Bitcoins-hard-fork-Bitcoin-unlimited-segregated-witness-explained-2017-3> Accessed 16 June 2017.

Wilmoth J, ‘Coincheck to Delist Privacy Coins Monero, Zcash and Dash’ (*CCN.com* 19 May 2018) <https://www.ccn.com/coincheck-to-delist-privacy-coins-monero-zcash-and-dash/> Accessed 27 May 2018.

Wong J, ‘China’s Bitmain Dominates Bitcoin Mining’ (*Quartz* 20 August 2017) <https://qz.com/1053799/chinas-bitmain-dominates-bitcoin-mining-now-it-wants-to-cash-in-on-artificial-intelligence/> Accessed 1 June 2018.

Wood J, ‘Crypto Exchanges: Custodial vs Non-Custodial vs Decentralized’ (*Medium* 18 March 2018) <https://medium.com/@jacobrobertwoods/crypto-exchanges-custodial-vs-non-custodial-vs-decentralized-3d1d04cf205> Accessed 2 December 2019.

Yanfei W, ‘PBOC Inches Closer to Digital Currency’, (*China Daily* 14 October 2017) <http://www.chinadaily.com.cn/business/2017-10/14/content_33235955.htm> Accessed 6 July 2018.

Young J, ‘China’s Stricter Bitcoin Regulations Will Strengthen Hong Kong Market’ (*Cointelegraph* 16 September 2017) <https://cointelegraph.com/news/chinas-stricter-bitcoin-regulations-will-strengthen-hong-kong-market> Accessed 3 July 2018.

Zcash, ‘What is Zcash?’ (*Zcash* 2016) <https://z.cash/> Accessed 25 July 2017.

Zetter K, ‘How the Feds Took down the Silk Road Drug Wonderland’ (*Wired.Com* 18 November 2013) <http://www.wired.com/2013/11/silk-road/> Accessed 2 December 2019.

Zuberi M, ‘Bitcoin Identity Crisis: Currency or Property’? (*Lexology* 17 February 2016) <http://www.lexology.com/library/detail.aspx?g=65a1f5fb-521f-49f7-90f0-6aaa08ada139> Accessed 7 June 2016.

Other Sources

Szabo N, ‘*Smart Contracts’* (Unpublished Manuscript 1994).