

UNIVERSITY OF MALTA

THE CHALLENGES AND OPPORTUNITIES OF
BLOCKCHAIN TECHNOLOGY AND
CRYPTOCURRENCIES IN THE AMBIT OF GAMING LAW

*A thesis submitted in partial fulfilment of the
degree of Doctor of Laws (LL.D)*

EMMA PORTELLI BONNICI

Faculty of Laws

University of Malta

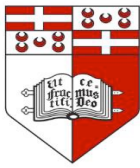
July 2017



University of Malta Library – Electronic Thesis & Dissertations (ETD) Repository

The copyright of this thesis/dissertation belongs to the author. The author's rights in respect of this work are as defined by the Copyright Act (Chapter 415) of the Laws of Malta or as modified by any successive legislation.

Users may access this full-text thesis/dissertation and can make use of the information contained in accordance with the Copyright Act provided that the author must be properly acknowledged. Further distribution or reproduction in any format is prohibited without the prior permission of the copyright holder.



UNIVERSITY OF MALTA

FACULTY/~~INSTITUTE~~/~~CENTRE~~/SCHOOL _____

DECLARATION OF AUTHENTICITY FOR POSTGRADUATE STUDENTS

Student's I.D. /Code _____

Student's Name & Surname _____

Course _____

Title of Thesis/Dissertation:

Word count _____

I hereby declare that I am the legitimate author of this Dissertation and that it is my original work.

No portion of this work has been submitted in support of an application for another degree or qualification of this or any other university or institution of higher education.

I hold the University of Malta harmless against any third party claims with regard to copyright violation, breach of confidentiality, defamation and any other third party right infringement.

As a Master's student, as per Regulation 58 of the General Regulations for University Postgraduate Awards, I accept that should my thesis/dissertation be awarded a Grade A, it will be made publicly available on the University of Malta Institutional Repository.

Signature of Student

Date

ABSTRACT

Malta already holds a top spot within the international gaming industry, and this thesis aims to ensure that Malta remains at the forefront of this through an in-depth analysis of how cryptocurrencies and the blockchain can be used within the national context. This text delves into the challenges and opportunities surrounding cryptocurrencies and the blockchain within the context of Maltese law, specifically contract law and gaming law. It aims to bring to the fore a discussion on the possibilities of including decentralised storage of information in the sphere of public sector, as well as other possible applications. The thesis attempts to explore the misconceptions surrounding the ‘anonymity’ aspect of cryptocurrencies whilst also delving into the criminal aspect which is too often the first thought that comes to mind upon thinking about cryptocurrencies. It also provides an in-depth discussion on smart contracts and their possible usage across the Maltese landscape and their interplay with traditional contract law.

CRYPTOCURRENCIES – GAMING – BITCOIN – BLOCKCHAIN – SMART
CONTRACTS

*To my parents, who have always made me feel like I could actually make this a reality –
thank you for your unwavering love and support.*

TABLE OF CONTENTS

DECLARATION OF AUTHENTICITY FOR POSTGRADUATE STUDENTS.....	ii
ABSTRACT.....	iii
TABLE OF CONTENTS	v
TABLE OF JUDGEMENTS.....	ix
TABLE OF LEGISLATION	x
ACKNOWLEDGEMENTS	xii
ABBREVIATIONS.....	1
INTRODUCTION	4
Chapter 1: Cryptocurrencies	7
1.1 Cryptocurrencies: a Brief History	7
1.2 An Introduction to Bitcoin, Altcoins and Currency	9
1.2.1 Bitcoin.....	9
1.2.2 Altcoins	12
1.2.3 The Value of Bitcoin.....	13
1.2.4 The Price of Bitcoin	14
1.2.5 The Possibility of a Bitcoin Exchange	14
1.2.6 Mining Bitcoin	17
1.2.7 The Double Spend Problem	18
1.3 The Dark Web and Dark Markets.....	19
1.4 The Relationship between the Dark Web and cryptocurrencies	22
1.5 A Comparative Analysis of the Legality of Cryptocurrencies.....	23
1.5.1 Introduction.....	23
1.5.2 Malta.....	23
1.5.3 The United Kingdom.....	25
1.5.4 The Isle of Man	27
1.5.5 The United States	27
1.5.6 The European Union.....	29
1.5.6.1 Luxembourg	31
1.5.6.2 Germany.....	32

1.5.7 Thailand	32
1.5.8 Other Jurisdictions.....	32
1.6 Conclusion	33
Chapter 2: The Blockchain	35
2.1 The Seven Design Principles of the Blockchain Economy	36
2.1.1 Networked Integrity	36
2.1.2 Distributed Power.....	39
2.1.3 Value as Incentive.....	39
2.1.4 Security	41
2.1.5 Privacy.....	41
2.1.6 Rights Preserved.....	42
2.1.7 Inclusion.....	43
2.2 The Trust Protocol	44
2.3 The Blockchain	45
2.4 Ethereum	47
2.5 The Implications of Decentralisation.....	50
2.6 The Various Applications of Blockchain Technology.....	52
Chapter 3: Smart Contracts	54
3.1 The Essence of the Contract	54
3.1.1 Elements for the Validity of a Contract	54
3.1.2 Different Types of Contracts.....	54
3.1.3 Verbal Agreements.....	58
3.1.4 Contract Law and Smart Contracts: a New Era?.....	58
3.1.5 The Enforceability of Gaming Debts and the Blockchain	59
3.2 Smart Contracts: an introduction	61
3.2.1 The Application of Smart Contracts in the Context of Traditional Contract Law	65
3.2.2 An Exception to the Application of Smart Contracts	66
3.3 Oracles	66
3.4 Conclusion	67
Chapter 4: The Challenges and Opportunities Pertaining to Money Laundering and The Financing of Terrorism Insofar as The Blockchain And Cryptocurrencies.....	68
4.1 Cryptocurrencies: a Misnomer?.....	68
4.2 Directives,Laws and Regulations.....	69

4.2.1 The Current Regime on Money Laundering and the Financing of Terrorism.....	69
4.2.2 The Electronic Money Directive	71
4.2.3 The Payment Services Directives.....	71
4.2.4 The Money Laundering Directives.....	72
4.2.5 The Central Bank of Malta Act	75
4.2.6 The Prevention of Money Laundering Act.....	76
4.2.7 The Prevention of Money Laundering and Funding of Terrorism Regulations	77
4.2.8 The Malta Gaming Authority's Stance	78
4.3 Cryptocurrencies, the Blockchain, Money Laundering and the Financing of Terrorism ..	80
4.4 The Way Forward	83
Chapter 5: Other Challenges and Opportunities in Gaming Law	85
5.1 The Technical Challenges to Implementation	85
5.1.1 The Technology Might not be Ready for the Mainstream.....	85
5.2.1 Unsustainable Energy Consumption.....	90
5.2.2 Governments Might Thwart it.....	91
5.2.3 Privatisation vs Accessibility.....	92
5.2.4 Inadequate Incentives for Mass Collaboration.....	93
5.2.5 Blockchain and Employment.....	93
5.2.6 Governing the Protocols.....	94
5.2.7 The Skynet: a Farfetched Concept Rooted in Reality	95
5.2.8 Anonymity and Control.....	96
5.2.9 The Illicit Aspect	97
5.3 The Legal Challenges to Implementation	98
5.3.1 Financial Transfers.....	99
5.3.2 Multi-Signature Transactions	100
5.3.3 Merchant Issued Digital Currencies and 'Coloured Coins'	100
5.3.4 Intellectual Property and Property Registers	101
5.3.5 Storage and Data Transfer	101
5.3.6 Decentralised Organisations	102
5.3.7 Securities and Financial Products.....	102
5.3.8 Competition Law.....	103
5.3.9 Accountability, Responsibility and Liability.....	103
5.3.10 Regulatory Change	104

5.3.11 Smart Contracts	104
CONCLUSION	105
BIBLIOGRAPHY	107
THESES	107
BOOKS	107
WORKING PAPERS	107
OTHER	108
EU PUBLICATIONS	109
ONLINE JOURNALS	110
ONLINE ARTICLES, WEBSITES AND BLOGS	110

TABLE OF JUDGEMENTS

USA

United States Court of Appeals, Second Circuit. United States of America, Appellee, v. Ross William Ulbricht, a/k/a Dread Pirate Roberts, a/k/a Silk Road, a/k/a Sealed Defendant 1, a/k/a DPR, Defendant-Appellant. Docket No. 15-1815; Decided: May 31, 2017

US Securities and Exchange Commission v. Trendon T. Shavers and Bitcoin Savings and Trust, Civil Action No. Civil Action No. 4:13-CV-416

State of Florida, 11 Circuit, The State of Florida v. Michell Abner Espinoza, Case Number F14-2923

EU

Skatteverket v David Hedqvist (2015) ECJ C-264/14

Malta

Salvatore Grech vs Carmelo Sive Charles Bennetti Et, 27th January 1961, (First Hall Civil Court)

Avukat Dottor Joseph Cassar Noe vs Joseph Grech Marguerat, 23rd June 1967, (Court of Appeal, Civil, Superior)

Bartoli vs Chetcuti, 13/06/2013

Gio Maria Muscat vs. Carmelo Vella, 25th February 1950, (First Hall Civil Court)

Felix Farrugia vs. Direttur tas-Sigurta' Soċjali, 19th October 2005, (Court of Appeal, Inferior).

Carmelo Parascandalo vs Procuratore Legale Pietro Paolo Lanzon Court of Appeal 17th April 1925

Borg Julia vs. Brignone Carmel, 6th October 1999, Court of Appeal (Civil, Superior)

Micallef vs. Micallef (22nd February 2006) (First Hall, Civil Court)

TABLE OF LEGISLATION

EUROPEAN UNION

Directives

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

Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering - Commission Declaration

Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing

Directive (EU) 2015/849 of the European Parliament and of the Council L of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC

Commission, Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council and repealing Council Directive 93/22/EEC

Council Directive 2009/110/EC of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions [2009]OJL267/11

Council Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC

Council Directive 2015/2366 (EU) of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015]OJL319

Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax

Malta

Criminal Code, Chapter 9 of the Laws of Malta

Civil Code, Laws of Malta Chapter 16

Trusts and Trustees Act, Chapter 331 of the Laws of Malta

Lotteries and Other Games Act, Chapter 438 of the Laws of Malta

Remote Gaming Regulations, Chapter 438.04 of The Laws of Malta

Isle of Man

Proceeds of Crime Act 2008 (AT 13 of 2008)

USA

The Uniform Commercial Code 1952

Others

Malta Gaming Authority, 'A White Paper to Future Proof Malta's Gaming Legal Framework'
(Malta Gaming Authority, July 2017)

ACKNOWLEDGEMENTS

I would like to thank my tutor Dr. Joseph F. Borg; my friends Catherine, Julia, Sarah, Robert, Kristina and Joseph for always being there when I needed company or someone to talk to; Alistair and Nicola for their guidance and input; KSU for adding activism to academia; my parents for always being there for me; my grandparents because they deserve nothing less; and the rest of my family for their boundless support and faith in me.

ABBREVIATIONS

AI	Artificial intelligence
AML	Anti-Money Laundering
BTC	Bitcoin
BTCST	Bitcoin Savings and Trust case
CBM	Central Bank of Malta
CBMA	Central Bank of Malta Act
CDD	Customer Due Diligence
CJEU	Court of Justice of the European Union
CoE	Council of Europe
CPU	Central Processing Unit
Dapps	Decentralised applications
DARPA	Defense Advanced Research Projects Agency
ECB	European Central Bank
ECHR	European Convention on Human Rights
ECJ	European Court of Justice
ECtHR	European Court of Human Rights
EEA	European Economic Area
EMD1	Electronic Money Directive
EMD2	Second Electronic Money Directive
ETF	Exchange Traded Fund
ETP	Exchange Traded Product
EU	European Union
EVM	Ethereum Virtual Machine

FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation
FIAU	Financial Intelligence Analysis Unit
FinCEN	Financial Crimes Enforcement Network
GDP	Gross Domestic Product
IRS	Internal Revenue Service
KYC	Know Your Client
MFSA	Malta financial services authority
MGA	Malta Gaming Authority
MIT	Massachusetts Institute of Technology
ML/TF	Money Laundering and the Financing of Terrorism
MLD1	The First Anti-Money Laundering Directive
MLD2	The Second Anti-Money Laundering Directive
MLD3	The Third Anti-Money Laundering Directive
MLD4	The Fourth Anti-Money Laundering Directive
MSBs	Money Service Businesses
NPPS	New Payment and Product Services
PKI	Public Key Infrastructure
PLMA	Prevention of Money Laundering Act
PoA	Proof of Activity
PoC	Proof of Capacity
PoE	Proof of Existence
PoS	Proof of Stake
PoS2	Proof of Storage

PoW	Proof of Work
PSD1	The First Payment Services Directive
PSD2	The Second Payment Services Directive
R&D	Research & Development
RGR	Laws of Malta Subsidiary Legislation 438.04. Remote Gaming Regulations
SEC	American Securities and Exchange Commission
SEPA	Single Euro Payments Area
SPV	Simplified Payment Verification
TOR	The Onion Router/Tor/The Onion Network
UBO	Ultimate Beneficial Owner
UK	United Kingdom
URL	Uniform Resource Locator
USA	United States of America
VAT	Value Added Tax
VCS	Virtual Currency Scheme
VPN	Virtual Private Network

INTRODUCTION

The aim of this thesis is to critically examine the technological advances in the field of cryptocurrencies and the blockchain, particularly in the ambit of gaming law. The future will not wait for us to catch up, and we need to ensure that our laws are comprehensive enough to embrace this new technology. Only then, can we ensure that Malta remains at the forefront of this industry.

Through the carefully divided chapter sections in this thesis, the author attempts to explore the multifaceted way in which cryptocurrencies and blockchain can be used to our advantage. This thesis primarily tackles Maltese law, but referring to a technology as nascent as this, would have been impossible without insight from different jurisdictions. A point of note is that, as yet, there is limited case law on the subject due to it still being in its infancy.

The thesis is divided into five chapters, each tackling a different aspect of the application of this technology: from introductory discussions on the foundations of Bitcoin pertinent to the understanding of the underlying blockchain technology, to an in-depth analysis of smart contracts and the way in which they interact with traditional Maltese contract law.

The first chapter gives the reader an introduction into the notion of cryptocurrencies, providing an overview of the more popular types of cryptocurrencies and altcoins, with an emphasis on Bitcoin as the primary example used throughout the thesis. Stemming from the original mastermind behind Bitcoin - Satoshi Nakamoto's white paper on Bitcoin¹ - until today's various applications of the skeletal software behind the Bitcoin model - the blockchain. In doing so, the author also explores the relationship between cryptocurrencies and the dark web, delving into the original cypherpunks and the landmark case concerning the dark website The Silk Road² - one of the most notorious of its kind.

The concluding part of this chapter provides a comparative analysis of the legislation of cryptocurrencies in different jurisdictions, such as the United Kingdom and The Isle of Man, in order for one to be able to gain a broader understanding of the legality of cryptocurrencies across the board.

¹ Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' [October 31, 2008] Metzger, Dowdeswell & Co Website

² The Silk Road is an online marketplace hosted on the Dark Web where individuals may purchase a myriad of illicit items such as illegal drugs or unlicensed firearms using Bitcoin. The websites hosted on the Dark Web are not indexed by search engines such as Google and thus do not show up through a simple Internet search. These sites are only accessible through the use of TOR software – web anonymiser.

Chapter Two constitutes an in-depth exploration of the design principles that make up the blockchain economy. Although this part of the thesis is rather technical, the author feels that it offers insight into understanding the entirety of the challenges and opportunities presented by this technology. This chapter delves into topics such as the distribution of power and consensus, and also touches upon the notions of privacy within the context of the blockchain.

The second chapter goes on to define the trust protocol, an integral aspect of the blockchain, which safeguards the transactions that take place over the Internet. Decentralisation is another aspect of this multi-faceted approach to the breaking down of the understanding of the blockchain, whereby the author explains the importance of this aspect of the technology. Decentralisation is the crux of this technology³ - it is a salient aspect of the blockchain, and it allows for the users to maintain a ledger across a number of decentralised locations, which increases security and transparency and makes it somewhat impenetrable to fraud and hacking.

Chapter Three concerns the smart contract - exploring the validity of traditional contracts under Maltese law, through an in-depth analysis of the provisions of the Maltese Civil Code⁴ pertaining to contracts. The mesh that exists between smart contracts and traditional contract law is explored in order to show the ease with which they could be transposed into the Maltese legal system.

Chapter Four explores the challenges and opportunities of cryptocurrencies pertaining to money laundering and the financing of terrorism, as well as examining the directives in place to prevent this criminal activity. It examines the stance of the Malta Gaming Authority vis-a-vis the introduction of cryptocurrencies, and the Government's vision for Malta to become a hub – much like it did for the gaming industry – for international companies that operate using cryptocurrencies. Thus, Malta's legislative intentions in this regard are being formulated. In light of the Malta Gaming Authority's White Paper⁵ on the reform of Malta's Gaming Legal Framework, it is of the utmost importance that these points are assessed throughout the formulation of the new regulations. The provision of proper regulation and

³ Sheel Tyle, Kaushal Mohit, 'The-blockchain-what-it-is-and-why-it-matters/' (<https://www.brookings.edu/blog/techtank/2015/01/13/the-blockchain-what-it-is-and-why-it-matters/>, 13 January 2015) <<https://www.brookings.edu/blog/techtank/2015/01/13/the-blockchain-what-it-is-and-why-it-matters/>> accessed 30 July 2017

⁴ Civil Code, Laws of Malta Chapter 16

⁵ Malta Gaming Authority, 'A White Paper to Future Proof Malta's Gaming Legal Framework' (Malta Gaming Authority, July 2017) <<http://www.mga.org.mt/wp-content/uploads/White-Paper-to-Future-Proof-Maltas-Gaming-Legal-Framework.pdf>> accessed 30 July 2017

adequate safeguards will enhance our position at the forefront of this technology and will ensure that the gaming industry's contribution to the national GDP continues to increase.

The challenges faced by the broad implementation of blockchain technology, both in the ambit of gaming law and in its more widespread use, are examined in Chapter Five. The author questions the readiness of the technology for mainstream implementation, and includes an interesting examination of current social behaviour and the changes which would be required in human behaviour with the implementation of blockchain technology.

The impact on financial services, the employment sector and the examination of the current legal framework is also discussed in this chapter. The author examines the inadequacy of the laws that are in place, and the current legal framework when dealing with the issues arising from the implementation of blockchain technology. These issues are mainly due to the fast pace of technological advances when compared to the rate at which legislation is amended or introduced. This highlights the ever-important point that laws should always be written in a technologically neutral manner. Whilst interpretation is of course still imperative in the understanding of the law, making laws more straightforward and comprehensible would lead to a more forward-thinking result, ensuring that situations such as the mention of the 'fax' in the past does not make the law redundant with the introduction of 'email' in the future.

Throughout the thesis, the author seeks to present solutions to the real problems facing the implementation of this technology, so that Malta will be present at the forefront of the industries exploiting these technological breakthroughs.

Chapter 1: Cryptocurrencies

1.1 Cryptocurrencies: a Brief History

‘A cryptocurrency is a medium of exchange, created and stored electronically in the blockchain, using encryption techniques to control the creation of monetary units and to verify the transfer of funds.’⁶ Cryptocurrencies are intangible, and hence, they may be fairly difficult to envisage as a concept. They have no intrinsic value or physical form, nor does any financial institution or bank determine their supply.⁷ One of the most impressive characteristics of many cryptocurrencies is the fact that the network on which some of them are stored is decentralised.⁸ This decentralisation makes them nearly impossible to hack, and this is paramount in the consideration of their importance. Decentralisation will be tackled in Chapter 2.

Conceptually, cryptocurrencies were first described in 1998 by an individual called Wei Dai.⁹ He disseminated his ideas on the Cypherpunks mailing list,¹⁰ which resulted in a sharing of information with like-minded individuals. The Oxford dictionary definition of Cypherpunk is a ‘person who uses encryption when accessing a computer network in order to ensure privacy, especially from government authorities.’¹¹ The author is of the opinion that this definition perfectly encapsulates their general motivations for assembly. The aforementioned mailing list constituted one of the few mediums through which any interested individuals could keep themselves updated on the ideas generated by other individuals at a time when the discussion was underground and still fairly low-key.

⁶ ‘Cryptocurrency’ (Urban Crypto) <<https://urbancrypto.com/cryptocurrency/>> accessed 30 July 2017

⁷ European Central Bank, ‘Virtual Currency Schemes’ (2012) <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> > accessed 30 July 2017

⁸ Eric Voorhees, ‘Is Bitcoin Truly Decentralized? Yes – and Here Is Why It’s Important’ (https://bitcoinmagazine.com/articles/bitcoin-truly-decentralized-yes-important-1421967133/by Erik Voorhees Jan 22, 2015 5:52 PM EST What is Poet? Is Bitc..., 22 Jan 2015) <<https://bitcoinmagazine.com/articles/bitcoin-truly-decentralized-yes-important-1421967133/>> accessed 30 July 2017

⁹ Wei Dai, ‘Http://www.weidaicom/bmoney.txt’ (Http://www.weidaicom/) <<http://www.weidai.com/bmoney.txt>> accessed 30 July 2017

¹⁰ The cypherpunks webmaster, ‘Cypherpunks Mailing List’ (https://www.cypherpunksto/list/, X) <<https://www.cypherpunks.to/list/>> accessed 30 July 2017

¹¹ ‘English Oxford Living Dictionaries’ <<https://en.oxforddictionaries.com/definition/cypherpunk>> accessed 30 July 2017

Cypherpunks are a group of people who advocate the widespread use of code.¹² This movement is primarily led by Julian Assange, the founder of WikiLeaks, and it has been since the movement's inception in the 1980s. Even though cryptography had been around prior to this inception, it was not yet mainstream and was only used in military and government agencies. The mailing list that was used to transmit the knowledge surrounding cryptocurrencies came about in 1992, as a forum for interested participants. This mailing list is still on-going but in a different capacity to that of its original inception. Cypherpunks' main 'coherent set of beliefs'¹³ is to advocate against corporate control and in favour of Internet privacy and security.¹⁴ Cypherpunks follow a libertarian philosophy, often to a radical degree. They list the main reasons why people join their group as being primarily one of status – being part of such a group is considered 'cool' – and secondly that of promoting liberty, through reducing the government's ability to interfere in the personal life and online persona of an individual; in fact, one of their mantras is that 'Cypherpunks break the laws they don't like'.¹⁵ Foreseeably, the growth of the Cypherpunk movement has sparked numerous controversies, primarily because of the actions they take in order to reach their end goals¹⁶. The basic ideas that drive the Movement are also reiterated in 'A Cypherpunk's Manifesto' – written in 1993 by Eric Hughes¹⁷.

Libertarian theory is the antithesis of authoritarian theory, the latter being akin to the situation found in the dystopian novel 1984 by George Orwell¹⁸, so as not to mention a real-life scenario. Libertarian theory advocates that the state should not be in control of information and that this information should be disseminated freely throughout the population.¹⁹ Thomas Jefferson, the third president of the United States, was quoted as saying:

The basis of our government being the opinion of the people, the very first object should be to keep that right; and were it left to me to decide whether

¹² Timothy C May, ' THE CYPHERNOMICON: Cypherpunks FAQ and More, Version 0666, 1994-09-10, Copyright Timothy C May ' (THE CYPHERNOMICON: Cypherpunks FAQ and More, Version 0666, 9 October 1994) < THE CYPHERNOMICON: Cypherpunks FAQ and More, Version 0.666, 1994-09-10, Copyright Timothy C. May. > accessed 30 July 2017

¹³ *ibid*

¹⁴ *ibid*

¹⁵ *ibid*

¹⁶ *ibid*

¹⁷ Eric Hughes, 'A Cypherpunk's Manifesto' (<https://www.activismnet/cypherpunk/manifestohtml>, 1993) < <https://www.activism.net/cypherpunk/manifesto.html>> accessed 30 July 2017

¹⁸ George Orwell, 1984 (Secker & Warburg 8 June 1949)

¹⁹ Mishra Sneha, 'Libertarian Theory of Mass Communication' (<https://www.businessstopianet/>) <<https://www.businessstopia.net/mass-communication/libertarian-theory-mass-communication>> accessed 30 July 2017

we should have a government without newspapers or newspapers without a government, I should not hesitate a moment to prefer the latter.²⁰

This ideology fits in with the libertarian way of thinking, preferring to have information disseminated without government rather than the contrary. This lack of centralised authority has led to apprehension by many, especially when one considers the negative aspect of libertarian theory which led to the negative occurrences upon the introduction of Bitcoin and the doors that this cryptocurrency opened to the criminal underworld.²¹

1.2 An Introduction to Bitcoin, Altcoins and Currency

The concept of the Bitcoin, the first actualisation of the idea of the cryptocurrency, was first thought up by Satoshi Nakamoto²² - a pseudonym for an individual or group of individuals that are as yet unknown. There has been much speculation surrounding the real identity of Nakamoto. Many people have been singled out as being involved; most denying any sort of relationship with the pseudonym, whilst others who wished to be made known as the original inventor could not prove their connection.

1.2.1 Bitcoin

Bitcoin: A Peer-to-Peer Electronic Cash System²³ was published in October 2008 on the Metzger, Dowdeswell & Co website, a New York based computer security and infrastructure consulting firm that has a website dedicated to a specified cryptography mailing list. This publication detailed the ins and outs of Bitcoin, offering insight into what was to become a massive game changer. A mere three months later, in January 2009, Nakamoto released the first software for Bitcoin on SourceForge,²⁴ which is an open source community that allows any individual to modify or enhance the source code. This code is the part of software that laypeople never really see - the building blocks to the finalised software. This release also saw the first ever units of the Bitcoin cryptocurrency being released into the world.

²⁰ Robert McChesney, John Nichols, *The Death and Life of American Journalism: The Media Revolution That Will Begin the World Again* (Nation Books 2010) 119

²¹ The use of cryptocurrencies on certain websites hosted on the dark web (n2) has linked their use to the nefarious and illegal uses on the dark web through their reputation.

²² Nakamoto (n1)

²³ *ibid*

²⁴ Satoshi Nakamoto, 'Http://satoshinakamotome/2009/01/09/bitcoin-v0-1-released/#selection-1570-15716' (Http://satoshinakamotome/, 9 January 2009)<<http://satoshinakamoto.me/>> accessed 30 July 2017

The lead developer for the Bitcoin digital currency project, Gavin Andresen, was quoted in a 2011 Forbes article written by Andy Greenberg - a lead journalist on the subject of Bitcoin and the dark web - as saying that 'Bitcoin is designed to bring us back to a decentralized currency of the people...this is like better gold than gold.'²⁵ The article also describes the *raison d'être* behind Bitcoin, and captures the nature and ideals the creator of Bitcoin wanted to embrace:

Bitcoin is different: It wholly replaces state-backed currencies with a digital version that's tougher to forge, cuts across international boundaries, can be stored on your hard drive instead of in a bank, and – perhaps most importantly to many of Bitcoin's users – isn't subject to the inflationary whim of whatever Federal Reserve chief decides to print more money.²⁶

When we spend money, we generally spend a currency that is representative, that is to say that it is backed by central government and regulated through a central bank, where the system is closely monitored and the currency is state regulated. Historically, currencies were often based on tangible commodities like gold, but after some time, that changed and fiat money became the norm. Fiat money, the etymology of the word coming from the Latin to mean, 'it shall be', is currency that is backed by the government but not physically represented by a commodity such as gold. The value of this kind of currency is determined through the regular principles of economics that we are accustomed to today, that of supply and demand, rather than the price of the actual commodity that makes up the physical representation of the money.²⁷ One such example of fiat money would be the US Dollar, which has no intrinsic value in itself, and it is only valuable insofar as the goodwill of the Government that backs it. The US Dollar was not always fiat money – there was a time in history where it was backed by the correlating amount of gold and silver in the banks vaults. This changed after The Great Depression where they reduced the amount of gold and silver that backed each dollar and then entirely abolished the system in 1971.²⁸

²⁵ Andy Greenberg, 'Crypto Currency' (www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html, 20 April 2011) <<https://www.forbes.com/forbes/>> accessed 30 July 2017

²⁶ *ibid*

²⁷ Investopedia, 'Fiat Money' ([Http://www.investopedia.com/terms/f/fiatmoney.asp](http://www.investopedia.com/terms/f/fiatmoney.asp)) <[http://www.investopedia.com/terms/f/fiatmoney.a](http://www.investopedia.com/terms/f/fiatmoney.asp) sp > accessed 30 July 2017

²⁸ 'Fiat money Economics' ([Https://www.britannica.com/topic/fiat-money](https://www.britannica.com/topic/fiat-money)) <<https://www.britannica.com/topic/fiat-money> > accessed 30 July 2017

In common language, it is often assumed that the term cryptocurrencies refers directly to Bitcoin. This is likely because for a long period of time, Bitcoin held the largest share in the cryptocurrency market – a fact that has changed dramatically during the writing of this thesis due to the exponential growth of Ether. At time of writing, Bitcoin holds just under 40% market share in the cryptocurrency market.²⁹ Although cryptocurrencies and Bitcoin are not interchangeable terms, since Bitcoin is one of the most popular and most widely known cryptocurrencies, any alternative currencies to Bitcoin are often referred to as altcoins.³⁰

This competitive nature of Bitcoin is evident through its constantly adapting and ever-changing code. This code is open source, a system similar to that used on Wikipedia, which means that anyone can view or edit the code. Each edit made to the code must be considered beneficial to the Bitcoin community at large before it reaches consensus. There is a core team of individuals who develop the Bitcoin code and should the users of the cryptocurrency view the changes favourably, then they will adopt those changes. In some cases, the jury remains out on what the ideal move forward is for Bitcoin, this happens in situations where there is no acquiescence from the community as to whether the new update is better than the old one. This can result in a fork of the network, and this scenario, although far from ideal, would not imply the end of Bitcoin.³¹ A fork in the network can best be described through example. In March 2013,

starting from block 225430, the blockchain literally split into two, with one half of the network adding blocks to one version of the chain, and the other half adding to the other. For the next six hours, there were effectively two Bitcoin networks operating at the same time, each with its own version of the transaction history. The split lasted for 24 blocks or 6 hours, finally resolving itself when one version of the chain conclusively pulled ahead of the other at

²⁹ Frank Chaparro, 'Ethereum's share of the cryptocurrency market has exploded' ([Http://www.businessinsider.com/ethereum-price-sends-marketcap-sky-high-vs-bitcoin-price-marketcap-2017-7](http://www.businessinsider.com/ethereum-price-sends-marketcap-sky-high-vs-bitcoin-price-marketcap-2017-7), 13 July 2017) <<http://www.businessinsider.com/ethereum-price-sends-marketcap-sky-high-vs-bitcoin-price-marketcap-2017-7>> accessed 30 July 2017

³⁰ Josiah Wilmoth, 'What is an Altcoin?' ([Https://www.cryptocoinsnews.com/altcoin/](https://www.cryptocoinsnews.com/altcoin/), 2014) <<https://www.cryptocoinsnews.com/altcoin/>> accessed 30 July 2017

³¹ Vitalik Buterin, 'Bitcoin Network Shaken by Blockchain Fork' ([Https://bitcoinmagazine.com/articles/bitcoin-network-shaken-by-blockchain-fork-1363144448/](https://bitcoinmagazine.com/articles/bitcoin-network-shaken-by-blockchain-fork-1363144448/), 12 March 2013) <<https://bitcoinmagazine.com/articles/bitcoin-network-shaken-by-blockchain-fork-1363144448/>> accessed 30 July 2017

block 225454, leaving the other chain largely abandoned, with only a small number of miners that are incapable of recognizing what has now become the main chain still mining it, while the bulk of the network quickly returned to normal.³²

1.2.2 Altcoins

The term altcoin is an abbreviation of the term Bitcoin alternative and they are regarded as such because they are often created with the aim of improving upon a certain facet or facets of the technology behind the Bitcoin.³³ There are hundreds of altcoins currently in existence, although few seem to have the vociferous backing and endorsement through public opinion and use that Bitcoin has managed to garner over the years. Another main contender would be Ether,³⁴ which as described above, has garnered a larger share of the cryptocurrency market as of late. The main selling point of these altcoins is that they are innovative, in the way that they experiment more freely, as they have less people to please, and they often do this by including different features not currently offered by Bitcoin. These changes vary from altcoin to altcoin, likely taking cues from their users and online platforms such as Reddit. Dash,³⁵ formerly known as Darkcoin, aspires to set the stage for completely anonymous transactions,³⁶ whereas Ripple ensures that inter-currency payments are made with ease.³⁷ Although from the outset it may seem as though having mildly altered replicas of the technology is futile and useless in the grand scheme of things, these altcoins serve to further decentralise the cryptocurrency community, whilst ensuring that Bitcoin remains competitive and innovative in its technologies.

³² ibid

³³ Wilmoth (n30)

³⁴ “Ether is a necessary element -- a fuel -- for operating the distributed application platform Ethereum. It is a form of payment made by the clients of the platform to the machines executing the requested operations. To put it another way, ether is the incentive ensuring that developers write quality applications (wasteful code costs more), and that the network remains healthy (people are compensated for their contributed resources).” Ethereum foundation (stiftung ethereum), zug, switzerland, 'Ether the Crypto-fuel for the Ethereum Network' (<https://www.ethereum.org>) <<https://www.ethereum.org/>> accessed 30 July 2017

³⁵ The dash network, 'Dash is Digital Cash. A revolutionary digital money system. Meet Digital Cash. Get Dash. 12.1 Update' (<https://www.dash.org>, 2017) <<https://www.dash.org/>> accessed 30 July 2017

³⁶ Eric Sammons, 'Dash, the anonymous evolution of Bitcoin' (<https://bravenewcoin.com/news/dash-the-anonymous-evolution-of-bitcoin/>, 29 April 2016) <<https://bravenewcoin.com/>> accessed 30 July 2017

³⁷ Ripple, 'Enabling the Internet of Value' <<https://ripple.com/>> accessed 30 July 2017

1.2.3 The Value of Bitcoin

It is important to assess the differentiation between the functionality of cryptocurrencies (like Bitcoin) and other currencies. Stephen Kinsella, a senior lecturer in economics at the University of Limerick and an Irish journalist, has been quoted as saying:

Bitcoin has no use value, only exchange value, and because it has no worth in use other than what others are willing to pay for it, it is always in a bubble: these happen when prices of assets get dislodged from their fundamental value. So Bitcoin is the perfect bubble.³⁸

This perfectly encompasses the way in which the people who own it utilise Bitcoin. In reality, the dollar is no different in this regard, as it also follows a pattern of demand and supply.³⁹ The difference arises in the fact that the currency is not supported by any one state, which, in turn, means that there is less of a demand for Bitcoin as no one is obliged to use it in their transactions (unlike how the Maltese obliged to use the euro when making a payment to any government department in Malta, for example). That being said, some companies have created a system whereby cryptocurrencies may be accessed via a tangible visa card that any individual can keep and use wherever visa is accepted – this will be explored further in Chapter Four. Moreover, there are certain retailers that have started to accept Bitcoin around the world.⁴⁰

Another important avenue when referring to the differences between a cryptocurrency like Bitcoin and a regular currency like the dollar, is the concept of seigniorage. This is 'the profit governments derive because the cost of minting coins or printing paper money is less than the market value of the money - the face value of the money minus the cost of physically making it.'⁴¹ Seigniorage is, of course, profitable to the state, and this source of revenue would be lost should the money being used through state backing be replaced by any altcoin or cryptocurrency.

³⁸ Stephen Kinsella, 'Once bitten twice shy, so stay away from Ponzi-like Bitcoins' (<http://www.independent.ie/opinion/columnists/stephen-kinsella/stephen-kinsella-once-bitten-twice-shy-so-stay-away-from-ponzilike-bitcoins-29764982.html>, 19 November 2013) <<http://www.independent.ie/opinion/>> accessed 30 July 2017

³⁹ Adam Hayes, 'Economics Basics: Supply and Demand' (<http://www.investopediacom/university/economics/economics3asp>) <<http://www.investopedia.com/>> accessed 30 July 2017

⁴⁰ Elise Moreau, '7 Major Retailers and Services That Accept Bitcoin' (<https://www.lifewire.com/big-sites-that-accept-bitcoin-payments-3485965>, 28 June 28 2017) <<https://www.lifewire.com/>> accessed 30 July 2017

⁴¹ 'Definition of seigniorage' (<http://lexiconft.com/term?term=seigniorage>) <<http://lexicon.ft.com/>> accessed 30 July 2017

1.2.4 The Price of Bitcoin

The price of Bitcoin is volatile – this is explained through the fact that, proportionately to other currencies, there are far fewer Bitcoin users, and any large purchases or sales of the currency can cause quite a ripple effect on the currency. Antithetically, the same purchases or sales of a currency that is stronger and has more of a foothold, like the Euro for example, would not fall victim to the same magnitude of fluctuations. In fact, on 22 May 2010, Mr. Hanyecz made the first real-world Bitcoin transaction by buying two pizzas in Florida for 10,000 BTC⁴² - with some individuals losing a large number of bitcoins and simply shrugging it off. Since that time, the price has increased, and, at time of writing, the price of one BTC was \$2777.65.⁴³ When attempting to determine Bitcoin's future in relation to its volatility, it is important to keep in mind that fact that the past volatility can mostly be attributed to the currency's rapid growth. Once this inevitably slows down, it would be a fair assumption that the volatility will also decrease.

1.2.5 The Possibility of a Bitcoin Exchange

In the early months of 2017, the American Securities and Exchange Commission (SEC) denied two applicants the possibility of having a Bitcoin ETF.⁴⁴

An Exchange Traded Fund (ETF) is a marketable security that tracks an index, a commodity, bonds, or a basket of assets like an index fund. Unlike mutual funds, an ETF trades like a common stock on a stock exchange. ETFs experience price changes throughout the day as they are bought and sold. ETFs typically have higher daily liquidity and lower fees than mutual fund shares, making them an attractive alternative for individual investors. Because it trades like a stock, an ETF does not have its net asset value calculated once at the end of every day like a mutual fund does.⁴⁵

⁴² Coindesk.com, (*CoinDesk*) accessed 30 July 2017

⁴³ Real-time Bitcoin Price Charts <<https://www.coindesk.com/price/>> accessed 30 July 2017

⁴⁴ 44 'SECURITIES AND EXCHANGE COMMISSION (Release No 34-80206; File No SR-BatsBZX-2016-30)' (https://www.secgov/rules/sro/batsbzx/2017/34-80206pdf, 10 March 2017) <<https://www.sec.gov/>> accessed 30 July 2017

⁴⁵ Exchange-Traded Fund (ETF)' (<http://www.investopediacom/terms/e/etfasp>) <<http://www.investopedia.com/>> accessed 30 July 2017

Needless to say, this would have had boundless implications for the future of Bitcoin had it been approved to be traded as an ETF. The SEC refused the application for a Bitcoin-tied Exchange Traded Fund stating,

Based on the record before it, the Commission believes that the significant markets for Bitcoin are unregulated. Therefore, as the Exchange has not entered into, and would currently be unable to enter into, the type of surveillance-sharing agreement that has been in place with respect to all previously approved commodity-trust ETPs—agreements that help address concerns about the potential for fraudulent or manipulative acts and practices in this market - the Commission does not find the proposed rule change to be consistent with the Exchange Act.⁴⁶

This action caused the value of Bitcoin to plummet by 18%, after a record high earlier in the same day.⁴⁷ The SEC is, at time of writing, in the process of reconsidering the application for the Bitcoin ETF.⁴⁸ As of April 2017, the SEC is also debating whether to allow the possibility of an Ether-based ETF. At time of writing, this has yet to be decided.⁴⁹

The fact that Bitcoin is a digital currency implies that it can be traded or invested, and sometimes even stolen.⁵⁰ Bitcoin is generated through a complex process called mining, which, without an adequate CPU, can be a long, arduous process. Many people who would like to get involved in the process of owning or trading Bitcoin often start by exchanging regular currency for Bitcoin at a Bitcoin exchange. Thus far, Bitcoin can be likened to any regular currency, but how is Bitcoin valued? In the case of a regular currency, the value of the currency is dependent on inflation and on the economy of the country amongst other things,⁵¹ but this does not apply to the nature of Bitcoin, and hence, this is where the two

⁴⁶ *ibid* 45

⁴⁷ Laura Shin, 'SEC Rejects Winklevoss Bitcoin ETF, Sending Price Tumbling' (<https://www.forbes.com/sites/laurashin/2017/03/10/sec-rejects-winklevoss-bitcoin-etf-sending-price-tumbling/#4a64e0a643c8>, 10 March 2017) <<https://www.forbes.com/sites/laurashin/>> accessed 30 July 2017

⁴⁸ William Suberg, 'Bitcoin ETF Reconsidered by SEC, Ethereum ETF Version May Be Approved' (<https://cointelegraph.com/news/bitcoin-etf-reconsidered-by-sec-ethereum-etf-version-may-be-approved>, 26 April 2017) <<https://cointelegraph.com/>> accessed 30 July 2017

⁴⁹ Stan Higgins, 'The SEC is Now Weighing an Ethereum ETF Proposal' (<https://www.coindesk.com/sec-now-weighing-ethereum-etf-proposal/>, 25 April 2017) <<https://www.coindesk.com/>> accessed 30 July 2017

⁵⁰ In 2013 the US Authorities seized \$5 million belonging to Mt. Gox – a global Bitcoin exchange. This situation and the publicity it brought with it have contributed to the negative reputation surrounding mainstream cryptocurrency use.

⁵¹ Investopedia staff, 'The Effects of Currency Fluctuations On The Economy' ([Http://www.investopediacom/articles/forex/080613/effects-currency-fluctuations-economyasp](http://www.investopediacom/articles/forex/080613/effects-currency-fluctuations-economyasp)) <<http://www.investopedia.com/>> accessed 30 July 2017

concepts differ. The principle of supply and demand is applicable to a myriad of elements in the sphere of economics, and the price determination of Bitcoin is one of them. When the demand for Bitcoin increases, then the price of bitcoins increases and vice versa. Currently, there is only a limited number of Bitcoin in circulation and because of the process of mining; the influx of new bitcoins into the market is predictable.⁵² The rate at which bitcoins are being mined is decreasing and this fact, coupled with the fact that the Bitcoin market is less popular than regular markets (such as that of the euro or the dollar), the market price is more volatile, and any single shift can create quite a ripple effect in this small bubble.⁵³

This exchange rate volatility came about through the use of an independent monetary policy and free capital flow being prioritised over Bitcoin having a fixed exchange rate.⁵⁴ There is a concept of international economics, known as the Impossible Trinity, which states that it is impossible to have all three of the aforementioned qualities subsisting simultaneously. As explained by Pierre Rochard in his article 'The Bitcoin Central Bank's Perfect Monetary Policy', the interest rates of Bitcoin are calculated based on the:

arbitrage between the expected return of holding Bitcoin versus the expected return of lending them out. The expected return of holding Bitcoin is completely tied to its expected future exchange rate because Bitcoin are currently a pure vehicle currency.⁵⁵

He also observes that, since many Bitcoin owners have higher expectations for the exchange rates than borrowers are generally willing to pay, there exists a de facto trend that bitcoins 'will continue to be hoarded and Bitcoin-denominated credit markets will continue to be under-developed until either the expectations of Bitcoin-holders adjust downward or are met.'⁵⁶

⁵² JP Buntinx, 'Bitcoin Mining Difficulty Increases by 1664%' (<https://themerkle.com/bitcoin-mining-difficulty-increases-by-16-64/>, 24 January 2017) <<https://themerkle.com/>> accessed 30 July 2017 □□□□

⁵³ Bitcoin.org, (*Bitcoin.org*) accessed 30 July 2017

⁵⁴ Pierre Rochard, 'The Bitcoin Central Bank's Perfect Monetary Policy' (<http://nakamotoinstitute.org/mempool/the-bitcoin-central-banks-perfect-monetary-policy/#selection-117-1723>, 15 December 2013) <<http://nakamotoinstitute.org/>> accessed 30 July 2017

⁵⁵ *ibid*

⁵⁶ *ibid*

1.2.6 Mining Bitcoin

Bitcoin, unless purchased from a trader, can only be attained through the process of mining. Mining is essentially when an individual chooses to use their computer-generated power to solve puzzle-like algorithms.⁵⁷ These algorithms are referred to as blocks. Once a block has been decrypted, or solved, Bitcoin is transferred to the owner of the CPU.⁵⁸ The issue here is that at the inception of Bitcoin, it used to take a regular person with a regular computer a short amount of time to crack the code and decipher a block,⁵⁹ nowadays, with the current situation, it takes a dedicated person with a very powerful processor a long time to crack a single block. This means that the amount of computer power spent on the processing of transactions is higher. Mining is also related to the decentralised aspect of Bitcoin and the blockchain, which shall be tackled in Chapter Two.

Bitcoin mining is something that can be done by anyone. As explained previously, it used to be far simpler to mine Bitcoin as the power required to mine a single Bitcoin was less than it is nowadays, but this has not deterred interest. Mining requires the miner to purchase specialised hardware on which to run specific mining software.⁶⁰ This software alerts itself to transactions taking place through the network and works to process and confirm these transactions.⁶¹ The way miners get paid is through the transaction fees that the users can opt to shell out in order to have a transaction processed faster, and the new bitcoins come to exist through a fixed formula, which is why the market growth is so predictable.⁶²

Transactions are confirmed in a block, which then forms part of the blockchain (an in-depth analysis of which will take place in Chapter Two) and this block requires the software to publish the formulae that were required to crack the algorithm along with it.⁶³ This proof is required in order to guarantee the chronology of the blockchain, an aspect of the blockchain that has tremendous repercussions. These are the calculations that have made Bitcoin harder to generate, as they have become harder to solve. They require the miner (or rather, the miner's software) to attempt various calculations at incredible speeds. When more people start to mine, the network increases the difficulty of solving the algorithm in order to ensure

⁵⁷ 'How Bitcoin Mining Works' (<https://www.coindesk.com/information/how-bitcoin-mining-works/>, 22 December 2014) <<https://www.coindesk.com/>> accessed 30 July 2017

⁵⁸ *ibid*

⁵⁹ Bitcoin.org (n53)

⁶⁰ 'How Bitcoin Mining Works' (n57)

⁶¹ *ibid*

⁶² *ibid*

⁶³ *ibid*

that the average time spent doing these calculations remains ten minutes. Hence, mining has become an incredibly competitive and somewhat lucrative business that many individuals are investing in.⁶⁴

More bitcoins are created upon the discovery of a new block through the aforementioned means. The rate at which a miner may discover a block is adjusted periodically, and it is set to decrease over time so much so that the maximum number of bitcoins in existence is set to not exceed 21 million.⁶⁵ The reason behind this specific figure is not definitive, but speculation from industry insiders follows the rationale that it matches the schedule at which the blocks are halved (the process by which mining is made more difficult). Satoshi Nakamoto has never confirmed or denied these speculative answers. This decreasing supply algorithm was chosen as it emulates the rate at which regular commodities such as gold are mined.⁶⁶

The fixed interval of blocks is the basis for the fact that each time a miner discovers a new block, the reward is halved.⁶⁷ The exact time at which the reward will be halved is not scientifically accurate, as it is a mere assumption-based prediction. It is estimated that the last Bitcoin will be mined in the year 2140.⁶⁸

1.2.7 The Double Spend Problem

An oft-cited problem with cryptocurrencies is the double spend problem. This entails the risk that an individual might concurrently send one unit of currency to two different sources. 'A currency system in which value comes apart from the currency itself is useless.'⁶⁹ With fiat currency, the double-spend problem is an unlikely scenario, due to its tangible nature, and information about the whereabouts of a physical currency is hard to misrepresent. This is not the case with cryptocurrencies.

⁶⁴ Bitcoin.org (n53)

⁶⁵ Stackexchange.com, (*Stackexchange.com*, x) accessed 30 July 2017

⁶⁶ Kiran Vaidya, 'Economics of Bitcoin' (<https://medium.com/all-things-ledger/economics-of-bitcoin-fc4e1fd46864>, 11 December 2016) <<https://medium.com/>> accessed 30 July 2017

⁶⁷ Jacob Donnelly, 'What is the 'Halving'? A Primer to Bitcoin's Big Mining Change' (<https://www.coindesk.com/making-sense-bitcoins-halving/>, 12 June 2016) <<https://www.coindesk.com/>> accessed 30 July 2017

⁶⁸ StackExchange (n65)

⁶⁹ Erik Bonadonna, 'Bitcoin and the Double-Spending Problem' (<http://blogs.cornell.edu/info4220/2013/03/29/bitcoin-and-the-double-spending-problem/>, 29 March 2013) <<http://blogs.cornell.edu/>> accessed 30 July 2017

‘When digital currency is exchanged, there is a very real possibility that the currency could be copied over to the recipient, with the “original” still intact in the owner’s possession.’ Without the means to prevent this double-spend problem, recipients of cryptocurrencies would not have the necessary protection safeguards in place, and this might render the use of cryptocurrencies somewhat futile.

The decentralised nature of the Bitcoin meant that, initially, people were sceptical of its safeguards against this problem. Nakamoto’s foresight led him to ensure that every transaction is verified before its conclusion. It is this verification, that is undertaken by the miners, that ensures a solution to the double spend problem.

Bitcoin was created in the darkest days of the financial crisis.⁷⁰ A commonly understood principle of economics is that if there is too much influx of currency at one time, the value of the currency will drop, but if there is too slow a growth of the currency it will also be negative.⁷¹ Bitcoin was designed to be a self-stabilising economy.⁷²

1.3 The Dark Web and Dark Markets

The Internet is larger than we know or can totally process and the World Wide Web that we are privy to in our daily lives comprises approximately 4% of the total Internet, whilst the other 96% is made up of what is known as the deep web.⁷³ This invisible Internet is not commonly used by the general proponents of the Internet, but is usually left to a more specific subset of people, often linked to nefarious activity.⁷⁴ The scepticism surrounding the mainstream use of the components of the dark web – which will be delved into below – (components in this context should be taken to mean those other concepts that are closely linked but still external to) can likely be blamed on the high percentage of illegal activity that takes place through the sites. This can be likened to the concept of torrenting. Torrenting is not illegal per se, but the bad reputation it has garnered, is likely due to the fact that most people use it for illegal means, such as pirating media.

⁷⁰ Blythe Masters, 'Cryptocurrency a Response to Financial Crisis' (<http://www.wsj.com/video/cryptocurrency-a-response-to-financial-crisis-says-ceo/D28A8012-413F-447E-AA5A-F1911BA64FC3.html>, 14 June 2016) <<http://on.wsj.com/>> accessed 30 July 2017

⁷¹ Vaidya (n66)

⁷² *ibid*

⁷³ Zach Epstein, 'How to find the Invisible Internet' (<http://bgr.com/2014/01/20/how-to-access-tor-silk-road-deep-web/>, 20 January 2014) <<http://bgr.com/>> accessed 30 July 2017

⁷⁴ The Silk Road (n2)

The deep web and the dark web are not interchangeable terms. Whilst the dark web makes up a small portion of the deep web, both the dark web and the deep web cannot be accessed by conventional search engines.⁷⁵ The dark web refers to the encrypted network that exists between Tor servers and their subscribing clientele.⁷⁶

Generally, the dark web is used by a myriad of individuals, from cypherpunks and staunch advocates for privacy, whistleblowers, dissidents, hackers, drug dealers, pornography distributors – including the even more sinister child pornography distributors, investigative reporters and journalists, and many other types of individuals who find it convenient to make use of this cloak of anonymity.⁷⁷ The dark web has often been implicated in a significant amount of incredibly varied illegal activity, from drug smuggling to terrorist recruitment, the sale of illegal merchandise like human organs, blood diamonds, ivory and the distribution of illegal weaponry.⁷⁸

The Silk Road, founded at the start of 2011, is one of the more popular websites that can be found on the dark web. The trades and exchanges that take place on the Silk Road marketplace are frequently criminal in their nature, and the goods and services offered on the site range from narcotics and weaponry to the more sinister gun for hire placements or schematics for nefarious 3D printouts (such as weaponry).⁷⁹ Much of the hesitation surrounding the adoption of Bitcoin on a mainstream level as well as the use of the dark web in itself can likely be traced back to the amount of news articles and arrests that came from that era of the Internet.

Testament to the illicit nature of the Silk Road, is evident through a simple Google search of “the silk road” where, on the first page of links, one finds a website called thesilkroaddrugs.org, which is no misnomer.⁸⁰ The persistent nature of Silk Road is evident through the fact that it has been shut down many times by American authorities and has always found a way to resurface, This is mainly due to the fact that the individuals behind Silk Road are very good at what they do, and with each new seizure, shut down or FBI raid,

⁷⁵ *ibid*

⁷⁶ *ibid*

⁷⁷ Wendy Boswell, 'Who Uses the Dark Web, and Why?' (<https://www.lifewire.com/who-uses-dark-web-3481563> , 16 March 2017) < <https://www.lifewire.com/> > accessed 30 July 2017

⁷⁸ Don Reisinger, 'The Things You Can Buy on the Dark Web Are Terrifying' ([Http://fortune.com/2015/12/07/crime-underground-web/](http://fortune.com/2015/12/07/crime-underground-web/) , 7 December 2015) <<http://fortune.com/>> accessed 30 July 2017

⁷⁹ *ibid*; and The Silk Road (n2)

⁸⁰ 'A Guide to Accessing the Silk Road Reloaded' ([Https://silkroaddrugs.org/a-guide-to-accessing-the-silk-road-reloaded/](https://silkroaddrugs.org/a-guide-to-accessing-the-silk-road-reloaded/)) <<https://silkroaddrugs.org>> accessed 30 July 2017

they upgrade the software, add extra security measures and attempt to evade capture. The first take down of Silk Road happened in 2013, it was re-launched as Silk Road 2.0 in 2014, shut down again and re-launched again as Silk Road 3.0 – the latter still being online⁸¹. Ross William Ulbricht, who went by the pseudonym “Dread Pirate Roberts”, was arrested for his connection with Silk Road, and is currently serving a life sentence without the possibility of parole in a New York prison.⁸² He was accused of running Silk Road as well as a multitude of other crimes in connection to his lucrative business.⁸³ The list of charges brought against Ulbricht included narcotics trafficking conspiracy, computer hacking conspiracy and money laundering conspiracy.⁸⁴ Ulbricht is also alleged to have enlisted a user of the Silk Road to murder another user who was threatening to release the supposedly anonymous identities of the users of the Silk Road.⁸⁵

Although this anecdote may seem like a tangent from the concept of cryptocurrencies and Bitcoin, the history behind their popularity is integral to their thorough understanding. The correlation between Silk Road and Bitcoin is that the former is partially responsible for the popularity of Bitcoin in online marketplaces, being one of the first sites to accept Bitcoin as payment.⁸⁶

The fact that the Silk Road and other dark net markets accept Bitcoin as payment is not a mere coincidence. Bitcoin affords the proponents of these markets a level of anonymity that could not otherwise be guaranteed. The anonymous nature of the dark web is what allows it to function at peak capacity, ensuring a no-paper trail purchase through the use of VPNs, Tor and Bitcoin. The author is of the opinion that it is these three elements combined that allow for the perfect storm of avoidance of consequences with regard to certain illegal transactions and services that take place on the dark web.

⁸¹ Jessica Roy, 'Feds Raid Online Drug Market Silk Road' (<http://nationtimecom/2013/10/02/alleged-silk-road-proprietor-ross-william-ulbricht-arrested-3-6m-in-bitcoin-seized/> , 2 October 2013) <<http://nation.time.com/>> accessed 30 July 2017

⁸² United States Court of Appeals, Second Circuit. United States of America, Appellee, v. Ross William Ulbricht, a/k/a Dread Pirate Roberts, a/k/a Silk Road, a/k/a Sealed Defendant 1, a/k/a DPR, Defendant-Appellant. Docket No. 15-1815; Decided: May 31, 2017

⁸³ *ibid*

⁸⁴ *ibid*

⁸⁵ Criminal Chargesheet for Ross William Ulbricht, 13MAG2328, Southern District of New York, 27th September 2013

⁸⁶ The Silk Road (n2)

1.4 The Relationship between the Dark Web and cryptocurrencies

There exists a somewhat symbiotic relationship between the dark web and cryptocurrencies, which can be explained through the way in which cryptocurrencies are used and the reasons for their use on the dark web and subsequently on the aforementioned dark markets. The deep web is built to allow encrypted end-to-end communications named “The Onion Router”, “The Onion Network” or Tor.⁸⁷ According to their website, “The Tor network is a group of volunteer-operated servers that allows people to improve their privacy and security on the Internet.”⁸⁸ Tor's users employ this network by connecting through a series of virtual tunnels rather than making a direct connection, thus allowing both organisations and individuals to share information over public networks without compromising their privacy.⁸⁹ Along the same lines, Tor is an effective censorship circumvention tool, allowing its users to reach otherwise blocked destinations or content. Tor can also be used as a building block for software developers to create new communication tools with built-in privacy features.”⁹⁰

Tor was originally funded by the US Office of Naval Research in 1995, and was then further developed by the Defense Advanced Research Projects Agency (DARPA) in 1997.⁹¹ Sometime later, the Tor network became a reality and reached the sphere of mainstream usage. According to Joseph Babatunde Fagoyinbo in his book titled ‘The Armed Forces: Instrument of Peace, Strength, Development and Prosperity’, the

Onion network involves adding a layer of encryption for each router node along the path that operator's data travel: each encryption layer being peeled back one at a time by routers along the way. Each router unpeels a single layer to get instructions on where to send the data packets next, but cannot see where the data packets have come from. None of these nodes knows the

⁸⁷ “The Tor network is a group of volunteer-operated servers that allows people to improve their privacy and security on the Internet. Tor's users employ this network by connecting through a series of virtual tunnels rather than making a direct connection, thus allowing both organizations and individuals to share information over public networks without compromising their privacy. Along the same line, Tor is an effective censorship circumvention tool, allowing its users to reach otherwise blocked destinations or content.” <https://www.torproject.org/about/overview.html.en>

⁸⁸ *ibid*

⁸⁹ *ibid*

⁹⁰ *ibid*

⁹¹ Joseph Babatunde Fagoyinbo, *The Armed Forces: Instrument of Peace, Strength, Development and Prosperity* (May 2013)

origin of those packets, nor the ultimate destination, nor does it have access to the contents of data transfer.⁹²

1.5 A Comparative Analysis of the Legality of Cryptocurrencies

1.5.1 Introduction

Currently, there exists an international lack of regulatory coherence in the way in which cryptocurrencies are tackled – or rather, not tackled – by countries all around the world. There are some countries around the world where cryptocurrencies are regulated, some have restricted their use or banned them entirely, whilst others have legislated for and authorised their use.

Despite this, many of the regulatory bodies around the globe are setting guidelines and putting rules in place in order to make individuals and businesses aware of the various ways through which these new technologies could be used in the sphere of online gambling once combined with the standard financial system already in place.

1.5.2 Malta

Joseph Cuschieri, the Chairman of the Malta Gaming Authority has stated that

Cryptocurrencies are an attempt to create a virtual currency, backed up by a technology block-chain that manages its transactions. I still see it as a risk, and the authority's position is that we still do not accept crypto-currencies. The authority has received very few requests to accept cryptocurrencies, and we have always refused- we are looking to adopting a national approach and given it's a financial instrument we shall be collaborating with the Central Bank, the FIAU and the MFSA.⁹³

⁹² ibid

⁹³ Paul Cocks, 'Aiming to make Malta the Silicon Valley of gaming' ([Http://www.maltatoday.com.mt/business/business_news/68155/aiming_to_make_malta_the_silicon_valley_of_gaming#WX3smcaB2Ru](http://www.maltatoday.com.mt/business/business_news/68155/aiming_to_make_malta_the_silicon_valley_of_gaming#WX3smcaB2Ru), 4 August 2016) <<http://www.maltatoday.com.mt/>> accessed 30 July 2017

Cuschieri also sees a very positive future for Malta at the helm of the industry, stating that ‘my vision is for Malta to become the Silicon Valley of the industry, and I think we are getting there.’⁹⁴

This willingness to move forward with the Maltese framework for Bitcoin and other cryptocurrencies requires an analysis of the issues that one might find in doing so. Currently, Malta has not made any steps to regulate cryptocurrencies, although Prime Minister Joseph Muscat stated at a conference in August 2017 that he would like to see Malta at the forefront of the sector, ‘The rise of cryptocurrencies can be slowed but cannot be stopped...Some financial institutions are painstakingly accepting the fact that the system at the back of such transactions is much more efficient and transparent than the classical ones.’ He believes that,

rather than resist, European regulators should innovate and create mechanisms in which to regulate cryptocurrencies, in order to harness their potential and better protect consumers, while making Europe the natural home of innovators.⁹⁵

These words imply that the future of Maltese cryptocurrency regulation is on the horizon.

Currently, Malta does not have any laws that are specifically applicable to the concept of cryptocurrencies, and there is nothing in the Remote Gaming Regulations (RGR) that expressly bans the use of cryptocurrencies in gaming law, as the regulations were formed prior to the mainstream use of cryptocurrencies and hence are not included in the list of methods through which funds may be received under article 35(4) of the RGR as follows:

the licensee shall not accept cash from a player and funds may be received from the player only by any of the following methods: (i) credit cards; (ii) debit cards; (iii) electronic transfer; (iv) wire transfer; (v) cheques; (vi) any other method approved by the Authority.⁹⁶

The Malta Gaming Authority (MGA) does not approve of the use of cryptocurrencies in a Maltese scenario as they are yet unregulated. That being said, anything that is not specifically

⁹⁴ *ibid*

⁹⁵ Kevin Helms, 'Malta's Prime Minister says Europe should become the Bitcoin Continent' (<https://newsbitcoin.com/maltas-prime-minister-europe-bitcoin-continent/>), 24 February 2017) <<https://news.bitcoin.com/>> accessed 30 July 2

⁹⁶ Remote Gaming Regulations, Chapter 438.04 of The Laws of Malta, Article 35 (4)

illegal in a country is a de facto legality, in line with the recognised legal principle of *nulla poena sine lege*.

Seeing as Bitcoin is not deemed as a regulated instrument under the EU's Markets in Financial Instruments Directive 2004/39/EC⁹⁷, as yet, there are no licensing requirements for companies that deal in Bitcoin in order for them to obtain a licence from the Malta Financial Services Authority, in line with the Malta Investment Services Act, and become regulated in their activities⁹⁸.

The MGA is currently working towards finding a solution for the myriad of operators that wish to use cryptocurrencies. That being said, this was not always the case, as Maltese licensed operator Vera&John, who claimed to “have become the first regulated and licensed Internet casino to begin accepting the Bitcoin virtual currency”⁹⁹ were made to suspend their acceptance of the cryptocurrency after MGA intervention.¹⁰⁰

1.5.3 The United Kingdom

The UK Government has held that Bitcoin is not regulated under UK law, and as yet, the Bank of England remains skeptical of Bitcoin, although less so of the blockchain technology behind it, as stated by the Governor of the Bank of England in a statement released online:

The great promise of distributed ledgers for central banks is their potential to enhance resilience. Distributing the ledger means multiple copies of the system. It can continue to operate if parts get knocked out. That removes the single point of failure risk inherent in a centralised system.¹⁰¹

⁹⁷ Commission, Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council and repealing Council Directive 93/22/EEC

⁹⁸ Charles Cassar, 'Virtual Currencies: Risks and Regulations in Malta and Other Jurisdictions' [2015] EMLR IV

⁹⁹ 'Vera&John becomes first regulated online casino to accept Bitcoin' (<http://www.igamingbusiness.com/news/verajohn-becomes-first-regulated-online-casino-accept-bitcoin>, 30 January 2014) <<http://www.igamingbusiness.com/>> accessed 30 July 2017

¹⁰⁰ 'Vera&John suspends Bitcoin payment facility' (<http://www.igamingbusiness.com/news/verajohn-suspends-bitcoin-payment-facility>, 16 April 2014) <<http://www.igamingbusiness.com/>> accessed 30 July 2017

¹⁰¹ Ian Demartino, 'Bank of England Explores Blockchain, Says Digital Currency is Far Off' (<http://www.coindesk.com/bank-england-blockchain-digital-currency/>, 17 June 2016) <<http://www.coindesk.com/>> accessed 30 July 2017

In 2015, the UK Gambling Commission warned Bitcoin gambling sites that in order to provide UK residents the opportunity to gamble on their sites they require a licence, even if this happens to be done via a digital currency. It stated that:

The Commission neither prohibits nor encourages Bitcoin – we are interested only in ensuring the proper regulation of gambling products consumed in Britain. The currency is almost irrelevant as all operators need to satisfy themselves, and us, that they can fully meet all our requirements – particularly the requirements that ensure crime is kept out of gambling and consumers are protected.¹⁰²

In an April 2016 report entitled “Action Plan for Anti-Money Laundering and Counter-Terrorist Finance”, the UK treasury stated that:

This [focus on exchanges] is consistent with a risk-based approach, and we note that extending the perimeter of anti-money laundering regulations beyond digital currency exchange firms (for example to wallet providers) would not deliver any benefits in terms of mitigating money laundering and terrorist finance risk, and would place significant burdens on firms in this innovative and embryonic sector.¹⁰³

Arguably, no AML rules would be imposed upon digital currency wallet providers in order to allow for the sector to grow without this added burden. This resulted from research into the field of digital currencies and the stakeholders involved, and the same report highlighted the fact that evidence points to ‘a low level of illicit activity in digital currency networks’, which might be the reason for this rather lax approach¹⁰⁴.

¹⁰² Criz Hombrebueno, 'UK Gambling Commission warns bitcoin gambling websites' (<https://calvinayre.com/2015/07/01/business/uk-gambling-commission-warns-bitcoin-gambling-websites/>, 1 July 2015) <<https://calvinayre.com/>> accessed 30 July 2017

¹⁰³ HM Treasury HomeOffice, 'Action Plan for anti-money laundering and counter-terrorist finance', April 2016 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/517992/6-2118-Action_Plan_for_Anti-Money_Laundering__web_.pdf> accessed 30 July 2017

¹⁰⁴ Stan Higgins, 'UK Treasury Won't Seek AML Rules for Bitcoin Wallet Providers' (<http://www.coindesk.com/uk-treasury-we-wont-regulate-bitcoin-wallet-providers/>, 25 April 2016) <<http://www.coindesk.com/>> accessed 30 July 2017

1.5.4 The Isle of Man

In 2014, the Isle of Man started making headway in the regulation of cryptocurrencies,¹⁰⁵ a move that makes a lot of sense considering their dynamic position in the gaming law sector. The Financial Supervision Commission of the Isle of Man drafted a bill to attempt to regulate digital currencies and Anti-Money Laundering rules (AML).¹⁰⁶ As of 2015, digital currency operators must adhere to the AML laws already in force in the country through simple amendments in their Proceeds of Crime Act.¹⁰⁷

In 2016, the Isle of Man made strides towards changing its gambling regulations in order to allow gamblers to use cryptocurrencies as they would regular money.¹⁰⁸ In 2017, changes were made to the gambling regulations in order to afford the casinos that have been using Bitcoin the opportunity to become licensed and extend the protection of the players and the companies themselves through their removal from this grey area.¹⁰⁹

1.5.5 The United States

At the time of writing, the USA has yet to properly regulate the cryptocurrency industry. After the Government shut down the Silk Road,¹¹⁰ an investigation was launched by the Homeland Security and Governmental Affairs Committee of the Senate in order to assess the risks and issues that this type of technology brings with it.¹¹¹ The FBI commented on this and informed the Committee of its position, stating that it recognises virtual currencies as

¹⁰⁵ Lester Coleman, 'Bitcoin Gambling Approved in Isle of Man by Regulator' (<https://www.cryptocoinsnews.com/bitcoin-gambling-approved-in-isle-of-man-by-regulator/>), 1 May 2016) <<https://www.cryptocoinsnews.com/>> accessed 30 July 2017

¹⁰⁶ *ibid*

¹⁰⁷ *ibid*

¹⁰⁸ Daniel Williams, 'Isle of Man Could Become Key Blockchain Destination in Europe Due to Virtual Currencies Implementation' (<http://www.casinoguardian.co.uk/2017/01/24/isle-man-become-key-blockchain-destination-europe-due-virtual-currencies-implementation/>), 24 January 2017) <<http://www.casinoguardian.co.uk/>> accessed 30 July 2017

¹⁰⁹ *ibid*

¹¹⁰ Andy Greenberg, 'The Silk Road's Dark-Web Dream is Dead' (<https://www.wired.com/2016/01/the-silk-roads-dark-web-dream-is-dead/>), 14 January 2016) <<https://www.wired.com/>> accessed 30 July 2017

¹¹¹ Kavya Sukumar, 'Government eyes regulation of "Bitcoins"' (<https://www.usatoday.com/story/news/politics/2013/08/26/bitcoin-virtual-currency-regulations/2702653/>), 26 August 2013) <<https://www.usatoday.com/>> accessed 30 July 2017

‘legitimate financial services’¹¹² but understands that there are inherent risks attached to this advanced digital currency.

In 2013, the Financial Crimes Enforcement Network (FinCEN) issued non-binding guidelines on the applicability of some of the relevant regulations, requiring Bitcoin exchanges and miners to register as Money Service Businesses (MSBs) and hence apply certain AML rules¹¹³. This attempt was critiqued by industry insiders, one stating that ‘FinCEN is clearly trying, in its somewhat bumbling way, to squeeze a square technological peg into its round regulatory hole.’¹¹⁴

In the Bitcoin Savings and Trust case (BTCST) of 2013, the federal judge ruled on the question of whether such investments fell within the definition of ‘securities’ under US securities law.¹¹⁵ The judge ruled against the arguments of the defence that Bitcoin was not money and stated that it is subject to these US laws as it constitutes ‘a currency or form of money.’¹¹⁶

On 25 March 2014, the Internal Revenue Service (IRS) issued a notice providing that, for tax purposes, Bitcoin is to be considered property and not currency.¹¹⁷

To add further layers of incoherency to the matter, in a 2016 money laundering case, a Miami-Dade judge ruled that bitcoins cannot be equivalent to money, stating that ‘this Court is not an expert in economics, however, it is very clear, even to someone with limited

¹¹² 'Legitimate' Bitcoin's value soars after Senate hearing' (<http://www.bbc.com/news/technology-24986264> , 19 November 2013) < <http://www.bbc.com/> > accessed 30 July 2017

¹¹³ ‘Application of FinCEN’s Regulations to Persons Administering, Exchanging or Using Virtual Currencies’ (18 March 2013) FIN-2013-G001 <<https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf>> accessed 30 July 2017

¹¹⁴ Timothy B Lee, 'New Money Laundering Guidelines Are A Positive Sign For Bitcoin' (<https://www.forbes.com/sites/timothylee/2013/03/19/new-money-laundering-guidelines-are-a-positive-sign-for-bitcoin/#1e63993d33ad> , 19 March 2013) <<https://www.forbes.com/>> accessed 30 July 2017

¹¹⁵ *US Securities and Exchange Commission v. Trendon T. Shavers and Bitcoin Savings and Trust*, Civil Action No. Civil Action No. 4:13-CV-416

¹¹⁶ *ibid*

¹¹⁷ 'IRS Virtual Currency Guidance : Virtual Currency Is Treated as Property for US Federal Tax Purposes; General Rules for Property Transactions Apply' (<https://www.irs.gov/uac/newsroom/irs-virtual-currency-guidance> , 25 March 2014) <<https://www.irs.gov/>> accessed 30 July 2017

knowledge in the area, that Bitcoin has a long way to go before it the equivalent of money.¹¹⁸

The first step forward towards regulation in the US was the creation of the BitLicense in the state of New York,¹¹⁹ which attempts to regulate these cryptocurrencies by regulating the purveyors of them – the commercial operators as though they were regular financial operators (similarly to the way they were referred to in the 2013 FinCEN rules as aforementioned). This requires them to abide by AML and KYC regulations.¹²⁰

1.5.6 The European Union

There is currently no regulation on cryptocurrencies within the EU's legislative framework, although some regulation does exist in some member states. A few member states have issued guidelines, opinions or warnings regarding virtual currencies, often through their central banks or regulators. In this aspect, Germany has made some headway, considering virtual currencies to be units of account and not equivalent to legal tender.¹²¹

Seeing as the European Central Bank (ECB) is the central bank for the euro and it is also tasked with administering European Union monetary policy, its relative silence on this issue is somewhat concerning to the member states that look to the ECB as a point of reference for their monetary regulatory frameworks. The ECB has not yet included the regulation of cryptocurrencies within its competence, but since the member states' attempts to regulate or discuss them has resulted in so many varied responses, it is the opinion of the author that it would be ideal for the ECB to provide a position of clarity, in view of proper financial stability.

¹¹⁸ Kelly Phillips erb, 'Miami Judge Rules That Bitcoin Is Not Money' (<https://www.forbes.com/sites/kellyphillipserb/2016/07/27/miami-judge-rules-that-bitcoin-is-not-money/#7d0b11994a6d>, 27 July 2016) <<https://www.forbes.com/>> accessed 30 July 2017

¹¹⁹ Stan Higgins, 'New York Reveals BitLicense Framework for Bitcoin Businesses' (<http://www.coindesk.com/new-york-reveals-bitlicense-framework-bitcoin-businesses/>, 17 July 2014) <<http://www.coindesk.com/>> accessed 30 July 2017

¹²⁰ *ibid*

¹²¹ Tanja Aschenbeck-Florange, 'Regulation of Bitcoins in Germany: First comprehensive statement on Bitcoins by German Federal Financial Supervisory Authority (BaFin)' (<https://bitcoinmagazine.com/articles/regulation-bitcoins-germany-first-comprehensive-statement-bitcoins-german-federal-financial-supervisory-authority-ba-fin-1391637959/>, 5 February 2014) <<https://bitcoinmagazine.com/>> accessed 30 July 2017

The ECB has issued two reports on virtual currency schemes, one in 2012¹²² and an updated version in 2015.¹²³ In these reports, cryptocurrencies fall within the definition of ‘virtual currency schemes’ (VCS). The original 2012 definition of VCS was:

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 community¹²⁴

while the updated definition was adapted slightly to cater for the technological advancements in this field, removing the words ‘unregulated’ and digital ‘money’ to become ‘digital representation of value, not issued by a central bank, credit institution or e-money institution, which in some circumstances can be used as an alternative to money.’¹²⁵ This would automatically imply that cryptocurrencies are not to be considered as ‘money’.

The EU legal framework on payment services is comprised of the Electronic Money Directive (EMD1),¹²⁶ the Second Electronic Money Directive (EMD2),¹²⁷ the Payment Services Directive (PSD1)¹²⁸ and the Second Payment Services Directive (PSD2).¹²⁹ EMD2 was primarily aimed at bringing EU legislation up to date on these emerging technological advances in cryptocurrencies and ensuring that the laws on e-money institutions are in line with the obligations as set forth in the PSD2. Upon careful analysis of the definition of “E-money” as held in the PSD2, it is evident that EMD2 does not cater for the inclusion of cryptocurrencies within its ambit.

¹²² ECB (n7)

¹²³ European Central Bank, ‘Virtual Currency Schemes – a Further Analysis’ (2015) <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> > accessed 30 July 2017

¹²⁴ *ibid*

¹²⁵ *ibid*

¹²⁶ Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions

¹²⁷ Council Directive 2009/110/EC of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions [2009]OJL267/11

¹²⁸ Council Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC

¹²⁹ Council Directive 2015/2366 (EU) of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015]OJL319

The ECB held that Bitcoin ‘clearly falls outside the scope of the Payment Services Directive’¹³⁰ and this, by extension, can also be applied to an analysis of PSD2, which also appears to exclude cryptocurrencies from its scope of regulation, specifically because they are not a currency of a EU Member State.¹³¹

At the time of writing there has only been one European Court of Justice case that ruled on the issue of cryptocurrencies as ‘money’, and that was the 22 October 2015 case of *Skatteverket v David Hedqvist*.¹³² The question to be answered in this case was concerning whether transactions exchanging Bitcoin to fiat currency or vice versa ought to be subject to the VAT provisions. The ECJ ruled in the negative, and said that Member States were obliged to exempt any

transactions, including negotiation, concerning currency, bank notes and coins used as legal tender, with the exception of collectors’ items, that is to say, gold, silver or other metal coins or bank notes which are not normally used as legal tender or coins of numismatic interest.¹³³

The implications of this judgement are that Bitcoin is to be considered ‘money’ seeing as it falls within the definition as provided in the VAT Directive.¹³⁴

1.5.6.1 Luxembourg

The Commission de Surveillance du Secteur Financier issued a communication in 2014¹³⁵ affording Bitcoin and other cryptocurrencies the status of “currency”. Luxembourg issued their first BitLicence in October 2015.¹³⁶ It is the first EU member state to license a cryptocurrency exchange.

¹³⁰ ECB (n7)

¹³¹ ECB (n7)

¹³² *Skatteverket v David Hedqvist* (2015) ECJ C-264/14

¹³³ *ibid*

¹³⁴ Council Directive 2006/112/EC of 28 November 2006

¹³⁵ 'VIRTUAL CURRENCIES' [2014] Commission de Surveillance du Secteur Financier <http://www.cssf.lu/fileadmin/files/Publications/Communiques/Communiques_2014/Communique_virtual_currencies_140214.pdf> accessed 30 July 2017

¹³⁶ Cédric Buisine, 'First European BitLicense granted in Luxembourg' (<http://www.lexology.com/library/detail.aspx?g=c796229b-03be-446c-b777-7d89aef97726>, 30 November 2015) <<http://www.lexology.com/>> accessed 30 July 2017

1.5.6.2 Germany

The German financial regulatory authority, Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), have also begun to consider the regulatory implications of blockchain technology within their current framework. In early 2016 BaFin published an article entitled “Distributed Ledger: The technology behind virtual currencies: the example of blockchain” which promoted the idea of keeping a close eye on any advancements in order to best ascertain the risks of implementation of Distributed Ledger Technology.

1.5.7 Thailand

In 2013, the Thai Central Bank ruled that Bitcoin does not fall within the definition of ‘currency’¹³⁷. For a time, it was thought that Thailand had become the first country to ban Bitcoin, but the reality is slightly different. In 2013 Bitcoin Company Limited had attempted to petition the Thai Government to be able to use Bitcoin in Thailand, and set up a meeting with the Bank of Thailand in order to get the ball rolling.¹³⁸ Rather than making any headway in this regard, Senior officials from the Foreign Exchange Administration and Policy Department stated that: ‘due to lack of existing applicable laws, capital controls and the fact that Bitcoin straddles multiple financial facets...Bitcoin activities are illegal in Thailand.’¹³⁹

1.5.8 Other Jurisdictions

While most countries have yet to even legislate on the subject of virtual currencies, very few have afforded them some kind of legal status at all. There are only four countries that have outlawed these types of currencies: Bangladesh, Bolivia, Kyrgyzstan and Ecuador, to have made Bitcoin, and likely all other virtual currencies explicitly illegal. The Bangladesh Central Bank issued a statement in late 2014 stating ‘Bitcoin is not a legal tender of any country. Any

¹³⁷ 'Thailand's Bitcoin ban is not quite what it seems' (<https://qzcom/110164/thailands-infamous-bitcoin-crackdown-is-not-quite-what-it-seems/> , 31 July 2013)<<https://qz.com/>> accessed 30 July 2017

¹³⁸ Nathan Ingraham , 'Bitcoin tries to become a legal currency in Thailand, gets outlawed instead' (<https://www.theverge.com/2013/7/29/4569126/bitcoin-tries-to-become-legal-currency-in-thailand-gets-outlawed>, 29 July 2013) <<https://www.theverge.com/>> accessed 30 July 2017

¹³⁹ Saiyai Sakawee, 'Bank of Thailand tells citizens not to use Bitcoin to buy products or services because it's not a currency' (<https://www.techinasia.com/bank-thailand-tells-citizens-bitcoin-buy-products-services-currency>, 18 March 2014) <<https://www.techinasia.com/>> accessed 30 July 2017

transaction through Bitcoin or any other cryptocurrency is a punishable offence.’¹⁴⁰ In Bolivia, in 2014, the central bank released an unequivocal statement that, ‘it is illegal to use any kind of currency that is not issued and controlled by a government or an authorised entity.’¹⁴¹ In July 2014, the National Bank of the Kyrgyz Republic issued a statement that:

‘At the same time we should not forget that under the legislation of the Kyrgyz Republic the sole legal tender on the territory of our country is the national currency of Kyrgyzstan ‘som.’ And the use of ‘virtual currency’, bitcoins, in particular, as a means of payment in the Kyrgyz Republic will be a violation of the law of our state.’¹⁴²

1.6 Conclusion

The future of cryptocurrencies around the world is yet to be properly seen, and we can only hope for adequate regulation, so that individuals may be safeguarded against the riskier and more nefarious facets of these cryptocurrencies.

One way states are attempting to make headway is through the introduction of regulatory sandboxes, which “usually implement a set of rules that allow trailblazers to test their products and business models in a live environment with minimal legal requirements. The majority of these programs come with predefined restrictions, such as limitations on clients, time-limit testing, predetermined exceptions, and testing under regulator supervision. Their purpose is to minimize legal uncertainty, improve access to investment, and create rules for new products and business models.”¹⁴³ There are many trailblazing countries already making

¹⁴⁰ Why Bangladesh will jail Bitcoin traders' ([Http://www.telegraph.co.uk/finance/currency/11097208/Why-Bangladesh-will-jail-Bitcoin-traders.html](http://www.telegraph.co.uk/finance/currency/11097208/Why-Bangladesh-will-jail-Bitcoin-traders.html) , 15 September 2014) <<http://www.telegraph.co.uk/>> accessed 30 July 2017

¹⁴¹ Anthony Cuthbertson, 'Cryptocurrency Round-Up: Bolivian Bitcoin Ban, iOS Apps & Dogecoin at McDonald's' ([Http://www.ibtimes.co.uk/cryptocurrency-round-bolivian-bitcoin-ban-ios-apps-dogecoin-mcdonalds-1453453](http://www.ibtimes.co.uk/cryptocurrency-round-bolivian-bitcoin-ban-ios-apps-dogecoin-mcdonalds-1453453) , 20 June 2014) <<http://www.ibtimes.co.uk/>> accessed 30 July 2017

¹⁴² The National Bank of the Kyrgyz Republic, 'Warning of the National Bank of the Kyrgyz Republic on the spread and use of the “virtual currency”, in particular, bitcoins (bitcoin)' ([Http://www.nbkrgk/searchoutjsp?item=31&material=50718&lang=ENG](http://www.nbkrgk/searchoutjsp?item=31&material=50718&lang=ENG), 18 July 2014) <<http://www.nbkrgk/>> accessed 30 July 2017

¹⁴³ Dan Cummings, 'Regulatory Sandboxes: A Practice For Innovation That Is Trending Worldwide' ([Https://www.ethnews.com/regulatory-sandboxes-a-practice-for-innovation-that-is-trending-worldwide](https://www.ethnews.com/regulatory-sandboxes-a-practice-for-innovation-that-is-trending-worldwide) , 1 March 2017) <<https://www.ethnews.com/>> accessed 30 July 2017

use of this system, such as the UK, Russia, Canada, Switzerland and Australia.¹⁴⁴ This system allows for growth and experimentation with minimised risk and the author believes it to be a possible way forward for Malta.

¹⁴⁴ *ibid*

Chapter 2: The Blockchain

Satoshi Nakamoto's conception of Bitcoin in 2008¹⁴⁵ is considered one of the most important developments in currency and monetary policy, it being the first of its kind insofar as it is a digital asset that is not backed by any one bank or country and no centralized controller.¹⁴⁶ Even more pertinent to modern day life than the concepts behind Bitcoin itself is the technology behind the cryptocurrency. The blockchain is a tool that affords the users distributed consensus. There are various applications of blockchain technology and the author aims to delve further into these in the coming chapters.¹⁴⁷

Blockchain technology has been referred to as 'the technology likely to have the greatest impact on the next few decades.'¹⁴⁸ Every so often, around the world, a new technology is created that is to have a massive impact on humankind. The creation of the wheel, the inception of the Internet, and the discovery of penicillin: each of these discoveries serving to shape the way we viewed the world around us at a specific moment in history. Blockchain technology is one such creation, set to redefine that which we know to be the norm in the realm of contract law, Internet transactions, asset registry and other varied spheres.¹⁴⁹

The computers that run the blockchain for Bitcoin are often referred to as nodes. Some of these put forward their processing power in order to solve the mathematical problem related to the creation of a block. These are the miners as described in the previous chapter. The action of solving the complex algorithms is referred to as mining, this is an analogy mostly based on gold mining, which is a far more tangible concept. Mining can be done by the average computer-minded individual as a hobby, or it can be done by people who take it far more seriously. In the latter case, it often tends to include processors that are specifically optimised for their mining capability. Not every node is a mining node. The nodes that are not involved in the mining process are those nodes performing the verification of the received data before then routing it to the peer connections.¹⁵⁰ It is only then that the mining nodes

¹⁴⁵ Nakamoto (n1)

¹⁴⁶ Rochard (n54)

¹⁴⁷ 'A Next-Generation Smart Contract and Decentralized Application Platform' (<https://github.com/ethereum/wiki/blob/master/pages/white-paper/%5Benglish%5D-white-paper.md>, 23 March 2016) <<https://github.com/>> accessed 30 July 2017

¹⁴⁸ Don Tapscott, [TED] (June 2016) "How the blockchain is changing money and business" Retrieved from: <https://www.ted.com/talks/don_tapscott_how_the_blockchain_is_changing_money_and_business#t-9390> accessed 2 February 2017

¹⁴⁹ *ibid*

¹⁵⁰ 'How Bitcoin Mining Works' (n57)

come into play in order to convert the unordered transactions into the ordered, and properly recorded transactions into a block of data – this block is the next block on the chain. In order to add a new block to the chain, the new block must include a nonce – a randomly generated number – as well as the hash of the previous block.¹⁵¹ It is this nonce that includes the random element, as it cannot be predicted which computer will eventually land upon the correct value. It is purely based on processing power (the speed at which the computer can try different variations of numbers in order to find the correct one), and luck.¹⁵²

2.1 The Seven Design Principles of the Blockchain Economy

In Don Tapscott's book "Blockchain Revolution: how the Technology behind Bitcoin is Changing Money, Business and The World", the seven design principles of the Blockchain economy are listed, which Tapscott believes to emanate from the works of Satoshi Nakamoto, specifically his 2008 white paper¹⁵³ on the technology behind Bitcoin: ¹⁵⁴ 'Satoshi never wrote about these principles, but they are implicit in the technology platform he unleashed. We see them as principles for shaping the next era of the digital economy, and an era of renewed trust.'

In this paper Nakamoto never attempted to reinvent the wheel, he merely extended the current technological climate to include this new era of a digital economy that would cater to the needs of the future.

2.1.1 Networked Integrity

The first principle mentioned is that of networked integrity. This ties in closely with the Trust Protocol (as described in Chapter 2.2), the double spend problem (which is tackled in Chapter One), and the concept of consensus. Satoshi Nakamoto wanted to remove the middleman in exchanges and transactions, and also remove the level of uncertainty relating to the history of the transactions – letting the blockchain be self-evident as a definitive ledger of the history of

¹⁵¹ ibid

¹⁵² ibid

¹⁵³ Nakamoto (n1)

¹⁵⁴ Don Tapscott and Alex Tapscott, *Blockchain Revolution How the Technology Behind Bitcoin is Changing Money, Business and The World* (Penguin Random House 2016) 29

the transactions.¹⁵⁵ This is called consensus. Vitalik Buterin, the creator of Ethereum, has been quoted as saying, ‘consensus is a social process, human beings are fairly good at reaching consensus without any help from algorithms.’¹⁵⁶

In the case of Bitcoin, consensus is reached through the proof of work (PoW) mechanism. This was described as follows in the Tapscott book:

To achieve consensus, the Bitcoin network uses what’s called a proof of work mechanism. This may sound complicated but the idea is a simple one. Because we can’t rely on the identity of the miners to select who creates the next block, we instead create a puzzle that is hard to solve (i.e. takes a lot of work), but easy to verify (i.e. everyone else can check the answer very quickly). Participants agree that whoever solves the problem first gets to create the next block. Miners have to expend resources (computing hardware and electricity) to solve the puzzle by finding the right hash, a kind of unique fingerprint for a text or data file. For each block they find, miners receive Bitcoin as a reward. The puzzle is mathematically set up to make it impossible to find a shortcut to solve it. That’s why, when the rest of the network sees the answer, everyone trusts that a lot of work went into producing it.”¹⁵⁷

This process, as arduous as it might sound, is the lynchpin that guarantees consensus.

Aside from the concept of the PoW mechanism as aforementioned, there are other consensus mechanisms in existence that, essentially, have the same aims. The first version of the Ethereum blockchain used the same kind of PoW mechanism, but further versions of the same technology shall likely be replacing the PoW mechanism with a proof of stake (PoS) mechanism,¹⁵⁸ which requires miners to invest in a value of the commodity – in order for them to create a ‘stake’ in the commodity. In the PoS mechanism, the creator of the following block is determined through a semi-random mechanism, and the likelihood that one person is chosen over another is dependent on the stake that the individuals have. In PoW systems, we

¹⁵⁵ Nakamoto (n1)

¹⁵⁶ Vitalik Buterin, 'Proof of Stake: How I Learned to Love Weak Subjectivity' (<https://blog.ethereum.org/2014/11/25/proof-stake-learned-love-weak-subjectivity/>, 25 November 2014) <<https://blog.ethereum.org/>> accessed 30 July 2017

¹⁵⁷ Tapscott (n154) 31

¹⁵⁸ Tapscott (n154) 32

refer to the creation of new blocks as ‘mining’ (similar to the way gold is mined), but in PoS systems, the term used to refer to the creation of blocks, is ‘forging’ or ‘minting’ (similar to the way blacksmiths forge materials). Another differentiation between the two systems is that in PoW, new coins can be created, and miners are rewarded with currency, but generally, in PoS, there are no block rewards, but they are incentivised through the obtainment of transaction fees. The latter type of proof has garnered some controversy in its application, due to the criticism that people who are new to the mechanism, either need someone to vouch for them, or else, they must have some kind of prior reputation in order to participate.

Proof of Activity (PoA)¹⁵⁹ is yet another mechanism that can be used in order to achieve the same ends. It is an amalgamation of the PoW and PoS mechanisms that requires a randomised number of miners to use a cryptokey and sign off on the block before the block becomes an official part of the blockchain.¹⁶⁰ Another method of guaranteeing consensus is Proof of Capacity (PoC),¹⁶¹ which requires miners to dedicate a specific volume of their hard drive towards mining. Similarly, Proof of Storage (PoS) involves miners that allocate and share disk space in a distributed cloud.¹⁶²

The importance of storage should not be underestimated. Data stored on the blockchain is different, and hence valuable because it is specific: the exact time and date of publication is relevant to future transactions, and therefore it must be preserved in its entirety.¹⁶³ This is where one can truly understand the importance of mining. Upon reaching consensus, each miner maintains a decentralised copy of the full ledger, which safeguards against hacking and fraud.¹⁶⁴ Paul Brody of Ernst & Young has remarked that regardless of the consensus mechanism one opts for, ‘the blockchain ensures integrity through clever code rather than through human beings who choose to do the right thing.’¹⁶⁵

The implications of network integrity for all sectors of society, from social, to political, property etc. all of which can benefit from this new wave of implicit trust.

¹⁵⁹ *ibid*

¹⁶⁰ *ibid*

¹⁶¹ *ibid*

¹⁶² *ibid*

¹⁶³ Tapscott (n154) 31

¹⁶⁴ *ibid*

¹⁶⁵ Tapscott (n154) 33

2.1.2 Distributed Power

The second principle as mentioned in the book is that of distributed power. This system implies that no individual can unilaterally shut the system down.¹⁶⁶ There is ultimate transparency, as the individuals can all see the actions of the other individuals. Before the conception of blockchain technology, there was no way of safeguarding against the overbearing nature of centralised data. Now, with blockchain, the pros of attempting to override the Bitcoin blockchain do not supersede the cons in a financial context. As the situation stands, any person is able to download a copy of the blockchain, which allows for a decentralised nexus of power.¹⁶⁷ As Tapscott put it:

The blockchain resides everywhere. Volunteers maintain it by keeping their copy of the blockchain up to date and lending their spare computer processing units for mining. No backdoor dealing. Every action or transaction is broadcast across the network for subsequent verification and validation. Nothing passes through a central third party; nothing is stored on a central server.¹⁶⁸

Another important aspect of Bitcoin's substance is the realisation that Nakamoto ensured this decentralised aspect of the technology even further, where they removed all requirements of any intermediary, like a central bank or treasury, and instead, each miner who solves one of the algorithms is rewarded accordingly and each new block is linked to both the previous blocks and the subsequent blocks in the chain.¹⁶⁹

2.1.3 Value as Incentive

The third design principle is value as incentive, which aims to align the incentives of all stakeholders involved.¹⁷⁰

Before this technology, the issue that existed may be explained through the use of the banking crisis and the recession affecting the United States between 2007 and 2010 as a prime example. Prior to this period, mortgages and loans were handed out at attractive rates

¹⁶⁶ *ibid*

¹⁶⁷ Tapscott (n154) 34

¹⁶⁸ Tapscott (n154) 34-35

¹⁶⁹ Tapscott (n154) 31

¹⁷⁰ Tapscott (n154) 35

to people without sufficient understanding of the risks.¹⁷¹ This led to severe, long-lasting consequences for the economy.

People are not infallible, and many individuals in that position might easily have gone down the same route due to the incentive structure in place in banking institutions¹⁷². Nakamoto designed Bitcoin so that miners were incentivized to work on it.¹⁷³ Before this was the case, larger corporations were given all the tools necessary to take a larger amount of value from the networks that give them the rights. Through the influx of this new technology, people now act in their own self-interest. Now, no matter how selfishly people act, the actions benefit the system overall, and not merely their personal benefit. Tapscott describes this as follows:

Bitcoin is an incentive for miners to participate in creating a block and linking it to the previous block. Those who complete a block first get a quantity of bitcoins for their efforts. Satoshi's protocol rewarded early adopters handsomely with bitcoin: for the first four years, miners received 50 bitcoins (BTC) for each block. Every four years, the reward per block would halve: 25 BTC, 12.5 BTC, and so on. Because they now own bitcoin, they have an incentive to ensure the platform's long-term success, buying the best equipment to run mining operations, spending energy as efficiently as possible, and maintaining the ledger. Bitcoin is also a claim on the blockchain, not just as an incentive to participate in mining and transacting with others but through ownership in the platform itself. Distributed user accounts are the most basic element of the cryptographic network infrastructure. By owning and using bitcoin, one is financing the blockchain's development.

¹⁷¹ John V Duca, 'Subprime Crisis' (https://www.federalreservehistory.org/essays/subprime_mortgage_crisis, 22 2013)<<https://www.federalreservehistory.org/>> accessed 30 July 2017

¹⁷² Tapscott (n154) 35

¹⁷³ Nakamoto (n1)

2.1.4 Security

The fourth design principle is that of security.¹⁷⁴ This rests primarily in the decentralised aspect of the blockchain, which implies that there is no central point of failure, and if anyone acts in a way that is detrimental the only detriment is to themselves.¹⁷⁵ Hacking, identity theft, phishing, malware, spam, and cyberbullying all constitute the undermining of the security of the individual in society. Technology is not safeguarded against these things, because the service providers do not require a high level of protection from the people using their services, for example, password requirements are often very easily hacked. If we are to move forward with new technologies and advance with the times as is required to progress, including the aspect of communicating monies directly between parties and negating the necessity of a middleman, these communications need to be hack-proof.¹⁷⁶

Nakamoto, in his white paper,¹⁷⁷ required participants to use PKI – which involves users having two keys, where one is for encryption and one for decryption. Tapscott believes that ‘if we’re both using bitcoin, if we can store and exchange bitcoin securely, then we can store and exchange highly confidential informational and digital assets securely on the blockchain.’¹⁷⁸

2.1.5 Privacy

The fifth principle is that of privacy,¹⁷⁹ which advocates that people ought to be in control of their data, and decide what and when they want to share with anyone else. This principle closely echoes the anonymous aspect of the cypherpunks’ manifesto tackled in Chapter One. The issue at hand here is that most technology companies collect and mine data in order to be able to monetise it in the future.¹⁸⁰

¹⁷⁴ Tapscott (n154) 39

¹⁷⁵ *ibid*

¹⁷⁶ Tapscott (n154) 40

¹⁷⁷ Nakamoto (n1)

¹⁷⁸ Tapscott (n154) 40

¹⁷⁹ Tapscott (n154) 41

¹⁸⁰ ‘Monetizing data while respecting privacy: How data-use governance can unlock business value and mitigate risk’ (<https://www.pwc.com/us/en/increasing-it-effectiveness/publications/creating-business-value-with-data-usage.html>, August 2016) <<https://www.pwc.com/>> accessed 30 July 2017

The breakthrough aspect of Bitcoin was that individuals are not required to use their real identities in order to register for an account.¹⁸¹ On the blockchain, one can elect to retain an element of personal anonymity, since one is not required to place any sensitive personal information in any central database. The blockchain protocol allows the user to retain control over privacy in any given environment.¹⁸² This is mutually beneficial for companies too, as they are put in a bad light when they are hacked and their customers' data is breached. With that in mind, companies are opening up with the aim of changing the way corporations relate to consumer data.

While the blockchain in itself remains public domain, as it resides on a decentralised network and anyone can opt to view it at any given time, users remain pseudonymous, with no centralised storage of their real-world identities.¹⁸³ With blockchain technology, we would be able to be in control of our virtual lives in a more tangible way.

2.1.6 Rights Preserved

Rights preserved is the sixth design principle and encompasses the fact that ownership rights are transparent and enforceable. Individual freedoms are recognised and respected. We hold this truth to be self-evident – that all of us are born with certain inalienable rights that should and can be protected.¹⁸⁴

At the start of the Internet, the main driving force was that of finding different and more advanced ways to exercise these rights properly. The Uniform Commercial Code¹⁸⁵ was used in the USA in order to remove the necessity of negotiating and creating contracts for every item, but middlemen were still necessary in order to manage transactions, and this brought with it the obvious flaws; time consuming, delays, float, etc. With the blockchain, rights become clear and more enforceable. The PoW system requires that transactions are timestamped, this means that, combined with PKI, the blockchain provides a solution to the double spend problem, as well as being able to track and confirm ownership of all coins in circulation, whilst each transaction is irrevocable. Tapscott describes the situation as follows:

¹⁸¹ This relates to the pseudonymous nature of the blockchain referred to in Chapter 2.1.5

¹⁸² *ibid*

¹⁸³ Tapscott (n154) 44

¹⁸⁴ Tapscott (n154) 45

¹⁸⁵ Legal information institute, 'Uniform Commercial Code' (<https://www.lawcornelledu/ucc>) <<https://www.law.cornell.edu/>> accessed 30 July 2017

As the Ledger of Everything, the blockchain can serve as a public registry through such tools as Proof of Existence (PoE), a site that creates and registers cryptographic digests of deeds, titles, receipts, or licenses on the blockchain. Proof of Existence doesn't maintain a copy of any original document; the hash of the document is calculated on the user's machine, not on the PoE site, thus ensuring confidentiality of content. Even if a central authority shuts down Proof of Existence, the proof remains on the blockchain. So, the blockchain provides means of proving ownership and preserving records without censorship.¹⁸⁶

Smart contracts are considered the breakthrough in this regard, as they allow for a situation wherein transactions can proceed upon the occurrence of predefined benchmarks that have been agreed upon by all parties to the contract. The implications of this are endless and they will be tackled separately in Chapter Three.

2.1.7 Inclusion

The final design principle is that of inclusion, wherein everyone around the world can be afforded the ability to participate in the global blockchain economy through the lowering of the barriers to participation.¹⁸⁷ This principle links closely to the concepts of capitalism and welfare, as there are millions of people in yet emerging economies that do not have access to basic rights and opportunities, such as access to the Internet or economic opportunities. There are still many people who do not even have access to a bank account, which in turn prevents them from transacting and affecting various payments and exploring the myriad of opportunities that are only available via the Internet.

Nakamoto designed the system to work with the Internet but it could run without it if necessary.¹⁸⁸ Many people who use the blockchain use "simplified payment verification" (SPV) which can mobilise the blockchain. This implies that anyone with a phone can participate in this emerging economy, without the prerequisite formalities of a bank account, address, proof of citizenship or birthdate.

¹⁸⁶ Tapscott (n154) 46

¹⁸⁷ Tapscott (n154) 49

¹⁸⁸ Nakamoto (n1)

The use of the blockchain also lowers the cost of money transfers, lowers the barrier to having a bank account and investing whilst supporting global entrepreneurship and trade, making it easier for people located in the world's poorer economies to become valid participants in this emerging global economy; this idea provides boundless hope for the world's future.¹⁸⁹

2.2 The Trust Protocol

As early as the 1980s, people were trying to find solutions to the countless problems that the Internet inevitably brought with its boundless prospects, these primarily being issues of privacy and security.¹⁹⁰ There used to be a time, where paying via credit card was considered to be asking for trouble. Nowadays, the Internet is far more secure, and purchases via credit card are made every day.¹⁹¹

In 1993, David Chaum created a digital payment system called eCash,¹⁹² which made paying over the Internet much easier to do, in a safe and anonymous manner. At the time, people were not as keen on using the Internet for their shopping, and hence the company was not a long-term success, even though the technology behind it went on to be much bigger than even Chaum likely imagined it to be. In 2008, as discussed in Chapter One, Satoshi Nakamoto made a massive breakthrough in this sphere, with the publication of his paper which outlined the protocol for a peer-to-peer electronic cash system called Bitcoin.¹⁹³ The implications of Bitcoin reached far and wide, falling within the basic ambit of Nick Szabo's paper entitled 'The God Protocol'.¹⁹⁴ This 'God Protocol' was described as a massive breakthrough in technology, where God was the third party responsible for transactions between two parties. Since Bitcoin works through the blockchain, this God Protocol is established through the third-party medium of mining.¹⁹⁵ It is a 'trusted transaction(s) directly between two or more

¹⁸⁹ Antifragile, 'The 7 Design Principles of a Blockchain Economy' (<https://steemit.com/steemit/@antifragile/the-7-design-principles-of-a-blockchain-economy>, August 2016) <<https://steemit.com/>> accessed 30 July 2017

¹⁹⁰ Tapscott (n154) 4

¹⁹¹ *ibid*

¹⁹² Ian Grigg, 'How DigiCash Blew Everything' (<https://cryptome.org/jya/digicrashhtm>, 10 February 1999) <<https://cryptome.org/>> accessed 30 July 2017

¹⁹³ Nakamoto (n1)

¹⁹⁴ Nick Szabo, 'The God Protocols' (<http://nakamotoinstitute.org/the-god-protocols/>, 1997) <<http://nakamotoinstitute.org/>> accessed 30 July 2017

¹⁹⁵ *ibid*

parties, authenticated by mass collaboration and powered by collective self-interests, rather than by larger corporations motivated by profit.¹⁹⁶

Blockchain technology has allowed for a system whereby person A can send money to person B without having to go through an intermediary, like PayPal, a bank or even a credit card company.

Blockchain refers to the underlying technology behind cryptocurrencies such as Bitcoin. This technology has heralded practical use for a myriad of applications, ranging from transactions in everyday online purchases to more complex transactions in the remit of iGaming.

In Chapter One, the author discussed the price of Bitcoin. 'Price' differs to 'value,' as the value is the regard for the benefits that Bitcoin can have. Price is the monetary cost of the Bitcoin, or the price at which they are valued at any one time. The useful nature of Bitcoin, more importantly the technology that propels it, is the result of technological drive and innovation, and the features consequentially held in this technology are of incredibly value, which is currently mostly untapped by mainstream businesses and possible clientele. The value that Bitcoin has is not just 'value' as a general definition but can be sub-defined into scientific value, technological value, secured value, design value, developmental value, network value, and contract and application value.¹⁹⁷ These different aspects of the value of Bitcoin each serve to highlight the usefulness of the technology by outlining the pros involved.

2.3 The Blockchain

An article written by Joichi Ito, the director at MIT Media Lab, alludes to the fact that the Blockchain is to trust as the Internet is to information, and like the original Internet, the blockchain has potential to transform everything.¹⁹⁸

Chapter One briefly assessed the method by which Bitcoin is mined. In this chapter, this concept of mining is thoroughly explained for the concept to be better understood in the context of the blockchain.

¹⁹⁶ Tapscott (n154) 5

¹⁹⁷ Venzen Khaosan, 'What Determines the Value of Bitcoin?' (<https://www.cryptocoinsnews.com/determines-value-bitcoin/>, 22 September 2014) <<https://www.cryptocoinsnews.com/>> accessed 30 July 2017

¹⁹⁸ Joichi Ito, Neha Narula, Robleh Ali, 'The Blockchain Will Do to the Financial System What the Internet Did to Media' (<https://hbr.org/2017/03/the-blockchain-will-do-to-banks-and-law-firms-what-the-internet-did-to-media> , 9 March 2017) <<https://hbr.org/>> accessed 30 July 2017

The most innovative feature of this new technology is the fact that the cryptocurrencies are not saved in a file on a server somewhere, but are represented through the transactions as recorded in the blockchain. This blockchain acts as a globalised ledger of transactions, which is distributed over a large network that is provided by volunteers around the world. This negates the idea of a centralised database that can possibly be hacked or altered and makes this a much safer way of handling the information. The blockchain also uses an incredibly strong encryption in order to maintain its level of security. This system is a two-key system that requires the public and the private keys to be accessed.¹⁹⁹ The blockchain is also verified and stored every ten minutes, with the new block linking to the previous block only when all of the checks and balances have been verified and cleared.²⁰⁰ The structure that this follows implies that in order to change a transaction (to hack the database), one would have to rewrite the entirety of the blockchain, which would be a near impossible feat. Don Tapscott, in his book 'Blockchain Revolution' held that:

The blockchain is a distributed ledger representing a network consensus of every transaction that has ever occurred. Like the world wide web of information, it's the worldwide ledger of value – a distributed ledger that everyone can download and run on their personal computer.²⁰¹

In an incredibly simplified manner, the blockchain works in the following way: Firstly, an individual requests a transaction – these transactions might involve cryptocurrency transactions or a contractual clause, for example. This transaction is broadcast to a network of computers which validate the transaction using algorithms. Once verified, the transaction is combined with other transactions to create a block of data for the ledger. The block is then added to the existing chain, creating an unalterable and indisputable chronology of blocks – the blockchain. The transaction is complete and the cryptocurrency transaction or contractual clause is affected²⁰².

¹⁹⁹ Tapscott (n154) 6

²⁰⁰ ibid

²⁰¹ Tapscott (n154) 7

²⁰² Blockgeeks, 'What is Blockchain Technology? A Step-by-Step Guide For Beginners' (<https://blockgeeks.com/guides/what-is-blockchain-technology/>)<<https://blockgeeks.com/>> accessed 30 July 2017

Mining, the process through which Bitcoin is created, makes it nearly impossible for any individual to add new blocks of transactions into the blockchain. As stated previously in the design principles, this process of mining protects the neutrality of the blockchain by ensuring that no single individual is capable of gaining enough power to block transactions of his choosing.²⁰³ The blockchain is immutable and irrevocable, and mining is the cause for this safeguard, as it makes it borderline impossible to reverse a previous transaction.²⁰⁴

2.4 Ethereum

Vitalik Buterin is the Russian-born Canadian founder of Ethereum. He was born in 1994, and whilst most people his age were still studying, he became the co-founder of a massive blockchain based platform that has enormous capabilities, far beyond our current level of comprehension²⁰⁵. Vitalik Buterin's first foray into this field of cryptocurrencies and blockchain started with an interest in Bitcoin, which he says seemed like the natural fit for him,

I specialize in generalism, I had all these different interests, and somehow Bitcoin seemed like a perfect convergence. It has math. It has its computer science. It has its cryptography. It has its economics. It has its political and social philosophy. It was this community that I was immediately drawn to. I found it really empowering.²⁰⁶

After discovering this passion, he initially scoured online forums in an attempt to get hold of some Bitcoin. He came across someone who was starting a blog called 'Bitcoin Weekly' and started to write some articles for that blog, in exchange for Bitcoin²⁰⁷. He moved on and started writing for a different publication, 'Bitcoin Magazine',²⁰⁸ and upon realising that he was spending a lot of his time on this new project, he dropped out of university and made, what would later be known as Ethereum, his life project. He created Ethereum as an open source project, which means that the code is available to anyone to alter and elaborate upon

²⁰³ How Bitcoin Mining Works (n57)

²⁰⁴ *ibid*

²⁰⁵ Vitalik Buterin, 'A Next-Generation Smart Contract and Decentralized Application Platform' (<https://github.com/ethereum/wiki/wiki/White-Paper>) <<https://github.com/>>accessed 30 July 2017

²⁰⁶ Tapscott (n154) 278

²⁰⁷ *ibid*

²⁰⁸ Tapscott (n154) 279

and it is generally offered to people for free, money being made through other projects that work alongside it.²⁰⁹ This allowed for programmers to have a platform with the flexibility required to develop varied technology.

Ethereum was originally described by Buterin in late 2013²¹⁰ after spending time working in the Bitcoin community. Shortly thereafter, he published the Ethereum white paper,²¹¹ which outlined the Ethereum protocol and smart contracts architecture. In January 2014, Vitalik announced Ethereum at The North American Bitcoin Conference in Miami, Florida, USA.²¹² Ethereum went live in June of 2015. Ethereum is currently the second longest and fastest growing public blockchain. Vitalik also teamed up with Dr. Gavin Wood, to co-found Ethereum, and the latter published the Ethereum Yellow Paper in April 2014,²¹³ which served as the technical description of the Ethereum Virtual Machine (EVM).

Apart from developing the required software for Ethereum, a massive effort to round up the resources was necessary in order to get the cryptocurrency and blockchain up and running., Ethereum organised a presale of Ether tokens, the Bitcoin equivalent for Ethereum, in order to organise a network of developers, stakeholders, miners and investors.²¹⁴

Buterin, Wood and Wilcke set up another legal entity, ETH DEV,²¹⁵ with the purpose of overseeing the process of Ethereum development, which had taken a backseat to the aforementioned presale, and in order to keep the momentum up they released several proof-of-concept versions of the Ethereum software.²¹⁶ According to Tapscott,

[Ethereum] blockchain has some extraordinary capabilities. One of them is that you can build smart contracts. It's kind of what it sounds like. It's a

²⁰⁹ *ibid*

²¹⁰ Ethereum community revision 41fc2c03, 'History of Ethereum' (<http://ethdocs.org/en/latest/introduction/history-of-ethereum.html>, 2016) <<http://ethdocs.org/en/latest/introduction/history-of-ethereum.html>> accessed 30 July 2017

²¹¹ Buterin (n205)

²¹² History of Ethereum (n210)

²¹³ *ibid*

²¹⁴ *ibid*

²¹⁵ ETHDEV is not an acronym, it is a consortium of organizations established across various jurisdiction that functions as the development arm of Ethereum.

²¹⁶ 'A Brief History of Ethereum From Vitalik Buterin's Idea to Release' (<https://cointelegraph.com/ethereum-for-beginners/a-brief-history-of-ethereum-from-vitalik-buterins-idea-to-release>) <<https://cointelegraph.com/>> accessed 30 July 2017

contract that self-executes, and the contract handles the enforcement, the management, performance and payment²¹⁷

In its most diluted form, Ethereum is an open software platform that uses blockchain technology to enable developers to create decentralised applications for public consumption.²¹⁸ Ethereum is different to other blockchains, as although all blockchains are able to process code, they are often limited, but Ethereum works to create whatever coding operation is required by developers, allowing for the creation of thousands of applications that go beyond the generally understood Bitcoin or payment service.²¹⁹ It has been referred to as ‘a cryptoeconomically-secured platform for development of any kinds of decentralized applications,’²²⁰ and this definition seems to encapsulate the idea of Ethereum perfectly.

The EVM is a Turing-complete computer that is capable of using an international network of public nodes in order to execute scripts in a cryptographically secure manner. It can be likened to Bitcoin in the way that it shares similar characteristics, even considering the fact that Buterin, the creator of the EVM, started off as a Bitcoin enthusiast, makes a lot of sense in this context, but it goes one step further than Bitcoin, insofar as it is able to run any kind of contract. Both networks (Bitcoin and EVM) have a ledger that records the accounts. However, EVM also includes the list of contracts held (in code). Generally, people tend to spend a percentage of their money on credit card fees (a small amount, but still substantial enough to notice, often around 3%). In lieu of this, but to the same end, EVM users pay small amounts of money referred to as ‘gas’ in order to have their money shifted through the network.²²¹ These amounts are much smaller than the average credit card fee, and hence, are preferable to the users. The average transaction costs very little, irrespective of the sum being moved, unlike the percentage system used by banks.²²²

²¹⁷ Blockgeeks, 'What is Ethereum? A Step-by-Step Beginners Guide' (<https://blockgeeks.com/guides/what-is-ethereum>) <<https://blockgeeks.com/>> accessed 30 July 2017

²¹⁸ *ibid*

²¹⁹ *ibid*

²²⁰ Buterin (n216)

²²¹ Blockgeeks (n217)

²²² Peter Brogden, 'Smart Contracts and Web 3.0: The Evolution of Law?' (SCL, 2017) <<https://www.scl.org/articles/3907-smart-contracts-and-web-3-0-the-evolution-of-law>> accessed 24 May 2017

2.5 The Implications of Decentralisation

When it comes to decentralisation, this integral concept in the discussion on Bitcoin is oftentimes misunderstood. The origin of the idea that drives the concept of decentralisation is a simple one, and it can be seen as far back as Shakespeare's *Merchant of Venice*, where Antonio says: 'My ventures are not in one bottom trusted, nor to one place; nor is my whole estate upon the fortune of this present year.'²²³ This, in modern day parlance, translates to 'do not put all your eggs in one basket'. What is the true meaning of 'decentralisation' in this context?

The exact meaning of decentralisation in cryptocurrency debates depends on the context, but when diluted, decentralisation refers to a method of co-operation between peers with no centralised storage of information.²²⁴

As described in Chapter Two, the decentralised nature of Bitcoin may, in fact, be one of its truly innovative features that serve to set it apart from other cryptocurrencies or fleeting technologies. This decentralisation seems somewhat vague, as there does not seem to be consensus on what is the true *raison d'être* of decentralisation, whether Bitcoin melds with that or how it can be improved. The decentralised nature of Bitcoin stems from its use of a distributed database, where information is not all stored in one place but in varied locations owned by individuals around the world.²²⁵

Although decentralisation advocates multiple points of control or information storage, most of the systems built within the structure are centralised, since they are run by specified individuals in easily determinable locations with specific computer systems. This makes them vulnerable and creates a somewhat ironic situation where there exists decentralised technology and yet, all the things that exist upon it are centralised.

While this *de facto* centralisation exists, the true breakthrough aspect of this that adds legitimacy to the claim that Bitcoin is truly decentralised is that users can opt out. Bitcoin

²²³ The *Merchant of Venice*, William Shakespeare, (1.1.42-44)

²²⁴ <http://www.coindesk.com/decentralized-proven-otherwise/>

²²⁵ Bernard Marr, 'A Complete Beginner's Guide To Blockchain' (<https://www.forbes.com/sites/bernardmarr/2017/01/24/a-complete-beginners-guide-to-blockchain/#7593a8a76e60> , 24 January 2017) <<https://www.forbes.com/>> accessed 30 July 2017

allows this, but central banks and regular fiat money do not.²²⁶ “Decentralization of status does not necessarily mean the decentralization of the process.”²²⁷ Another way of understanding decentralisation is to liken it to a diversified investment portfolio, just like in the previous example referring to Shakespeare’s Merchant of Venice.

As described by Chang Jia in the article ‘What Is the True Meaning of “Decentralization” in Blockchain Technology?’,²²⁸ where an attempt is made to differentiate between true and perceived decentralisation,

Should the degree of the relationship among these assets be unknown, then the Principle of Maximum Entropy may apply: assume these assets are of a maximum randomness. For a blockchain, assume the nodes enjoy absolute freedom of decision-making and are not entrusting developers with disproportionate power and also delegating them to do the bookkeeping. By contrast, though the Proof of Work incentive causes the appearance of centralization of computational power (in fact it’s dispersed, although a few hands control the greatest amount of computational power), nobody could stop you from joining in the mining or the R&D of mining devices. It’s a decentralized process of free competition. It’s like voting in an election: While a democracy could produce a Canadian prime minister like Justin Trudeau (son of former prime minister, Pierre Trudeau) thereby creating a blood succession in appearance, the decentralization of the democratic process empowers its legitimacy.²²⁹

²²⁶ Erik Voorhees, 'Is Bitcoin Truly Decentralized? Yes – and Here Is Why It’s Important' (<https://bitcoinmagazine.com/articles/bitcoin-truly-decentralized-yes-important-1421967133/>), 22 January 2015) <<https://bitcoinmagazine.com/>> accessed 30 July 2017

²²⁷ Jia chang, 'Op-Ed: What Is the True Meaning of "Decentralization" in Blockchain Technology?' (<https://bitcoinmagazine.com/articles/guest-post-what-is-the-true-meaning-of-decentralization-in-blockchain-technology-1474558340/>), 22 September 2016) <<https://bitcoinmagazine.com/>> accessed 30 July 2017

²²⁸ ibid

²²⁹ ibid

2.6 The Various Applications of Blockchain Technology

‘[Blockchain] is to Bitcoin, what the Internet is to email. A big electronic system, on top of which you can build applications. Currency is just one.’ - Sally Davies, FT Technology Reporter.

In a MaltaToday article published on the 23 July 2017, entitled ‘Malta lays the Groundwork for a Blockchain Revolution’,²³⁰ Silvio Schembri, the Parliamentary Secretary for the Digital Economy, stated that plans for Malta to begin to harness this technology would be set out in a twofold manner: firstly, for blockchain to be used across the board in the public sector, and ultimately for Malta to become a hub for international companies that operate using this technology.²³¹

At this stage, the applications of blockchain technology seem practically endless. From infrastructure, to property to banking, there seems to be a use for it in nearly all facets of society. Blockchain can be defined as a ‘database protocol developed to underpin Bitcoin.’²³² The recorded information in the blockchain is updated simultaneously and transactions are only accepted to form part of the blockchain after they are worked on by a variety of individuals. This kind of technology has eliminated the requirement for middlemen in many diverse financial transactions, and has hence, created new methods of record keeping and carrying out of financial services.²³³

The best way to describe the groundbreaking implications of blockchain technology can be seen in the Tapscott book, where Don Tapscott describes it as follows:

This new digital ledger of economic transactions can be programmed to record virtually everything of value and importance to humankind: birth and death certificates, marriage licenses, deeds and titles of ownership, educational degrees, financial accounts, medical procedures, insurance

²³⁰ Tim Diacono, 'Malta lays the ground for a blockchain revolution' (http://www.maltatoday.com.mt/business/business_news/79185/malta_lays_the_ground_for_a_blockchain_revolution#WX4hB8aB2Rs, 26 July 2017) <<http://www.maltatoday.com.mt/>> accessed 30 July 2017

²³¹ *ibid*

²³² Oscar Williams-Grut, 'Santander is letting staff use the tech behind bitcoin to send money to each other' (<http://uk.businessinsider.com/santander-develops-blockchain-international-payment-app-with-ripple-2016-5>, 27 May 2016) <<http://uk.businessinsider.com/>> accessed 30 July 2017

²³³ Oscar Williams-Grut, 'GOLDMAN SACHS: 5 practical uses for blockchain — from Airbnb to stock markets' (<http://www.businessinsider.com/goldman-blockchain-beyond-the-hype-practical-uses-2016-5/#sharing-economy-building-trust-on-platforms-like-airbnb-1>, 28 May 2016) <<http://www.businessinsider.com/>> accessed 30 July 2017

claims, votes, provenance of food, and anything else that can be expressed in code. The new platform enables a reconciliation of digital records regarding just about everything in real time. In fact, soon billions of smart things in the physical world will be sensing, responding, communicating, buying their own electricity and sharing important data, doing everything from protecting our environment to managing our health. This Internet of Everything needs a Ledger of Everything. Business, commerce, and the economy need a Digital Reckoning.²³⁴

One example of a lucrative application for this kind of technology is the financial services industry, which has already started to rebrand and privatise blockchain technology, now referring to it as ‘distributed ledger technology,’²³⁵ which marks their attempt at reconciling the security, speed and cost of Bitcoin with a closed system that requires the permission of a financial institution to use.²³⁶

²³⁴ Tapscott (n154) 7

²³⁵ Alistair Maughan, 'Blockchain - Legal and regulatory issues around distributed ledger technology' ([Http://www.ciocouk/opinion/legal-briefing/blockchain-legal-regulatory-issues-around-blockchain-3638814/](http://www.ciocouk/opinion/legal-briefing/blockchain-legal-regulatory-issues-around-blockchain-3638814/), 20 April 2016) <<http://www.cio.co.uk/>> accessed 30 July 2017

²³⁶ Tapscott (n154) 8

Chapter 3: Smart Contracts

3.1 The Essence of the Contract

The essence of traditional contract law can be summed up through the definition of a contract as held in the first article under title IV, sub-title I ‘of Contracts’ in the Maltese Civil Code,²³⁷ whereby it is held that ‘a contract is an agreement or an accord between two or more persons by which an obligation is created, regulated, or dissolved.’²³⁸ This traditional notion is the crux of contract law, establishing the voluntary nature of a pact, entered into by two or more parties, concerning an agreement on specific terms and which is enforceable by law.

3.1.1 Elements for the Validity of a Contract

The Civil Code, in article 966,²³⁹ sets out the four requisite elements for the validity of a contract:

- (a) capacity of the parties to contract;
- (b) the consent of the party who binds himself;
- (c) a certain thing which constitutes the subject-matter of the contract;
- (d) a lawful consideration.²⁴⁰

Once the aforementioned conditions are met, a contract can be said to be valid and legally binding.

3.1.2 Different Types of Contracts

Obligations, under Maltese law, may fall under one of five categories. Obligations which arise by operation of the law are referred to as *ex lege* obligations. Obligations which do not arise by operation of the law can come about through four other headings; *ex contracto*, *ex quasi contracto*, *ex delicto* or *ex quasi delicto*. In the past, *ex contracto* obligations were only valid if they fell within a certain category. This system was abolished through the Code

²³⁷ Civil Code, (n4)

²³⁸ *ibid* Article 960

²³⁹ Civil Code (n4) Article 961

²⁴⁰ Civil Code (n4) Article 966; Article 966(d) is also referred to as ‘causa’

Napoleon and since then, citizens have the ability to enter into any type of contract as long as the requisite formalities (capacity, consent, object and *causa*) are met.

Natural obligations are those obligations that are not based on positive law but upon principles of equity and natural law, and hence, are not enforceable through a court of law.²⁴¹ If such obligations are performed, they may not be rescinded, and the receiver of the thing is not obliged to restore it. The Civil Code does not define 'natural obligations' but makes reference to them in the ambit of *indebiti solutio* in Article 1021.²⁴²

A person who receives, whether knowingly or by mistake, a thing which is not due to him under any civil or natural obligation, shall be bound to restore it to the person from whom he has unduly received it.²⁴³

Because of a lack of clear definition within our code, we refer to Roman law in order to assess the requisite validity of a natural obligation. Under Roman law, in order for a natural obligation to be recognised, there were two necessary elements; the link between parties and the absence of recognition or enforceability of such link. This is one of the few situations within our law that the intentional element is bypassed by the act itself. An example of a natural obligation is the payment of a debt for which enforceability has been time barred by prescription.

Carbonnier further clarifies natural obligations into three other subheadings:

1. A civil obligation that degenerates into a natural obligation, this is the case in the example above, or if an obligation was made in the wrong form but was affected regardless of its lack of enforceability in a court of law.
2. A duty of conscience transformed into a natural obligation comes about when a person fulfils something even though they are not bound by law or contract to do so. Here, the law does not initially recognise the existence of that obligation, but once it is affected, the law does not allow one to retract such action.
3. Debts or honour arising in the field of gaming and betting. Due to the exclusion of gaming and betting debts found within the Civil Code,²⁴⁴ in order for gaming and

²⁴¹ Natural obligation' ([Http://lawinorg/natural-obligation/](http://lawinorg/natural-obligation/)) <<http://lawin.org/>> accessed 30 July 2017

²⁴² Civil Code (n4) Article 1021

²⁴³ *ibid*

betting to be recognised as valid in Malta, a licence is required from the relevant authority.²⁴⁵ Carbonnier is of the opinion that, following the same logic as held within the other natural obligations, if the losing party pays the bet, he cannot later retract such payment. This notion is not universally accepted due to the fact that the original object of the contract is illegal.

As an example of contract law seen in the practice and ambit of gaming law, the First Hall Civil Court judgement of *Grech vs. Bennetti*²⁴⁶, makes reference to this notion stating:

“Fil-gurisprudenza taghna giet amMESSA l-obligazzjoni naturali ghar-rigward tal-imhatria, u ghalhekk ma jidhirx li jista’ jkun hemm raguni biex ma tkunx amMESSA anki f’kaz ta’ loghob projbit mil-ligi. Il-legislatur, imbagħad, jirrikonoxxi l-figura tal-obligazzjoni naturali, u saħansitra jirregola l-effetti tagħha, billi jiddisponi illi ma hemmx jedd ta’ azzjoni għal hlas lura jekk dak li thallas kellu jingħata bis-saħha ta’ obligazzjoni naturali.... Izda, biex ikun hemm dan l-effett, jehtieg li l-pagament ikun sar b’effett ta’ att guridikament validu, b’mod illi l-irrepetibbilita’ tal-pagament tippresupponi illi l-loghob ikun genwin u mingħajr qerq.”²⁴⁷

The elements of contractual obligations are reiterated in the case of *Cassar vs Grech Marguerat*,²⁴⁸ where the court established that while the debtor who pays that due from a natural obligation voluntarily is precluded from recovering the amount paid, such as in a fair game, in the case of cheating or fraudulence present in the original game, one may recover the debts paid to the creditor.²⁴⁹

The limitation of contractual obligations as examined by our Courts within the ambit of gaming law is evident and coupled with the fact that Malta does not subscribe to the doctrine of precedence is also likely responsible for the differentiation between judgements of similar facts. Typically, cases on the subject of gaming law would characteristically relate to the consideration. Article 990 of the Civil Code²⁵⁰ states that the consideration of a contract is to be deemed unlawful if it is contrary to morality or public policy - a rule which is also backed

²⁴⁴ Civil Code (n4)

²⁴⁵ The Malta Gaming Authority (MGA) is the relevant authority on gaming and betting licenses in Malta

²⁴⁶ *Salvatore Grech vs Carmelo Sive Charles Bennetti Et*, 27/01/1961, (First Hall Civil Court)

²⁴⁷ *ibid*

²⁴⁸ *Avukat Dottor Joseph Cassar Noe vs Joseph Grech Marguerat*, 23/06/1967, (Court of Appeal, Civil, Superior)

²⁴⁹ *ibid*

²⁵⁰ Civil Code (n4) Article 990

by criminal law, specifically in article 338(ii) of the Criminal Code²⁵¹. The latter two articles of the law were cited as the reason for which the claims of the plaintiff were dismissed in *Bartoli vs Chetcuti*²⁵². In doing so, the Court stated that:

Ghalhekk ghal dawn ir-ragunijiet il-Qorti hija soddisfatta li c-cirkostanzi kienu certament tali illi jnisslu aktar minn sospett ragonevoli illi l-ammont reklamat mill-konvenut kellu origini mill-loghob illegali. Per konsegwenza, l-obbligazzjoni assunta mill-konvenut hija nulla minnhabba causa illecita.²⁵³

The Courts have recognised the payment of a natural obligation arising out of an illegality, such as in the case of *Muscat vs Vella*²⁵⁴, where the amount of rent stipulated went above the legal parameter set for rent, and the Court did not allow the plaintiff to recover that which was paid over and above the legal sum, stating that:

Meta wiehed ikun ħallas il-kera awmentat mingħajr l-awtorizzazzjoni tal-Board fuq imsemmi, u jkun ħallsu mingħajr ma kien fi żball, mhix amMESSA r-ripetizzjoni tal-kera hekk imħallas, għax min jaċċetta l-għoli tal-kera, igawdi l-fond, u jħallas il-kera b'dak l-għoli, ma jistax wara żmien jirrepeti dik il-kera. Imma dan japplika biss għar-ripetizzjoni tal-kera li jkun ga tħallas, u mhux ukoll għall-kera li jkun għadu ma tħallasx.²⁵⁵

Here, the Court did not consider this law to be a matter of public policy, but one protecting the interests of the private party.

This would not be the case had the law been in place to safeguard public policy, as confirmed in the judgement *Felix Farrugia vs. Direttur tas-Sigurta' Soċjali*,²⁵⁶ which concerned an act of usury. In this case, the Court allowed the sum of money paid in usury to be restored to the aggrieved party.²⁵⁷

The position regarding the information held by the parties regarding the status of the obligation has been that knowledge is immaterial, and therefore natural obligations exist

²⁵¹ Criminal Code, Chapter 9 of the Laws of Malta, Article 338(ii)

²⁵² *Bartoli vs Chetcuti*, 13/06/2013

²⁵³ *ibid*

²⁵⁴ *Gio Maria Muscat vs. Carmelo Vella*, 25/02/1950, (First Hall Civil Court)

²⁵⁵ *ibid*

²⁵⁶ *Felix Farrugia vs. Direttur tas-Sigurta' Soċjali*, 19/10/2005, (Court of Appeal, Inferior)

²⁵⁷ *ibid*

objectively. Hence, natural obligations arise even if the parties are not aware of such obligation. *Parascandalo vs Lanzon*²⁵⁸ is the leading judgement in this regard.

3.1.3 Verbal Agreements

Consent given in the oral form is considered sufficient for an agreement to be considered valid between two or more parties. Oftentimes, the validity of a contract requires a higher level of manifestation of consent and not merely an oral expression. However, the law does not always specify the level of manifestation required for validity, and this means that the parties are free to manifest their consent in any matter; this is called ‘free manifestation.’ An increase of the level of manifestation required is the requirement of a private writing. The list of contracts that require such writing can be found in article 1232 of the Civil Code²⁵⁹, and some examples of such would be a promise of sale, a civil partnership, a promise of loan, a compromise, a suretyship agreement, and leases - these are referred to as ‘written manifestations.’ The ‘solemn manifestation’ comes about when the requirement of the law is that of a public deed. Some examples requiring of a public deed is the transfer of immovable property, the creation of real rights such as servitudes over immovable property, the hypothecation of property, the creation of emphytheusis, and a consensual deed of personal separation.²⁶⁰

3.1.4 Contract Law and Smart Contracts: a New Era?

The question that arises in the analysis of the principles and rules of our codes relating to contract law, is how can one ensure that a blockchain-based smart contract will satisfy all of the requirements of Maltese contract law? The complication of verbal agreements in the event of a dispute will also arise in disputes where the underlying agreement was finalised by means of a smart contract translated into the programming language used for blockchain.

The challenges faced traditionally with verbal contracts, are likely to be eradicated if smart contracts become a mainstream medium for entering into agreements, especially when taking into consideration that the agreement will be digitally translated for the purpose. How then

²⁵⁸ *Carmelo Parascandalo vs Procuratore Legale Pietro Paolo Lanzon* 17th April 1925 (Court of Appeal)

²⁵⁹ Civil Code (n4) Article 1232

²⁶⁰ *ibid*

will the parties ensure that the underlying requirements of contract law have been fulfilled? This and other questions are just some of the legal and regulatory challenges we will be facing in the near future.

3.1.5 The Enforceability of Gaming Debts and the Blockchain

The enforceability of gaming debts is an era of the law that was developed with the growth of the industry as we know it today. Maltese law requires that there is conformity between the internal consent and that which is manifested externally. If there is disparity within such, and a person does not externally manifest that which is internally intended, the consent would be deemed invalid. This disformity could be voluntary or involuntary. Involuntary disformity can be either due to error, violence or fraud.²⁶¹ In the former case of voluntary disformity, a person can manifest that which he does not voluntarily intend, this is referred to as ‘simulation’.

Simulation can either be absolute or relative; absolute simulation comes about when a person does not want to contract at all, but appears to intend otherwise. Relative simulation is when the party to the contract does want to enter into a specific type of contract and undertake obligations, but appears to want to enter into a contract of a different nature entirely. Absolute simulation is commonplace during separation proceedings between spouses when attempting to avoid the division of certain assets. A good rule of thumb when understanding the concept of simulation and the dealings with such by the courts, is that the general principle is that the truth prevails over appearance, and this is no less the case within gaming law disputes.

One such case is that of Borg vs Brignone²⁶², Court of Appeal 6 October 1999. The facts of the case were as follows: The defendant lost a substantial amount of money to Borg through illegal gambling. They drew up a contract stating that the defendant had loaned money from Borg, and that he was binding himself to repay him within a defined period of time. Borg then passed away, leaving his heirs the contract of loan. Borg’s heirs sought to obtain payment from Brignone through these proceedings. The Court eventually concluded that the contract was simulated, uncovering the true *raison d’être* behind its original drafting. Being

²⁶¹ Micallef vs. Micallef (22/2/2006) (First Hall, Civil Court)

²⁶² Borg Julia vs. Brignone Carmel, 6th October 1999, Court of Appeal (Civil, Superior)

an illegal contract, both in terms of the Criminal Code article 338(ii)²⁶³ as well as under article 1713 of the Civil Code,²⁶⁴ the contract was not enforceable by the Court, and hence, the Court dismissed the case, stating that *‘il-kuntratt minn fejn titwieled din l-obligazzjoni huwa null’*.

In Title XII Of Gaming and Betting, article 1713 of the Civil Code²⁶⁵, the legislator ensures that no action for recovery of a debt arising from gaming or betting exists. It states that:

The law grants no action for a gaming debt, or for the payment of a bet. Nor does it grant any action; (a) for the recovery of any sum lent by any person who knew that such sum was intended for gaming; (b) for the recovery of any sum lent by any person interested in the game, for the payment of money lost at such game.’

An exception to such provision is found in the Lotteries and Other Games Act Article 49(3)²⁶⁶ which states that:

The provisions of article 1713 of the Civil Code shall not prejudice (a) the right of a licensee, operator, permit holder or person referred to in subarticle (1), to recover a debt arising from the acceptance of payment of a stake by any of the means of payment referred to in subarticle (1)(a) in accordance with the provisions of the said subarticle (1)(a); or (b) the right of a winner of a monetary prize under an authorised game or, as the case may be, under a game operated in terms of a permit granted under regulations made under article 78(3), to recover any debt arising from acceptance of payment of such prize by any of the means of payment referred to in subarticle (1)(b).²⁶⁷

Further exceptions to the general clause held in article 1713 in the Civil Code²⁶⁸ are included in the subsequent articles. Article 1714 allows for games that, ‘tend to help training in the use of arms, foot-races, horse-races, boat-races, ball-games and other games of the same kind which develop the dexterity and exercise of the body’²⁶⁹ - an exemption from the antecedent article. The Court here still has discretion to reduce any sum claimed in case it appears to be

²⁶³ Criminal Code (n251) Article 338(ii)

²⁶⁴ Civil Code (n4) Article 1713

²⁶⁵ *ibid*.

²⁶⁶ Lotteries and Other Games Act, Chapter 438 of the Laws of Malta, Article 49(3)

²⁶⁷ Civil Code (n4) Article 1713

²⁶⁸ *ibid*

²⁶⁹ Civil Code (n4) Article 1714

excessive. The following article 1715²⁷⁰ provides for the nullity of any agreement attempting to circumvent articles 1714 and 1715 in their entirety. A further exemption to those exemptions already held in article 1714 is that article 1716²⁷¹ allows for the:

loser at a game, not included in those mentioned in article 1714 [to] recover from the winner the sum or thing which he has already paid to him, provided he shall, by means of a judicial act, within two months to be reckoned from the day of payment, call upon the winner to return the sum or thing so paid.²⁷²

This allows the losing party to reclaim that which he forfeited, but only in the case of games not listed in the exception held in article 1714.²⁷³

Gaming debts under Maltese legislation are only enforceable insofar as their applicability within the Lotteries and Other Games Act under article 49(3).²⁷⁴ An extension of enforceability of such debts would include those debts that are not enforceable per se but cannot be receded under the veil of natural obligations and *solutio retentio*. It is far easier to create documentary evidence by reducing the verbal agreement to a contractual writing. This prevents any issues of enforceability, bar those where any of the formal requisite elements of a contract are not present at the start. The law has evolved with the gaming industry to afford protection. Whether the law of the future will also follow suit for smart contracts based on the blockchain has yet to be seen, however we are already living during times where there are many plans on a governmental level to ensure that the protections found in our law for the consumer in most industries, will also be extended to new technological advances of blockchain.

3.2 Smart Contracts: an introduction

Smart contracts were conceived through an extended application of the technology behind the Bitcoin, first released through Nakamoto's 2008 white paper on the subject.²⁷⁵ These contracts are new methods that aim to ensure contractual compliance in all spheres of life,

²⁷⁰ Civil Code (n4) Article 1715

²⁷¹ Civil Code (n4) Article 1716

²⁷² *ibid*

²⁷³ Civil Code (n4) Article 1714

²⁷⁴ Lotteries and Other Games Act (n266) Article 49(3)

²⁷⁵ Nakamoto (n1)

from contracts of sale of goods to social contracts. They are predictable, redeemable and irrevocable. According to an interview with Andreas M. Antonopoulos:²⁷⁶

If you have a big transaction with a specific control structure, you can predict the outcome at any period in time. If I have a fully verified signed transaction with a number of signatures in a multi-signature account, I can predict whether that transaction will be verifiable by the network. And if it is verifiable by the network, then that transaction can be redeemed and irrevocably so. No central authority or third party can revoke it, no one can override the consensus of the network. That's a new concept in both law and finance. The bitcoin system provides a very high degree of certainty as to the outcome of a contract...People could shut down the Internet, and I could still transmit that transaction over shortwave radio with Morse Code. A government agency could try to censor my communication, and I could still transmit that transaction as a series of smiley emoticons over Skype. As long as someone on the other end could decode the transaction and record it in the blockchain, I could affect the [smart contract]. So, we've converted something that, in law is almost impossible to guarantee, into something that has verifiable mathematical certainty.²⁷⁷

Nick Szabo, the cryptographer known for his research on digital currency, highlighted the fact that smart contracts can capture a greater array of information but they are also much more dynamic than regular contracts. He defined smart contracts as follows:

A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitration and enforcement costs, and other transaction costs.²⁷⁸

²⁷⁶ Tapscott (n154) 47

²⁷⁷ *ibid*

²⁷⁸ Michael Gord, 'Smart Contracts Described by Nick Szabo 20 Years Ago Now Becoming Reality' (<https://bitcoinmagazine.com/articles/smart-contracts-described-by-nick-szabo-years-ago-now-becoming-reality-1461693751/>, 26 April 2016) <<https://bitcoinmagazine.com/>> accessed 30 July 2017

In 1995, Szabo wrote an article entitled ‘Smart Contracts,’ which was then published in 1996, in the magazine *Extropy*.²⁷⁹ This article accurately described the developmental breakthroughs in this technology that are currently at the forefront of the sector’s priorities. It also described the parameters and pros and cons of the application of blockchain technology in contracts.

Szabo defined a contract as being, ‘a set of promises agreed to in a meeting of the minds [which] is the traditional way to formalize a relationship.’ The predictions made in the aforementioned article included the digital revolution and the change that would come about in the way that individuals contracted with one another, moving away from the traditional sense of the contract and towards a more intangible ideology involving cyberspace. Szabo defined smart contracts as, ‘a set of promises, specified in digital form, including protocols within which the parties perform on the other promises’ without the use of artificial intelligence.²⁸⁰ He believed that the advancement of computers and their ability to run complex algorithms in a less costly manner than the current scenario allows, would make it more likely that smart contracts would come into mainstream usage.

Taking into consideration the underlying requirements of contracts typically found in contract law of many jurisdictions, Szabo went on to describe the four main objectives of a smart contract; those being observability, verifiability, privacy and enforceability, and he believed that smart contracts would enhance these objectives and make them more attainable goals. Smart contracts, as described by Szabo, enable both parties to the contract to observe the other party’s performance of the duties and obligations in the contract. Only upon completion up to the previously agreed standards, would the details necessary for the execution of the contract be disclosed to both parties, in effect making the contract self-enforcing, thereby eliminating the time spent enforcing the contract. When it came to smart contracts, Szabo emphasised the fact that the traditional terms and conditions often ‘hidden’ in regular contracts, is a problem for the individuals getting the short end of the stick. He believed that ensuring that all parties to the contract were in agreement on the exact terms to which they were binding themselves, was of utmost importance, and the ‘fine print’ that generally gets neglected in regular contracts, would need to be catered for in the ambit of smart contracts too. Generally, the terms and conditions in normal contracts would allow for some of the individual’s personal data to become available to the other individual (take the example of a

²⁷⁹ *ibid*

²⁸⁰ *ibid*

POS system in a shop which can take information from the paying customer without their explicit consent and store it in a database for future use). Szabo's solution to this ever-present issue was to integrate within the smart contract, a visual representation of the elements of a transaction, moving away from a representation based solely on code, in order to eliminate this 'hidden' aspect of contracts.²⁸¹

In 1995 local businesses benefitted from fairly low transport and communication costs, through the influx of new technologies like fibre optic cables. In order for such businesses to expand globally, there still existed certain legal barriers to trade that involved legal costs, and other barriers such as compliance to foreign laws and regulations. Szabo rightly predicted that smart contracts could potentially remove these barriers to global trade.²⁸²

Szabo also spoke about the possibility of embedding smart contracts into actual physical property – coining the term 'smart property.' The aim of this, would be for property to afford the right individuals automatic access depending on the terms in the contract. The example he used was that of a leased car which would automatically ensure return of the car to the loaner in the case that a lessee did not make payments on time, eliminating the possibility of theft and reducing the necessity for litigious proceedings.

Szabo's ideology, written remarkably before its time in 1995, and doubted by many, has now clearly appeared to have become reality.²⁸³ Back in 1995, the ideas Szabo put forward, did not have the required technology to realise them. Nakamoto's paper on Bitcoin changed all that.

Insofar as their application in real life scenarios, one such example would be as follows: Mary would like to invest in John's business, but she does not know enough in order to establish trust, and it does not make financial sense to go through the effort of attempting to establish that trust. She would however, like to diversify her investments, and investing in this business would be a good way to do so. Through smart contracts, she need not establish the trust herself, as it is already present through the automatic execution of the contract. This technology enables transactions that could not otherwise happen. The creators of the software have integrated these attributes into the blockchain infrastructure. According to Tapscott:

²⁸¹ ibid

²⁸² ibid

²⁸³ ibid

still, through smart contracts, executives can be held accountable – they must abide by their commitments as enforced and settled by software. Companies can program relationships with radical transparency so everyone has a better understanding about what each party has signed up to do. And overall, like it or not, they must conduct business in a way that is considerate of the interests of other parties. The platform demands it.²⁸⁴

Applied within different industries altogether, smart contracts could most definitely facilitate shipping transactions, whereby late arrival fees – previously agreed upon increments whereby a certain time correlated to an amount, a longer amount of time would mean a different amount – would be charged instantly, as well as any other pay-for-performance agreement.²⁸⁵ Their application could also extend to the trade of financial products through the use of ownership tokens.²⁸⁶

3.2.1 The Application of Smart Contracts in the Context of Traditional Contract Law

One of the most salient points in the application of new technology to the traditional notions of contract law, would be the fact that the change that is being made is not to these traditional notions, but to the method, or process, by which traditional contracts take place.

Changes have been made to the methodology behind contracts in the past, from digital signatures and electronic signatures²⁸⁷ being accepted in order to facilitate commerce through a modern-day application of this otherwise traditional concept. The contractual nature of gaming law evolved in line with the needs of the industry, and Malta remained at the forefront of worldwide online gaming, through the protection offered from our legislative developments in the field. Now, our standard contracts are facing new challenges with the progress of technology and the evolution of blockchain, extending into contracts and commonly referred to as smart contracts as defined in the preceding section of this thesis. The

²⁸⁴ Tapscott (n154) 109

²⁸⁵ Cornelius Grossmann, 'Blockchain: Five Profound Legal Impacts | Cornelius Grossmann | Pulse | LinkedIn' (2016) <<https://www.linkedin.com/pulse/blockchain-five-profound-legal-impacts-cornelius-grossmann?articleId=6214393509496131584>> accessed 14 June 2017.

²⁸⁶ *ibid*

²⁸⁷ Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures; EU regulation № 910/2014 of 23 July 2014 on electronic identification; and Electronic Commerce Act, Chapter 426 Laws of Malta

intricacies of contract law will now be confronted with new challenges brought about by this technological breakthrough.

3.2.2 An Exception to the Application of Smart Contracts

As with all new technology, there are certain exceptions to the application of smart contracts. It is a recommendation of the author, that public law, the realm of notarial law, be excluded from the application of smart contracts. This would imply that immovable property also cannot be the subject of smart contracts, leaving them squarely within the field of private law. This should alleviate many of the concerns surrounding their mainstream usage.

The oft-touted myth that lawyers will become useless in a world where smart contracts are commonplace is just that. As it stands, many standard contracts can be downloaded from the Internet, containing boilerplate clauses and standard language. The fact that these exist has not precluded contracting parties from seeking legal advice, and the author believes that smart contracts would present an extension of this current situation. One parting thought, which the author believes to sum up this issue entirely, would be the following:

Smart contracts do not replace fluid thought. They do not replace the intellectual ability of humans to consider all sorts of nuances, engage in balancing, trade-offs etc. They do not extend to events where things go wrong.²⁸⁸

3.3 Oracles

One of the major stumbling blocks of smart contracts when put into practice is their connectivity between the execution of the contractual clause and the real-world objects – when the blockchain is required to acquire information from the real world in order to execute a clause, certain problems arise. Oracles are middleware that link smart contracts to the real world, drastically amplifying their possible applications.

²⁸⁸ 'Will Ethereum Based Smart Contracts Automate Contract Lawyers?' (<http://www.trustnodes.com/2017/04/04/will-ethereum-based-smart-contracts-automate-contract-lawyers> , 4 April 2017) <<http://www.trustnodes.com/>> accessed 30 July 2017

An oracle creates a transaction that keeps data within the chain. It ensures that each node has an identical copy of this data, enabling it to be used in the execution of a clause within a smart contract.

Put simply, instead of requiring a smart contract to extract data from the real-world, an oracle inputs this data onto the blockchain, thereby removing this hurdle to their widespread use.

3.4 Conclusion

The applicability and possibility of the use of smart contracts extends to many areas. Applied within the realm of gaming, smart contracts can be used as a solution for bad debts, whereby the debt would not even reach the stage of being a debt per se, as it would automatically be paid to the person to whom it is owed. They could also provide a simple mechanism through which players can bypass waiting time for their funds to reach their bank account, which is one of the major stumbling blocks that gaming companies face when attempting to attract new customers. This technological advancement would save time, prevent litigious suits and small claims, thereby decreasing the burden on our courts, and remove certain barriers to gaming, further contributing to the increase in this sector's already sizeable²⁸⁹ contribution to Malta's annual GDP. When compared to other areas of the law, gaming law is fast changing for the needs and protections of the consumer, and the transparency offered by the blockchain-backed technology is likely to be a matter of course particularly when taking into consideration that the MGA is set to soon allow the implementation of cryptocurrencies for licensed operators in the near future.²⁹⁰ This is a clear indication that the legislator is preparing for the eventuality that blockchain based technology is a close reality, and one which requires the protection of the law.

²⁸⁹ "Provisional estimates published by the National Statistics Office (NSO) indicate that the gaming industry directly contributed 13% of the total economic gross value added (GVA) generated in the Maltese economy during the first quarter of 2017, an increase of 10% compared to the first quarter of 2016 reaching a total GVA of €277m." Malta Gaming Authority, 'The National Statistics Office Publishes its Quarterly Report – The Gaming Sector Continues to Grow' ([Http://www.mgaorgmt/national-statistics-office-publishes-quarterly-report-gaming-sector-continues-grow/](http://www.mga.org.mt/national-statistics-office-publishes-quarterly-report-gaming-sector-continues-grow/), 8 June 2017) <<http://www.mga.org.mt/>> accessed 30 July 2017 and National Statistics Office Malta, 'Provisional estimates indicate that the Gross Domestic Product (GDP) for the first quarter of 2017 amounted to €2,4921 million, an increase of €1445 million or 62 per cent when compared to the corresponding period last year. In real terms, GDP went up by 42 per cent' ([Https://nsogovmt/en/News_Releases/View_by_Unit/Unit_A1/National_Accounts/Documents/2017/News2017_093pdf](https://nsogovmt/en/News_Releases/View_by_Unit/Unit_A1/National_Accounts/Documents/2017/News2017_093pdf), 8 June 2017) <<https://nso.gov.mt/en/>> accessed 30 July 2017

²⁹⁰ MGA (n5)

Chapter 4: The Challenges and Opportunities Pertaining to Money Laundering and The Financing of Terrorism Insofar as The Blockchain And Cryptocurrencies

It is a generally agreed upon notion that blockchain technology and the Dapps²⁹¹ that use this technology as their backbone have not yet reached mainstream use. These applications have yet to reach their full potential, and the repercussions of their more widespread use have yet to be truly known to us. Hereunder we shall discuss the current Maltese and EU legislative framework, as well as the technical and legal challenges that implementation brings with it insofar as the blockchain and cryptocurrencies relate to the issues of money laundering and the financing of terrorism.

4.1 Cryptocurrencies: a Misnomer?

At this point in time, there exists a certain lack of regulatory coherence with regard to whether cryptocurrencies, such as Bitcoin or Ethereum, fall within the definition of ‘money’. As of present, there are no specific EU regulations in force pertaining to the legal definition of cryptocurrencies, although, as discussed in Chapter One, certain countries have already restricted or banned the use of cryptocurrencies in trade, implying that they are not to be considered as monies under the law of the land. This question is imperative as it henceforth relates to the laws and regulations that are to apply to these types of currencies should they be considered to fall within the definition of ‘money’.²⁹²

Should these currencies be deemed to form part of the definition of ‘money’, the implication would be that certain AML rules and regulations that are in force would therefore be applicable to the use of cryptocurrencies. The European Central Bank (ECB) has released two reports on the matter - an analysis of the position of the ECB as to the status of cryptocurrencies in this regard.

²⁹¹ Blockgeeks, 'Dapps And The Decentralized Future' (<https://blockgeeks.com/guides/dapps-the-decentralized-future>) <<https://blockgeeks.com/>> accessed 30 July 2017

²⁹² Anita Ramasastry, 'Is Bitcoin Money? Lawmakers, Regulators and Judges Don't Agree' (<https://verdictjustia.com/2014/09/09/bitcoin-money>), 9 September 2014 <<https://verdictjustia.com/>> accessed 30 July 2017

The first ECB report in 2012²⁹³ stated that: ‘a virtual currency can be defined as 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.’²⁹⁴ In the 2015 report,²⁹⁵ the ECB made a few amendments to the definition of ‘virtual currency’, and defined it as: ‘a digital representation of value, not issued by a central bank, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money.’²⁹⁶ The latter document goes on to say that:

Even if the terms ‘virtual currency’ and ‘virtual currency schemes’ are used in this report, Eurosystem central banks do not recognise that these concepts would belong to the world of money or currency as used in economic literature, nor is virtual currency, money, currency or a currency from a legal perspective.²⁹⁷

4.2 Directives,Laws and Regulations

The author believes that, considering the increased interest in cryptocurrencies and their burgeoning popularity, one must ensure that the current AML framework is sufficient in order to safeguard against abuse through this new medium, or whether the legislators ought to consider a revamp of the current system already in place.

4.2.1 The Current Regime on Money Laundering and the Financing of Terrorism

As established in Chapter One, the EU framework on payment services may be said to be comprised of the EMD1,²⁹⁸ the EMD2,²⁹⁹ the PSD1³⁰⁰ and the PSD2,³⁰¹ as well as the Money Laundering Directives.³⁰² These directives set the tone for the direction that the EU member

²⁹³ ECB (n7)

²⁹⁴ *ibid* 6

²⁹⁵ ECB (n123)

²⁹⁶ *ibid* 25

²⁹⁷ *Ibid* 23

²⁹⁸ EMD1 (n126)

²⁹⁹ EMD2 (n127)

³⁰⁰ PSD1 (n128)

³⁰¹ PSD2 (n129)

³⁰² MLD1; MLD2; MLD3; MLD4

states generally adopt towards payment services. The question arises as to whether such currencies fall within the ambit of these directives at all though, or whether the directives are merely tools with which to regulate fiat currencies solely.

The 1994 Prevention of Money Laundering Act (PLMA)³⁰³ has been amended over the years, resulting in the final product we see today. It is mostly comprised of EU directives and Financial Action Task Force (FATF) recommendations³⁰⁴ – the latter being a 1989 G7 initiative that formed an intergovernmental organisation that was tasked with the development of anti-money laundering policies. In 2001, its scope was expanded in order to include the policy development on the financing of terrorism.

The 2014 FATF Report on Virtual Currencies Key Definitions and Potential ML/TF Risks³⁰⁵ illustrated the potential risks that convertible virtual currencies pose to ML/TF. This report reiterates the risks that were identified in the 2013 NPPS Guidance,³⁰⁶ which states that:

The G20 Principles for Innovative Financial Inclusion issued in 2010 promote the application of the proportionality principle as the right balance between risks and benefits by tailoring regulation to mitigate the risk of the product without imposing an undue regulatory burden that could stifle innovation. On a general basis, the proportionality criteria have already been endorsed by the FATF Recommendations. The proportionality criteria allow countries to apply a risk-based approach.³⁰⁷

The 2014 report also highlights the risks pertinent to systems that are decentralised,³⁰⁸ citing their anonymity as the primary reason for such, as well as the fact that there is no centralised authority. Also, decentralised systems do not afford law enforcement officials the ability to target specific individuals. The report states that the situation is further exacerbated by the speed of technological advancements that are constantly being made in this regard, which do

³⁰³ The Prevention of Money Laundering Act, chapter 373, Laws of Malta

³⁰⁴ Financial Action Task Force, 'Guidance for a Risk Based Approach - Prepaid Cards, Mobile Payments and Internet-Based Payment Services' (<http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPSpdf>, June 2013) <<http://www.fatf-gafi.org/>> accessed 30 July 2017

³⁰⁵ Financial Action Task Force, 'Virtual Currencies Key Definitions and Potential AML/CFT Risks' (*14 FATF Report on Virtual Currencies Key Definitions and Potential AML/CFT Risks*, June 2014) <14 FATF Report on Virtual Currencies Key Definitions and Potential AML/CFT Risks > accessed 30 July 2017

³⁰⁶ NPPS Guidance (n304)

³⁰⁷ NPPS Guidance (n304)

³⁰⁸ FATF Report (n305) 9-10

not allow legislators and regulators to keep up with the requirements of the situation as it evolves.³⁰⁹

4.2.2 The Electronic Money Directive

EMD1 aimed at ensuring that technological advancements in e-money services were facilitated and catered for, whilst encouraging competition between the varied participants on the market.³¹⁰ In doing so, it regulated e-money institutions by setting up a list of rules in order to safeguard the single market for such services in the EU. The EMD1 was specifically drafted to ensure continuity and consistency with the PSD with the consumers' and businesses' best interests in mind.³¹¹

4.2.3 The Payment Services Directives

The Payment Services Directive (PSD)³¹² was adopted in 2007, and aimed at creating a single market payment system within the EU. It paved the way for modern payment services in the European Union, and simplified the processing of such payments, in order to create a competitive, efficient and innovative environment. The PSD also created the legal platform for the Single Euro Payments Area (SEPA) a method of transferring euro denominated payments.

The Second Payment Services Directive (PSD2)³¹³ was proposed in 2013, and the intention behind the Commission's proposal of this revision, was to standardise and integrate payment efficiency across the EU. This allowed for a higher standard of consumer protection, and reduced costs to the consumers whilst also benefitting smaller companies through the creation of an equal playing field for them to be more likely to enter into this realm of business.³¹⁴

³⁰⁹ *ibid*

³¹⁰ EMD1 (n126)

³¹¹ *ibid*

³¹² PSD1 (n128)

³¹³ PSD2 (n129)

³¹⁴ '5 Things You Need To Know About PSD2 ' (<http://www.sepaforcorporates.com/single-euro-payments-area/5-things-need-know-psd2-payment-services-directive/>, 13 October 2015) <<http://www.sepaforcorporates.com/>> accessed 30 July 2017

In the 2012 ‘Virtual Currency Schemes’ document published by the ECB,³¹⁵ it was stated that: ‘bitcoin clearly falls outside the scope of the Payment Services Directive (2007/64/EC)’.³¹⁶ However, in October 2015, the newly adopted PSD2 extended the scope of the Directive to cover ‘third party payment providers’.³¹⁷ While this is true, this does not necessarily mean that cryptocurrencies fall within the ambit of such a provision, since cryptocurrencies are not the same as e-money, and this seems to be the general focus of the provisions held within PSD2. Aside from this, the Directive refers to payment transactions that take place in the member state’s currency – cryptocurrencies are the official denominated currency of none of the member states, and hence, it can be deduced that they do not fall within the ambit of this directive.³¹⁸

4.2.4 The Money Laundering Directives

In 1991, the EU made its first strides towards the fight against money laundering, with the introduction of MLD1.³¹⁹ MLD1 strived to define the requisite terms relating to the sphere of money laundering, such as financial institutions, credit institutions and money laundering itself. The Know Your Client (KYC) procedures we are familiar with today, were introduced through this Directive, through obligations set in place whereby the aforementioned institutions were obliged to garner certain knowledge about their clients upon the opening of an account, at the start of a business relationship, and also when transactions amounted to more than €15,000. This paved the way for some of the AML regulations we still have in place today. The MLD1 also afforded these institutions the option of further examinations when a transaction, regardless of the amount, was considered suspect. These institutions were also obliged to keep proper records, enhance their compliance procedures and carry out the appropriate training to bring their employees up to date with the new Directive.

In 2001, MLD2,³²⁰ which served as an amending directive to MLD1, pre-empted the influx of money laundering in the EU, and served as a launching pad for other states, even non-EU

³¹⁵ ECB (n7)

³¹⁶ PSD1 (n128)

³¹⁷ PSD2 (n129)

³¹⁸ *ibid*

³¹⁹ Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering

³²⁰ Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering - Commission Declaration

member states, to begin regulation. MLD2 defined criminal activity as being: ‘any kind of involvement in the commission of a serious crime’³²¹ which comprised of one or more of the following:

human trafficking for sexual or labour exploitation by criminal organization, serious fraud against the EU budget, corruption, an offence which may generate substantial proceeds and which is punishable by a severe sentence of imprisonment in accordance with the penal law of the Member State.³²²

MLD3 voided the first two, and whilst, in principle keeping much of the content of the second directive, it made significant strides in strengthening the measures in place to fight ML/TF. The 2003 and 2004 FATF recommendations, both contributed many of the salient points held within MLD3. An important change that came about through this Directive was the change in definition of ‘money laundering’ to include:

the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such activity to evade the legal consequences of his action;

the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from criminal activity or from an act of participation in such activity;

the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such activity;

participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions mentioned in the foregoing points.³²³

³²¹ *ibid*

³²² *ibid*

³²³ Directive 2005/60/EC of The European Parliament and of The Council Of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing

Aside from that, the somewhat ambiguous definition of ‘serious crimes’ was extended to include:

all offences which are punishable by deprivation of liberty or a detention order for a maximum of more than one year or, as regards those States which have a minimum threshold for offences in their legal system, all offences punishable by deprivation of liberty or a detention order for a minimum of more than six months.³²⁴

The MLD4,³²⁵ is part of a Commission action plan specifically set up to work against terrorist financing, as well as being a response to the April 2016 Panama Papers³²⁶ scandals. It became applicable locally by the 26 June 2017.³²⁷ This Directive replaced the MLD3. Primarily, it places importance on ultimate beneficial ownership and increased customer due diligence (CDD), whilst expanding the definition of a politically exposed person and broadening the criteria.³²⁸ It also lowered the cash payment threshold for traders of goods to €10,000, whilst expanding the scope of its application to the entirety of the gambling sector and not just casinos as it was prior to this change.

The MLD4 has also established an enhanced risk-based approach, necessitating evidence-based measures in order to recognise various risks present between different entities. With the implementation of this measure, the requisite entities will be required to undertake an assessment, identifying any risks that might affect their particular business, including any risks posed by their individual customers or transactions.³²⁹

³²⁴ *ibid*

³²⁵ DIRECTIVE (EU) 2015/849 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC

³²⁶ The International Consortium of Investigative Journalists, 'The Panama Papers - Politicians, Criminals and the Rogue Industry That Hides Their Cash' (<https://panamapapers.icij.org>, x) <<https://panamapapers.icij.org>> accessed 30 July 2017

³²⁷ Financial Intelligence Analysis Unit Malta, 'EU Legislation' (<http://www.fiumalta.org/legislation/eu-legislation>, X) <<http://www.fiumalta.org/>> accessed 30 July 2017

³²⁸ MLD4 (n325) article 3(9)

³²⁹ Advancing Financial Crime Professionals Worldwide, 'European Union Fourth Anti-Money Laundering Directive' (<http://www.acams.org/aml-resources/eu-fourth-aml-directive>) <<http://www.acams.org/>> accessed 30 July 2017

The MLD4,³³⁰ was set to be revised through a proposition made in July 2016. At time of writing, the amendment is still being drafted. The amendment that the author believes to be most relevant to this thesis, is that relating to the definition of virtual currencies, referring to them as:

A digital representation of value that can be digitally transferred, stored or traded and is accepted by natural or legal persons as a medium of exchange, but does not have legal tender status and which is not funds as defined in points (25) of Article 4 of the Directive 2015/2366/EC nor monetary value stored on instruments exempted as specified in Article 3(k) and 3(l) of that Directive.³³¹

As well as an obligation on all member states to include this definition within their national AML legislation, the definition of ‘obliged entities’ is extended in the latest revision to include virtual currency platforms and wallet providers within the scope of the directive. This extension of the definition pertaining to obliged entities will thereby extend the responsibilities of verifying customer identities and ensuring the adequate monitoring of transactions to these entities.³³²

4.2.5 The Central Bank of Malta Act

The Central Bank of Malta Act (CBMA)³³³ defines ‘currency’ as being “euro banknotes or euro coins or any other note or coin, by whatever name called, which is legal tender in the country outside Malta in which it is issued.”³³⁴

‘Legal Tender’ is any official medium of payment recognised by law, that can be used to extinguish a public or private debt, or meet a financial obligation.³³⁵ The national currency is legal tender in practically every country. A creditor is obligated to accept legal tender toward repayment of a debt. Legal tender can only be issued by the national body that is

³³⁰ MLD4 (n325)

³³¹ “MLD5” is not actually a Directive but a temporary name in reference to the upcoming MLD5 which – at time of writing – is still being drafted.

³³² Holly Whitehead, 'Five key points of the upcoming Fifth Anti Money Laundering Directive (5AMLD)' ([https://www.int-comp.com/ict-views/posts/2017/04/10/five-key-points-of-the-upcoming-fifth-anti-money-laundering-directive-\(5amlld\)/](https://www.int-comp.com/ict-views/posts/2017/04/10/five-key-points-of-the-upcoming-fifth-anti-money-laundering-directive-(5amlld)/), 10 April 2017) <<https://www.int-comp.com/>> accessed 30 July 2017

³³³ Central Bank of Malta Act, Chapter 204 of the Laws of Malta

³³⁴ *ibid* article 44

³³⁵ Investopedia, 'Legal Tender' (<http://www.investopedia.com/terms/l/legal-tender.asp>) <<http://www.investopedia.com/>> accessed 30 July 2017

authorised to do so, such as the US Treasury in the United States and the Royal Canadian Mint in Canada.³³⁶

This definition, by extension, does not seem to apply to cryptocurrencies, unless they are eventually considered to be legal tender in Malta.

This is one of the primary obstacles that Bitcoin and other cryptocurrencies will need to overcome should they ever become mainstream parts of the way a society transacts. Seeing as it is not illegal per se to accept payment for a service or a good in anything other than legal tender, it is still a possibility that shops and businesses can choose to accept cryptocurrencies as payment of their own accord.

4.2.6 The Prevention of Money Laundering Act

The Prevention of Money Laundering Act (PMLA)³³⁷ makes provision for the prevention and prohibition of the laundering of money in Malta. This act, rather than defining currency, defines property, since money laundering is broader than merely dealing with physical monies. It is defined in article 2³³⁸ as follows:

- (a) any currency, whether or not the same is legal tender in Malta, bills, securities, bonds, negotiable instruments or any instrument capable of being negotiable including one payable to bearer or endorsed payable to bearer whether expressed in euro or any other foreign currency;
- (b) cash or currency deposits or accounts with any bank, credit or other institution as may be prescribed which carries or has carried on business in Malta;
- (c) cash or items of value including but not limited to works of art or jewellery or precious metals; and
- (d) land or any interest therein;³³⁹

³³⁶ *ibid*

³³⁷ PMLA (n303)

³³⁸ PMLA (n303) article 2

³³⁹ PMLA (n303) article 2(a)

Through extension of the fact that Bitcoin and other cryptocurrencies are not considered legal tender insofar as the CBMA, but they fall outside the remit of such definition, they might actually be caught within the brackets of the definition set out in the PMLA through Article 2(a),³⁴⁰ which does not only apply to legal tender, but currency as a broader definition.

The determination of this is as yet unanswered, as to date, we do not have a conclusive case as to whether cryptocurrencies are to be considered currencies under Maltese law. While it is true that there have been no cases in the Courts of Malta, that does not exclude the assessment of similar cases in foreign jurisdictions. One such case was the US judgement *Securities and Exchange Commission v. Trendon T Shavers and Bitcoins Savings and Trust*,³⁴¹ where Bitcoin was determined to be a currency for the purposes of a conviction in fraud. In the case *Florida v Michell Espinoza*,³⁴² the Court held that Bitcoin is not to be considered legal tender for the purposes of the case.

Another notorious incident is one that was referred to in Chapter One, *United States v Ross Ulbricht 'Silk Road'*,³⁴³ where a federal court found Ross Ulbricht (the alleged mastermind behind the Silk Road), guilty of a myriad of offences, including money laundering charges based on the affirmation that Bitcoin was a currency for the purposes of conviction.³⁴⁴

The lacunae in the law that the refusal to regulate or recognise cryptocurrencies could lead to are not ideal, and hence, it is recommended that Malta paves the way towards recognition and regulation in the near future. This being said, the MGA and other bodies are already working towards such regulation.³⁴⁵

4.2.7 The Prevention of Money Laundering and Funding of Terrorism Regulations

In the preamble of the Regulations, it is made clear that the *raison d'être* of the regulations was to implement the MLD3 and as such, it mostly emulates that directive. There are a few

³⁴⁰ PMLA (n303) article 2(a)

³⁴¹ *Trendon T. Shavers* (n115)

³⁴² *State of Florida, 11 Circuit, The State of Florida v. Michell Abner Espinoza*, Case Number F14-2923

³⁴³ *Ross William Ulbricht* (n82)

³⁴⁴ Mike Masnick, 'Judge Not Impressed By Ross Ulbricht's 'But Bitcoin Isn't Money' Defense' (<https://www.techdirt.com/articles/20140710/06513427836/judge-not-impressed-ross-ulbrichts-bitcoin-isnt-money-defenses.html>), 10 July 2014) <<https://www.techdirt.com/>> accessed 30 July 2017

³⁴⁵ Refer to Chapter 4.2.8

differences between the directive and the regulations, most glaringly being the extension of the application of the regulations to ‘apply where any “relevant financial business” or any “relevant activity” as defined in the regulation is undertaken or performed through the Internet or other electronic means.’

Coincidentally, the regulations echo the 2013 NPPS Guidance, which advocates a risk-based approach.³⁴⁶ This kind of approach allows for the FIAU and other authorities to ensure that they tackle high risk situations and areas before others. The regulation obliges the entities to determine the risk that an applicant for business, or one already in a business relationship, poses, based on the listed criteria as follows: ‘customer background, country of origin, business activities, products, linked accounts or activities and public or other high profile positions.’³⁴⁷

4.2.8 The Malta Gaming Authority’s Stance

Currently, Malta has yet to legislate on Blockchain and Bitcoin, although, as mentioned in Chapter One, the Prime Minister has stated that legislation is imminent.

The author made reference to the Malta Gaming Authority, who were very forthcoming and answered a few questions regarding the current legal status of Bitcoin and other cryptocurrencies insofar as gaming applications are concerned, and whether the MGA has any plans in the pipeline to change this legal status.³⁴⁸

Currently, the MGA’s available licensees are not permitted to accept cryptocurrencies directly for deposits and/or wagers on the MGA-regulated offer. Should they wish to do so on the same URL as an MGA-regulated offer, but under separate regulation, the wallets would need to be separate (i.e. even if they use a payment service provider which also acts as a Bitcoin or other cryptocurrency exchange there can be no co-mingling of the funds in that respect). On the other hand, if the cryptocurrency is used solely as an exchange mechanism for quicker deposits and pay-outs, with the operator itself never coming into contact with cryptocurrency, but dealing solely in fiat currency, this is something that the MGA would assess on a case-by-case basis, as there is currently no standardised position on this vis-à-vis the Government.

³⁴⁶ NPPS Guidance (n304) article 7(9)(b)

³⁴⁷ NPPS Guidance (n304)

³⁴⁸ Email correspondence with Dr. Carl Brincat at MGA

In order to take the requisite steps forward in the acceptance of this new technology, the MGA has already commissioned a study, together with other national stakeholders, including the Malta Financial Services Authority (MFSA), the Central Bank of Malta (CBM), and the Financial Intelligence Analysis Unit (FIAU), split into two phases: Phase 1 is to identify the main risks (this has already been concluded but has not yet been made available to the public); and Phase 2 with the objective of developing the necessary framework to ensure that there are sufficient safeguards in place, such that the introduction of cryptocurrencies in the regulated environment does not prejudice their main concerns and objectives as a regulator. The Chairman of the MGA, Mr. Joseph Cuschieri, has mentioned this publicly in various fora.³⁴⁹

I am furthermore pleased to report that the Authority is undertaking in-depth studies on the role which crypto-currencies can play within the Maltese regulatory regime. In the context of the rapid developments in this area, which are taking place at a global level, the Maltese regulatory system cannot afford any loss in competitive edge in this regard, especially to sustain its reputation as a forward-looking jurisdiction which is friendly to compliant businesses. For this reason, the Authority is actively evaluating the circumstances and requirements necessary, which could eventually enable operators to conduct business in this manner as well. I am sure that this will also have important implications with respect to the interface between the gaming industry and capital and financial markets in Malta.³⁵⁰

³⁴⁹ *ibid*

³⁵⁰ Malta Gaming Authority, 'Capital Market Resources Towards the Development of Remote Gaming in Malta Speech delivered by Chairman, Malta Gaming Authority' ([Http://www.mgaorgmt/wp-content/uploads/Capital-Markets-and-Gaming-Speech-by-MGA-Chairmandocx-1pdf](http://www.mgaorgmt/wp-content/uploads/Capital-Markets-and-Gaming-Speech-by-MGA-Chairmandocx-1pdf), 28 April 2017) <<http://www.mga.org.mt/>> accessed 30 July 2017

4.3 Cryptocurrencies, the Blockchain, Money Laundering and the Financing of Terrorism

There are three stages of money laundering; placement, layering, and integration. The placement stage is the transfer of money from its original source.³⁵¹ Sometimes, the launderers are able to disguise or misrepresent the source and then place the cash into circulation through casinos, shops, financial institutions and the like.

There are many different ways in which this first stage of money laundering can be carried out. Currency smuggling requires the physical movement of the monies out of the country; bank complicity is a route often taken in jurisdictions where banks are amenable to bribery or where they are controlled by crime groups or families thereby removing the regular checks and balances one would find at a legitimate financial institution. The facilitation of foreign exchange markets in some jurisdictions has left them susceptible to money laundering through currency exchanges; brokers who would be able to disguise the original source of the funds through certain corporate structures. Financial institutions might also be used in order to hide the laundered money within clean money, which would require front companies and businesses in order to 'legitimise' the source of income.³⁵²

The second stage of a money laundering operation is that of layering. The idea behind this step is to make it more difficult for the authorities to detect money laundering. After the first stage of placement is successful (if within a bank or financial institution), the newly laundered money can be converted into monetary instruments such as banker's drafts. If the first stage did not require any financial institution, this stage would often require the resale of local assets, making the profit harder to trace.³⁵³

The final stage of money laundering is integration, which requires the already laundered money to be moved through the banking system and into the economy making it seem as though it was earned through legitimate means. This can be done through the purchase of

³⁵¹ 'Money Laundering in the EU' (<http://people.exeter.ac.uk/watupman/undergrad/ron/methods%20and%20stages.htm>, x) <<http://people.exeter.ac.uk/>> accessed 30 July 2017 and About business crime solutions inc, 'Money Laundering: A Three Stage Process' (https://www.moneylaundering.ca/public/law/3_stages_ML.php, x) <<https://www.moneylaundering.ca/>> accessed 30 July 2017 and Paul Renner, 'What is Money Laundering? The Three Stages in Money Laundering...' (<http://kycmap.com/what-is-money-laundering>) <<http://kycmap.com/what-is-money-laundering/>> accessed 30 July 2017

³⁵² *ibid*

³⁵³ *ibid*

legitimate businesses, investing in luxury goods or high-end assets, and through the purchase of both residential and commercial properties.³⁵⁴

Cryptocurrencies and ML/TF have a quasi-symbiotic relationship, with both creating the perfect storm for money laundering if not regulated properly. Cryptocurrencies afford the user the ability to transfer funds anonymously without authority supervision or regulation, and this is largely due to the lack of regulatory coherence surrounding the topic of cryptocurrencies. When altcoins are kept in a wallet (apps that are easily downloadable), it is fairly straightforward to launder that money (the origin of which is not known and is undeclared) and spend it in fiat currency or converted into fiat currency and deposited into a bank.

The current situation in Malta does not allow for cryptocurrencies to be used in gaming, as the MGA does not license operations that do not use fiat currencies. While this remains the current situation, it is also a fact that many foreign operators that use cryptocurrencies are not regulated by the MGA and have no intention of becoming so regulated, as it is very easy for them to avoid the need for regulation, as discussed in the paragraph below. One such example is SatoshiDice,³⁵⁵ a game set up by individuals that can be played in Malta, where the prize is given to the player in Bitcoin. Its lack of regulation in Malta does not stop Maltese individuals from playing, nor does it stop foreign-regulated companies from offering their services to Malta. The MGA, should they wish to proceed against these unregulated providers, it would be difficult to find the UBO of the company in order to take any action against them.

The author believes that the types of gambling sites that are dabbling in cryptocurrencies can best be divided into three: (a) those that require no registration by the client in order to set up an account with them - in this case the client would just deposit their cryptocurrency without signing up, simply using a pseudonym; (b) sites that require registration with an email address but have very lax requirements, so the names can be anonymised through false information that is never actually verified; or (c) fiat gambling sites that accept cryptocurrencies, which are not anonymous and would generally require a higher level of information such as country of residence, date of birth and full name and surname for

³⁵⁴ *ibid*

³⁵⁵ Satoshi dice, (<https://satoshidicecom/dice>, x) <<https://satoshidice.com/>> accessed 30 July 2017

registration. This being said, it is still fairly easy to sign up, and upon registration, the altcoins can be deposited through the games.³⁵⁶

Once the wallet contains Bitcoin or any other altcoin, the question arises as to what to do with the money. There are certain companies that create tangible plastic cards – resembling regular bank-issued credit or debit cards – that link to the wallet. This implies that an individual can pay via card wherever such card-payments are accepted in the currency of the area. Monaco,³⁵⁷ Bitpay³⁵⁸ and TenX³⁵⁹ are all examples of this service. These cards link altcoins to Visa cards allowing them to be used virtually anywhere. Many of these companies are registered in the Isle of Man, where they have lower regulatory standards for these kinds of ventures. The authorities in the Isle of Man would necessarily have to report the individual or individuals at fault to their home country authorities, however, one cannot be sure whether this reporting takes place.

If one takes a closer look at SatoshiDICE, for example, it is a blockchain-based betting game that allows for wagers on the game to be sent without access to the website. A transaction is made in Bitcoin to one of the addresses operated by the service. The service then determines whether the individual wins or loses, and sends the appropriate transaction in response with the pay-out in the case of a winning bet, or a fraction of the house's gain in the case of a losing bet.³⁶⁰

There are various ways in which ML/TF can take place through online gaming sites. One such example is when a player uses a method of payment that holds a different name than that of the account holder – perhaps suggesting that the name is a pseudonym. Another method is when a single player opens a multitude of accounts with different operators that allow the winnings to be converted into actual currency. This might also be tweaked slightly

³⁵⁶ 'Best Bitcoin Gambling Sites of 2017' (<https://gamblingbitcoin.com/bitcoin-gambling-sites>) <<https://gamblingbitcoin.com/>> accessed 30 July 2017

³⁵⁷ Monaco, 'MCO Token began trading on Bittrex, Liqui, Gatecoin & Livecoin' (<https://www.mona.co/tokensalehtml>) <<https://www.mona.co/>> accessed 30 July 2017

³⁵⁸ 'Load dollars using any bitcoin wallet, spend anywhere' (<https://bitpaycom/card/https://bitpaycom/card>) <<https://bitpay.com/>> accessed 30 July 2017

³⁵⁹ Making Cryptocurrencies Spendable Anytime Anywhere' (<https://www.tenxtech>) <<https://www.tenx.tech/>> accessed 30 July 2017

³⁶⁰ 'Satoshi Dice' (https://en.bitcoin.it/wiki/Satoshi_Dice, x) <https://en.bitcoin.it/wiki/Satoshi_Dice> accessed 30 July 2017

but would result in the same conclusion, whereby the same player opens multiple accounts with a single operator, allowing for them to circumvent checks on their total winnings.³⁶¹

That being said, the anonymous aspect of cryptocurrencies is not entirely anonymous, as it is more similar to being pseudonymous as described in Chapter Five. Operators, on the other hand, would also need to conform to KYC policies in their licensing jurisdiction. It is when these regulations are not well enforced or not up to standard that an issue starts to arise.

There are already KYC procedures in place in order to verify clients' identities, but there are also gaming operators that disregard their countries' laws and regulations, due to the ease by which one can evade these systems, since the nature of their business is online and intangible.

The RGR³⁶² impose a certain standard on licensees in order to ensure the verification of the identity, age, and place of residence of any player before they make a payment of more than €2,329.37 out of their account to another player.³⁶³ An important point of note is that the RGR do not take into consideration the prevention of financing of terrorism and only focuses on money laundering and the prevention thereof.

4.4 The Way Forward

In an article published in the newspaper MaltaToday on the 23 July 2017, entitled 'Malta lays the Groundwork for a Blockchain Revolution',³⁶⁴ Silvio Schembri, the Parliamentary Secretary for the Digital Economy, stated that plans for Malta to begin to embrace this technology are twofold: for blockchain to be used across the board in the public sector, and then for Malta to become a hub – much like it did for the gaming industry – for international companies that operate using this technology. Thus, Malta's legislative intentions in this regard are being formulated.³⁶⁵

The Maltese government is eyeing plans to implement Blockchain technology within the lands registry and the national health registries, ensuring a greater standard of transparency, security and a more cost-efficient method of storage – making it impossible for files to get

³⁶¹ Kathleen Sare, *The Use of Cryptocurrencies in Gaming: The Legal and Regulatory Considerations* (April 2016) 45 - 46

³⁶² RGR (n96)

³⁶³ RGR (n96) article 36

³⁶⁴ Diacono Tim (n230)

³⁶⁵ *ibid*

misplaced or lost. This will change the way that people and the government interact – from a transparent and easily accessible lands registry, to the ability to have control over health data to possible future extensions of the application of technology in the future.³⁶⁶

³⁶⁶ *ibid*

Chapter 5: Other Challenges and Opportunities in Gaming Law

5.1 The Technical Challenges to Implementation

Like many revolutionary technologies, there is promise, and there is peril to any attempt at implementation. Change is oft not welcomed by the mainstream populace, and it is for this reason that acceptance is made more difficult for something as intangible a concept as the blockchain. Generally speaking, when people do not understand something, it is far harder for them to accept it.

There are, as with all things, certain challenges to the implementation of blockchain technology on a mainstream level. These can be taken as challenges that can be overcome, or they can be determined insurmountable obstacles to the influx of this new wave of technology.

The challenges that will be assessed forthwith will be of a legal and a technical nature. The first part of this chapter will tackle the technical aspect whilst the second part will tackle the legal aspect.

5.1.1 The Technology Might not be Ready for the Mainstream

The fact that many individuals have yet to be exposed to even the purest conceptual form of cryptocurrencies and blockchain means that their understanding is likely far from ready to accept its use in everyday situations. Bitcoin has already received some negative press due to the Silk Road³⁶⁷ and Mt. Gox,³⁶⁸ amongst other occurrences, and this notorious reputation will not help the cause. There are at least eight issues that make up this problem of lack of appeal to mass consumers, and those will be discussed hereafter.

5.1.1.1 Infrastructure

Infrastructurally, there are no adequate exchanges or enough ATMs that dispense Bitcoin, so even in the midst of a financial crisis, should consumers suddenly wanted to use Bitcoin, they would have difficulty finding a source in their vicinity. If there was a crash of their currency, similar to the recent financial situation in Greece, would anyone have managed to exchange

³⁶⁷ The Silk Road (n2)

³⁶⁸ Mt. Gox (n50)

their fiat currency into a different, more stable cryptocurrency? This is highly unlikely, and it encapsulates a perfect example of a lacking infrastructural model insofar as mainstream consumption is concerned.³⁶⁹

Andreas Antonopoulos, a computer scientist who, due to his experience in the field, has been labelled one of the most influential people in Bitcoin³⁷⁰, has stated that this technology will give everyone:

the same capability a banker has today, not just access to a bank account, but access to the full power of a financial institution — the ability to trade and transact anywhere in the world in very, very short time — 24 hours a day, 365 days a year without limitations in any currency.³⁷¹

This holds true only if Bitcoin becomes a mainstream commodity, but until then, Antonopoulos also believes that the necessary infrastructure required to make this happen does not yet exist, and specifically mentions the 2015 economic crash in Greece as an example of this³⁷².

5.1.1.2 Transactional Capacity

Should the masses suddenly attempt to make use of the Bitcoin blockchain, it does not currently have the capacity to cater to that many people. If the people of Greece all attempt to use it at once, the outcome would be one with an increase of spam, a decrease of security, system failures, bugs, and the subsequent disappointment of all the new users, which would be an insurmountable setback for the technology.³⁷³

5.1.1.3 Inaccessibility

There exists an element of user unfriendliness when it comes to the interface with which one must interact in order to use Bitcoin. These require the individual to be code-compliant, which many users are not. ‘Most Bitcoin addresses are simply strings of between twenty-six

³⁶⁹ Tapscott (n154) 255

³⁷⁰ Allen Scott, 'The 10 Most Influential People in Bitcoin' (<https://newsbitcoin.com/top-10-influential-people-bitcoin/>, 13 April 2016) <<https://news.bitcoin.com/>> accessed 30 July 2017

³⁷¹ *ibid*

³⁷² Tapscott (n154) 255

³⁷³ *ibid*

and thirty-five characters beginning with a one or a three,' making them fairly difficult to type – it can be likened to an accelerated version of entering your card number into an online in order to make a purchase: tedious, frustrating and fraught with the real possibility of entering text and number incorrectly. There remains a lot of work to be done in order to bring blockchain technology to the masses, especially insofar as user interface and user experience are concerned.³⁷⁴

5.1.1.4 Illiquidity

As mentioned previously, the illiquidity of Bitcoin is due to the fact that the cryptocurrency is finite in quantity. There can only ever be 21 million BTC by the year 2140, these are also being mined at a diminishing rate. As of the 28th July 2017, the current amount of BTC in circulation reached 16,475,363.³⁷⁵ The monetary policy used to govern the Bitcoin system was discussed in depth in Chapter One. The fact that all Bitcoin terminology is likened to the mining of gold is no coincidence. The supply of the commodity does not change to keep the value the same, the value changes constantly and the supply is predetermined. This implies an increase in the value per coin upon an increase in users.

The illiquidity problem is not that hard to tackle – it is a question of making the use of Bitcoin the norm, where people can issue gift cards to each other, stores accept it as a form of payment etc., allowing for more and more people to be exposed to it and increasing the likelihood of it being used as a day-to-day currency.³⁷⁶

5.1.1.5 High Latency

The fifth issue is that of high latency. Latency is defined as:

The amount of time a message takes to traverse a system. In a computer network, it is an expression of how much time it takes for a packet of data to

³⁷⁴ *ibid*

³⁷⁵ 'Bitcoins in circulation' (<https://blockchaininfo/charts/total-bitcoins>) <<https://blockchain.info/>> accessed 30 July 2017

³⁷⁶ Tapscott (n154) 256

get from one designated point to another. It is sometimes measured as the time required for a packet to be returned to its sender.³⁷⁷

High latency in the context of Bitcoin is still faster than many of the payment mechanisms which we are currently accustomed to, but being at the cutting edge of technology, ten minutes, which is the current latency for Bitcoin is simply too long for the instantaneous nature of the Internet. Ten minutes can mean a difference in the price of goods that are time-sensitive, due to market timing attacks³⁷⁸ for example.

In Chapter One, the concept of different people changing the source code to suit their developing needs was discussed in depth. This fork in the Bitcoin code base would allow for the development of new altcoins that have a faster latency, such as Litecoin - with a block time of 2.5 minutes - a quarter of that of Bitcoin.³⁷⁹ Ripple³⁸⁰ and Ethereum,³⁸¹ although not mere changes in the Bitcoin source code, are two other blockchain platforms with an even shorter latency, that spans seconds, rather than the customary minutes seen with other blockchains.³⁸²

5.1.1.6 Behavioural Change

Netiquette has been defined as: ‘the rules of etiquette that apply when communicating over computer networks, especially the Internet.’³⁸³ The concept of netiquette will pave the way for the masses to become more technologically savvy in their use of block chain, thus minimising any teething problems for new users.

Aside from netiquette, we must learn to change the way we react to issues arising from our financial transactions. Credit card problems, ATM glitches and other stumbling blocks can be easily sorted out by calling the financial institution and sorting out the problems *viva voce*

³⁷⁷ 'Latency Definition' ([Http://www.lininfo.org/latencyhtml](http://www.lininfo.org/latencyhtml)) <<http://www.lininfo.org/>> accessed 30 July 2017

³⁷⁸ Ken Griffit and Ian Grigg, “Bitcoin Verification Latency: The achilles Heel for Time Sensitive Transactions,” white paper, February 3, 2014; <http://iang.org/papers/Bitcoinlatency.pdf>, accessed June 7th 2017; A timing attack is a security exploit that allows an attacker to discover vulnerabilities in the security of a computer or network system by studying how long it takes the system to respond to different inputs. (<http://searchsecurity.techtarget.com/definition/timing-attack>)

³⁷⁹ Tapscott (n154) 257

³⁸⁰ *ibid*

³⁸¹ *ibid*

³⁸² *ibid*

³⁸³ 'Netiquette' ([Http://www.dictionary.com/browse/netiquette](http://www.dictionary.com/browse/netiquette)) <<http://www.dictionary.com/>> accessed 30 July 2017

or by sending an email. There is widely understood protocol in place for a forgotten password, lost cheque book, or misplaced credit card. All can be replaced with the minimal downtime for customers. Generationally, we are not accustomed to having to back up our ‘money’ onto a storage device or on the cloud. Ensuring that we do not forget our passwords and making sure we keep our backups in diversified locations, in case something should happen to the primary place of use, are not yet ingrained into our behavioural patterns. If we attempt to transfer our assets to the blockchain, and neglect to take these necessary steps, we will quite simply lose our money. There is no 24/7 assistance available. It is the sole responsibility of the owner of the currency to take absolute care of its accessibility.

‘With great power, comes great responsibility’,³⁸⁴ nowhere is this more relevant than in this technologically advanced age, where the increase in the freedom we have with our monies is directly proportional to the increase in our responsibility to manage it appropriately and to safeguard against losses. In order to mitigate this responsibility though, there does exist the option of third party back up services.

5.1.1.7 Lack of Legal Recourse

In a situation where our transactions become irrevocable and the contracts we ‘sign’ become unavoidable, we leave little room for human beings. In the blockchain, we have basically eliminated the risk of non-performance of a contract. Nowadays, not all contract breaches become litigious - sometimes do not find the idea of proceedings in court to be worth their time, effort or money. How will the courts treat the case of a Bitcoin contract breach? Would we be able to discover the identity of the online counterparty? These are questions that can likely only be answered through the passage of time and experience, but the first ‘guinea pigs’ to this new blockchain world are going to be very interesting to follow, and will likely shape the way of the future.³⁸⁵

³⁸⁴ ‘Quote Investigator: Exploring the Origins of Quotations’ (<http://quoteinvestigator.com/2015/07/23/great-power/>, x) <<http://quoteinvestigator.com/>> accessed 30 July 2017

³⁸⁵ Tapscott (n154) 258

5.2.1 Unsustainable Energy Consumption

Nathan Schneider, the author of a 2015 article entitled 'After the Bitcoin Gold Rush',³⁸⁶ published on The New Republic's website, questioned the effort required to mine Bitcoin:

'Mining' is the engine that keeps the Bitcoin network working, but it has swelled into a resource-hungry, capital-intensive, centralized syndicate. Is the Internet's native currency worth all the effort? All that computing power, which could be curing cancer or exploring the stars, is locked up in machines that do nothing but process Bitcoin-type transactions.³⁸⁷

The consumption of energy required in order to mine Bitcoin is a huge problem for the future of the industry. The aforementioned article stated that: 'processing and protecting the more than \$3 billion worth of bitcoins in circulation requires more than \$100 million in electricity each year, generating a volume of carbon emissions to match.'³⁸⁸ The energy level required is inordinately high, both that required to run the equipment used to mine (the CPUs), as well as the energy required to cool down the processors after they do the work. In fact, many mining facilities are often located in cooler climates – placing Malta in an undesirable position in this regard.

When the value of Bitcoin increases, so does the competition to mine it. This increase in competition brings with it an increase in computing power used towards this end, and hence, each computational algorithm becomes increasingly difficult as more CPUs attempt to solve it. This is based on the hash rate, as described in Chapter Two. Stephen Pair, who is the CEO of BitPay said that 'all forms of money have a relationship to energy',³⁸⁹ and this, in the context of both fiat currencies and commodities like gold is actually true. Gold requires actual mining – which uses up energy. In order to manufacture gold artificially one would need even more energy, Pair here alludes to the concept of nuclear fusion.³⁹⁰

Eric Voorhees, who founded the coin exchange ShapeShift,³⁹¹ argues that the high energy consumption required to mine Bitcoin is similar to that used to keep banks functional – from

³⁸⁶ Nathan Schneider, 'After the Bitcoin Gold Rush' (www.newrepublic.com/article/121089/how-small-bitcoin-miners-lose-crypto-currency-boom-bust-cycle, 25 February 2015) <www.newrepublic.com/> accessed 30 July 2017

³⁸⁷ *ibid*

³⁸⁸ *ibid*

³⁸⁹ Tapscott (n154) 260

³⁹⁰ *ibid*

³⁹¹ 'About the Exchange' (<https://info.shapeshift.io/about>, x) <<https://info.shapeshift.io/>> accessed 30 July 2017

the lighting in the actual buildings, to the armoured trucks driving and using fossil fuels, to the complex security systems in place. He says that it is ‘not quite clear which is worse.’³⁹²

5.2.2 Governments Might Thwart it

Josh Fairfield, Professor of Law at Washington and Lee University School of Law, does not believe the court systems in place can effectively tackle the issues that arise through the widespread use of blockchain technologies, and he says:³⁹³

They (the courts) think that physicality is the dividing line between virtual property and intellectual property, and it’s not, there’s no intellectual property element, there’s no part of a bitcoin that is intellectual property, there’s no creative spark for copyright, there’s no patentable idea, there’s no patent, there’s no trademark.³⁹⁴

Until the technologies are properly understood, the likelihood of failure is high. Until they are understood, one cannot regulate them, put policies in place or safeguard the users. Law and policy will only be a setback unless done properly from the outset. The application of laws that are already in place to suit technologies that are current and future will not work. The current legal framework will likely fail at handling the questions and issues that will arise once people start using this technology more frequently. The dissemination of information, grass roots discussions, seminars and think tanks that include all the stakeholders in this technology, must be set up and put into play if we are ever to be at the forefront of these breakthroughs.

Fairfield stated in the same interview that: ‘the real fight is how do we take old rules meant for old technology and adapt them rapidly and competently,’³⁹⁵ Tapscott continues, ‘in order for them to be recognisable when we start using them but iterated so that they’re state of the art when the technology really hits’,³⁹⁶ Herein lies the challenge that Malta will face.

³⁹² Tapscott (n154) 260

³⁹³ Tapscott (n154) 263

³⁹⁴ *ibid*

³⁹⁵ Tapscott (n154) 264

³⁹⁶ *ibid*

5.2.3 Privatisation vs Accessibility

When powerful corporations and individuals use technology in their empires and privatise it in order to make the most out of it financially, the masses suffer the consequences of that lack of accessibility. Much of our digital experience has already fallen victim to this brand of usurpation, from using the App Store and Google Play Store in order to download independent applications on our phones, to search engines being rife with advertisements.

While this remains a stumbling block to blockchain technology, there is actually a fix to this issue. In 2014, there was a proof-of-stake (POS) currency that was hacked, where thieves managed to acquire eight million VeriCoins from an exchange.³⁹⁷ After the attack, the developers of VeriCoin released a new code that worked to roll back the damage. It forked the blockchain prior to the hack. The developers then ensured that exchanges co-operated with this change and made sure it was adopted so that the owners of the currency would not be affected permanently.³⁹⁸

Tapscott continues to discuss the possibility of a 51 percent attack,³⁹⁹ which, as defined by Investopedia, constitutes

an attack on a blockchain – usually bitcoins, for which such an attack is still hypothetical – by a group of miners controlling more than 50% of the network's mining hash rate, or computing power. The attackers would be able to prevent new transactions from gaining confirmations, allowing them to halt payments between some or all users. They would also be able to reverse transactions that were completed while they were in control of the network, meaning they could double-spend coins. They would almost certainly not be able to create new coins or alter old blocks, so a 51% attack would probably not destroy bitcoin or another blockchain based currency outright, even if it proved highly damaging.⁴⁰⁰

³⁹⁷ Stan Higgins, '8 Million VeriCoin Hack Prompts Hard Fork to Recover Funds' (<https://www.coindesk.com/bitcoin-protected-veriCoin-stolen-mintpal-wallet-breach/>, 14 July 2014) <<https://www.coindesk.com/>> accessed 30 July 2017

³⁹⁸ *ibid*

³⁹⁹ Tapscott (n154) 267

⁴⁰⁰ Investopedia, '51% Attack' (<http://www.investopediacom/terms/1/51-attackasp>) <<http://www.investopedia.com/>> accessed 30 July 2017

This is relevant to the idea of empires or nations attempting to destabilise the process – an idea that could stem from the fact that the blockchain has become powerful enough to chip away at the power of a nation or conglomerate with enough assets to see this through.⁴⁰¹

5.2.4 Inadequate Incentives for Mass Collaboration

‘Miners do have an incentive to maintain the Bitcoin infrastructure because, if the network fails, all the unconverted Bitcoin they’d earned (or could earn through mining would be lost or worthless or otherwise at risk.’⁴⁰² Miners are responsible for the distribution of power – the power to determine which transactions are represented by which block, and the power to mint new currency and vote on that which is true.

The issue is that since the number of mined bitcoins halves every four years, when the reward (miners’ incentive) drops drastically, what incentive will they have to keep doing what they are doing? As with many things in economics, this boils down to demand and supply – mining depends on the price of Bitcoin. Once the price drops, many Bitcoin miners will hoard or ‘park’ their supply in order to wait until the price increases. Miners who do not have this luxury, will generally start to mine a new currency that is faring better, or will join group mining pools in order to increase their odds, and get a fraction of the currency rather than no currency at all. The aforementioned is mostly applicable to individual miners and not industrial mining complexes.

5.2.5 Blockchain and Employment

One of the major criticisms facing the influx of blockchain technology as a widely used tool is that of the disruption of labour markets. Generally speaking, upon the introduction of a revolutionary technological innovation, there is the displacement of jobs. The Internet, for example, affected the jobs of travel agents and music retailers. On the other hand, the Internet also paved the way for small online businesses to thrive. Companies such as Airbnb and Uber, that give individuals the opportunity to earn extra money through commodities they already own will gain popularity and thrive.⁴⁰³

⁴⁰¹ Tapscott (n154) 267

⁴⁰² *ibid*

⁴⁰³ Tapscott (n154) 270

Blockchain technology is undoubtedly a revolutionary technology that will, of course, impact the financial services field. On the one hand, this industry could benefit from blockchain technology, through reductions in costs and an increase in transparency. That being said, the pros do not necessarily outweigh the cons, as with every revolution, there are things that will have to change. If this technology is adopted, certain aspects of the financial services industry, such as payment processors, security firms and high street banks – businesses that profit from inherent inefficiencies that exist in the current landscape – will see a loss in income, ergo a loss of jobs. While this is a near certainty, a loss of jobs in one sector generally means an increase or evolution of jobs in another sector – just like the Internet changed things for travel agents, it went on to generate jobs for Uber drivers or Airbnb hosts.⁴⁰⁴

Where security is mostly limited to actual tangible security personnel or cyber security and the protection of data, the latter will likely develop to cater to the blockchain, creating more jobs in this field. This is just one example, and it may be applied to more areas of employment.⁴⁰⁵ It can also be extended to the idea of monitoring that which is becoming automated – instead of people having to do the job, they must now oversee the job being carried out by the automation.⁴⁰⁶

If machines are creating so much wealth, then maybe it's time for a new social contract that redefines human work and how much time we should all spend making a living.⁴⁰⁷

5.2.6 Governing the Protocols

After electronic computers were developed in the 1950s, eventually it became clear, upon their mainstream use, that there was a vacuum for oversight and governance, and hence

⁴⁰⁴ *ibid*

⁴⁰⁵ Monica Eaton-Cardone, 'How blockchain will affect financial services employment' (<http://newsefinancialcareers.com/us-en/269710/how-blockchain-will-affect-financial-services-employment>, 4 January 2017) <<http://news.efinancialcareers.com/>> accessed 30 July 2017

⁴⁰⁶ Gautham, 'Will Blockchain Technology and Smart Contracts Steal Jobs from People?' (<http://www.newsbtccom/2016/07/31/smart-contracts-automation-employment/>, 31 July 2016) <<http://www.newsbtc.com/>> accessed 30 July 2017

⁴⁰⁷ Tapscott (n154) 271

Internet governance came into play. Internet governance has been defined as ‘the evolving policies and mechanisms under which the Internet community’s many stakeholders make decisions about the development and use of the Internet.’⁴⁰⁸

The relevance of Internet governance to the topic at hand, is that, the same way the Internet required governing bodies, so does the Bitcoin community. This is quite problematic, since this lack of governance is the preferred way for the Bitcoin community. The way the public blockchain is set up, creates an environment whereby individuals who do not know each other may agree to a set of rules, and work towards the benefit of the group. These rules are different in each public blockchain, but the underlying driving force is that of bringing people together without a centralised organisation necessary in order for them to reach consensus.⁴⁰⁹

Therefore, there exists a dilemma - those people who would like to keep the blockchain open, decentralised, and secure cannot seem to agree upon a way forward. Unless governance is tackled, the movement might self-implode.

5.2.7 The Skynet: a Farfetched Concept Rooted in Reality

The Skynet is a fictional AI warfare system that was introduced in the ‘Terminator’ franchise. In common parlance, it has come to connote a dystopian future where technology has begun to supersede human kind. While the Skynet remains firmly rooted in fiction⁴¹⁰, a minor extrapolation of the concept is not entirely farfetched.

Andy Greenberg, a writer for Wired magazine covering security, privacy, information freedom, and hacker culture, who can easily be considered to be one of the most prominent journalists in this field, recently participated in an experiment.⁴¹¹ Security researchers Charlie Miller and Chris Valasek successfully attempted to hijack a moving vehicle with Greenberg

⁴⁰⁸ NRO The Number Resource Organisation, 'Internet Governance' (<https://www.nronet/nro-and-Internet-governance>) <<https://www.nro.net/>> accessed 30 July 2017

⁴⁰⁹ Nick Tomaino, 'The Governance of Blockchains: A glimpse into governance structures the world has never seen before' (<https://thecontrolco/the-governance-of-blockchains-5ba17a4f5da6>, 28 February 2017) <<https://thecontrol.co/>> accessed 30 July 2017

⁴¹⁰ This concept was actually ‘uncovered’ in certain leaks by whistle-blower Edward Snowden, and here it’s ‘farfetched’ quality is meant in reference to the likeness to the film franchise and not the alleged connection with the NSA.

⁴¹¹ Andy Greenberg, 'Hackers Remotely Kill a Jeep on the Highway - with me in it' (<https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>, 2015) <<https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>> accessed 30 July 2017

in the driver's seat.⁴¹² The ease with which this was accomplished resulted in a recall of 1.4 million vehicles by Chrysler.⁴¹³

Tapscott's example of this technological takeover is that of the organisation Anonymous, which is an active hacktivist group with a distributed network of volunteers that engage in corporate sabotage, or whistleblowing, amongst others. Through the blockchain, Bitcoin could be compiled and held, and then used for nefarious means (for example retributive justice, such as the hiring of individuals specifically tasked to kill terrorists).⁴¹⁴ Consensus is required in order to release the funds for this activity. Once you have given consent, what legal liability pertains to you? What percentage responsibility do you have for the hypothetical deaths of these terrorists? These questions currently have no answers. That is why the regulation of blockchain and cryptocurrencies is of the utmost urgency and importance. It is better to be proactive than reactive to a disaster. As the old adage goes, prevention is better than cure.

5.2.8 Anonymity and Control

According to Tapscott:⁴¹⁵

While blockchains ensure a degree of anonymity, they also provide a degree of openness. If past behaviour is any indication of future intent, then we should expect corporations known for spying and countries known for waging cyberwarfare to redouble their efforts because value is involved – money, patents, access to mineral rights, the titles to land and national treasures.⁴¹⁶

An important point of note, is the misconception that Bitcoin is anonymous. It is not anonymous but it is actually pseudonymous - it offers privacy without anonymity. The ledger of transactions shows the details of those transactions through the publication of the

⁴¹² *ibid*

⁴¹³ Andy Greenberg, 'After Jeep Hack, Chrysler Recalls 14M Vehicles for Bug Fix' (<https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/>, 2015) <<https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/>> accessed 30 July 2017

⁴¹⁴ Tapscott (n154) 273

⁴¹⁵ Tapscott (n154) 274

⁴¹⁶ *ibid*

addresses. The level of privacy offered is through the fact that one does not know who owns those addresses. According to Jonathan Cross, a web developer:⁴¹⁷

Bitcoin's privacy can be compromised using tools that trace payments through the Blockchain identifying clusters of addresses owned by a single user, they can check geographical location where the transaction was first announced and identify 'end points' where Bitcoin is traded for fiat currency (for example on an exchange).⁴¹⁸

With technology as ground-breaking as blockchain, it will not come as a surprise that governments and companies will attempt to control the network. Privacy is a pivotal aspect of the current technology – one that makes it so popular amongst its users – and this means that privacy in this regard is no longer automatically guaranteed.

5.2.9 The Illicit Aspect

'People can harness brilliant technologies, from electricity to the radio and through to the Internet, for benevolent or malevolent goals.'⁴¹⁹ In Chapter One, the link between Bitcoin and The Silk Road was discussed. There is no unique facet of blockchain technology that makes it more effective to criminal activity than other technologies.

Bitcoin and blockchain have been used by criminals in the past, but the technology is not to blame for the criminal activity executed through its existence. It is the criminals themselves that should be faulted. With this perspective in mind, it is important to note, that the technology in itself could actually deter criminals from using it, due to certain aspects that would make it easier for them to eventually be caught out. A criminal, although presumably attempting to hide the money trail, still cannot circumvent the requirement to publish Bitcoin transactions on the blockchain, like every other user. Bitcoins are much easier to track and reconcile than their reputation allows individuals to believe.

⁴¹⁷ 'Jonathan Cross' (<https://www.quora.com/profile/Jonathan-Cross-10>) <<https://www.quora.com/profile/Jonathan-Cross-10>> accessed 30 July 2017

⁴¹⁸ *ibid*

⁴¹⁹ Tapscott (n154) 195-196

5.3 The Legal Challenges to Implementation

There is a myriad of legal challenges to the widespread implementation of blockchain technology, stemming from the push to substitute or complement the use of fiat currencies with cryptocurrencies. One of the primary issues surrounding the challenging aspect of implementation, is the fact that there is no central point of control or governance - the system is decentralised. The database uses cryptography in order to ensure security, and the fact that it is a publicly viewable ledger with a copy kept with each separate network user emphasises the transparent aspect of the technology. This lack of control or governance is seen to be a challenge to implementation.

Primarily, regulators and policy makers directed their focus towards cryptocurrency regulation in financial transactions, but the expansion of the technology behind the Bitcoin - that of distributed ledger technology, is likely to cause a ripple effect throughout many branches of law on both a national and an international level.⁴²⁰

One drawback to Bitcoin and other cryptocurrencies is the idea that they could potentially undermine the state. As of the twentieth century, governments became powerful and centralised organs that control fiat currency.

Whilst electronic payments have been increasing in popularity over the past few years, Bitcoin is without precedent as an independent currency with a decentralised network. If cryptocurrencies become widely adopted, they could potentially have a negative impact on governments in three central functions: taxation, police and macroeconomic stabilisation.⁴²¹

Levying taxes requires the state authorities to be able to identify the parties to a transaction or to their earnings, however the decentralised blockchain system, as well as the pseudonymity aspects of the technology create very difficult barriers to overcome. In the same way, the police force's ability to detect and investigate certain offences would be undermined.⁴²²

⁴²⁰ Judith Alison Lee, Jeff Steiner and Dustin McKenzie, 'Legal implications of expanded use of blockchain technology' (<https://www.financierworldwide.com/legal-implications-of-expanded-use-of-blockchain-technology/#WUGOrROGNE4>, November 2016) <<https://www.financierworldwide.com/legal-implications-of-expanded-use-of-blockchain-technology/#.WUGOrROGNE4>> accessed 30 July 2017

⁴²¹ Charles Cassar (n98)

⁴²² *ibid*

Central banks generally oversee the fiat currencies pertaining to the country that they economically regulate. In an economy complemented by cryptocurrencies, it would be far more difficult to implement monetary policy than in a single currency economy. Another salient point is the fact that in the case of an economic depression in a Bitcoin economy, states would be unable to pursue remedial action in the new virtual currency market, potentially resulting in unrecoverable losses.

According to Dr Charles Cassar,⁴²³ a practitioner in Maltese financial services and corporate law, one such way in which governments might be able to remedy the aforementioned threats would be to regulate transactions involving all cryptocurrencies, and would require records of purchases and sales that are made. The issue with this, just like the issue with the recently proposed law in the US⁴²⁴, is that it is very difficult to detect and enforce laws regulating cryptocurrencies. Cassar states that a more feasible approach might be the regulation of exchanges – bringing them up to par with banks, vis-a-vis their customers, so that they are bound to conduct due diligence and follow KYC procedures.⁴²⁵

5.3.1 Financial Transfers

Currently, cryptocurrencies are already being used as mediums of exchange. The technological backbone of Bitcoin, the blockchain, can also be applied to the global transfer of funds. R3CEV LLC, a distributed database technology company, heads up a consortium of many of the world's largest financial institutions⁴²⁶ in order to further the research on the topic and explore the application of the technology and its use in the financial sector. One major issue with this, is that this technology might not fit squarely within the parameters of the current laws and regulations governing the financial sector, and amendments to these laws, or added legislation, might be necessary to facilitate these types of transfers.⁴²⁷

⁴²³ *ibid*

⁴²⁴ 'Updated Law Will Oblige Travelers Entering US to Declare Digital Currency Holdings' (<http://www.altcointoday.com/law-will-oblige-travelers-entering-us-to-declare-digital-currency-holdings/>, 10 June 2017) <<http://www.altcointoday.com/law-will-oblige-travelers-entering-us-to-declare-digital-currency-holdings/>> accessed 30 July 2017

⁴²⁵ Charles Cassar (n98)

⁴²⁶ Jemima Kelly, 'Exclusive: Blockchain platform developed by banks to be open-source' (*"Exclusive: Blockchain platform developed by banks to be open-source"* Reuters UK, 20 October 2016) <"Exclusive: Blockchain platform developed by banks to be open-source". Reuters UK> accessed 30 July 2017

⁴²⁷ Charles Cassar (n98)

5.3.2 Multi-Signature Transactions

Blockchain technology can be used through multi-signature transactions in a situation when a financial instrument or an asset is held by a third party on behalf of two other parties that are in the process of completing a transaction. The funds or assets are held until predetermined contractual obligations have been fulfilled.⁴²⁸

In Malta, this might include a number of different services, such as being a security trustee, being a trustee in a commercial transaction or holding of documents or shares on a fiduciary basis. The contracting parties would deposit funds to a virtual currency address whilst a third party to the transaction acts as a ‘middle man.’ In order for the transaction to be finalised, there must be the signature of two thirds of the parties to the deal. The laws regulating trusts and trustees in Malta, primarily the Trusts and Trustees Act,⁴²⁹ uses language such as ‘delivers’ or ‘held’ which do not accommodate these less tangible transactions.⁴³⁰

5.3.3 Merchant Issued Digital Currencies and ‘Coloured Coins’

Coloured coins are a complex concept, but summarised, they can be described as being tagged transactions in cryptocurrency, so that the tagged ‘coin’ would represent a certain asset (such as a voucher for example), whilst also retaining its original market value as a coin in whatever denomination of Bitcoin that was used in the transaction.⁴³¹

These advances in technology, through this new application of cryptocurrencies, add further confusion to the regulatory system currently in place in foreign countries. This implies that, should Malta attempt to regulate cryptocurrencies and the blockchain, legislators ought to take this into consideration.

One such example of this notion in action is the ‘BitLicense’ that was described in Chapter One.

⁴²⁸

Investopedia, 'Escrow' ([Http://www.investopediacom/terms/e/escrow.asp#ixzz4mnxD32v4](http://www.investopediacom/terms/e/escrow.asp#ixzz4mnxD32v4)) <<http://www.investopedia.com/terms/e/escrow.asp#ixzz4mnxD32v4> >accessed 30 July 2017

⁴²⁹ Trusts and Trustees Act, Chapter 331 of the Laws of Malta

⁴³⁰ Charles Cassar (n98)

⁴³¹ *ibid*

5.3.4 Intellectual Property and Property Registers

Through the application of blockchain technology, registers that are currently analogue could evolve. One such example could be through land registry, so that titles could be verified without the requirement of a centralised third-party system. Something similar could also be done with intellectual property registers. In Malta, intellectual property rights are granted through the Industrial Property Registrations Directorate (The IP Office), allowing them to be supplemented or entirely based upon a decentralised ledger. As with other applications of blockchain technology, the author believes that this method would lead to less opportunities for fraudulent intervention, as well as increased security and minimal transfer costs.

Piracy is another aspect of intellectual property that might be positively influenced by this technology. Dr Cornelius Grossmann, a managing partner for Ernst & Young and the Global Head of Law for the firm, gives the following salient example of how this could be applied: ‘if the use of a music file anywhere in the world is automatically recorded by a public blockchain, and the transaction can be validated, digital rights theft will become almost impossible.’⁴³²

5.3.5 Storage and Data Transfer

Any data can be stored on the blockchain, such as information pertaining to personal identities, digital signatures etc. The details of personal identities could be stored on a ledger, with the result of such being that the identities remain pseudonymous. There are multiple applications for these stored identities. One such use could be the reduction of fraud on peer-rating sites or the possibility of using them to provide trust ratings for lending services or peer-to-peer marketplaces.⁴³³

These applications come with certain concerns about the privacy of the individuals being identified through these means. Storing a large-scale composite of data on a ledger, which, while generally thought to be very safe, would be incredibly sensitive and damaging to the individuals at risk in the case of a breach of security.

⁴³² Grossman (n285)

⁴³³ *ibid*

Although cryptographic ledgers are widely seen as secure, if personally identifiable data from elsewhere were exposed and correlated to blockchain data, or if blockchain data were aggregated and analysed, transactions could be tracked and compared even with a pseudonymous ledger.⁴³⁴

5.3.6 Decentralised Organisations

The corporate sphere might also benefit from blockchain technology. The technology could be applied to distribute certain rights, such as voting rights for example. The use of smart contracts could be used to further the application of this technology, such as in the case of dividend distribution, which could be done automatically upon acquiescence of the members. There are certain issues that come along with this sort of application though, such as the liability of organisations in the case of a situation where the laws are broken, as it would be hard to define who is ultimately responsible for the breach. Grossmann, in his article on the legal impact that blockchain might have, also raises a point concerning the legal status of decentralised organisations.⁴³⁵

5.3.7 Securities and Financial Products

Originally, stocks were represented through the issue of physical certificates. These were exchanged or revised whenever there was a stock trade. Eventually, the system evolved where intermediaries took the position of physical traders of the certificates, negating the necessity of actually trading these certificates, and creating the concept of beneficial owners and stock holders – with the traders being the holders and the beneficial owners being those individuals that held the stock without physically holding the certificate. There are, of course, negative repercussions of this, adding to the confusion and entanglement of ultimate beneficial owners and the laws relating to such. These discrepancies could easily be solved through an increase in the transparency that goes hand-in-hand with the distributed ledger technology that is the blockchain.⁴³⁶

⁴³⁴ *ibid*

⁴³⁵ *ibid*

⁴³⁶ *ibid*

An American company, Overstock.com, has been granted approval by the Securities and Exchange Commission (SEC) to trade securities on a digital platform where the publicly distributed ledger would be maintained by a subsidiary of the company.⁴³⁷ This substitutes the notion of a broker as illustrated above, and allows the issuers of a security to have a real-time 'list' of the owner of the securities.⁴³⁸

5.3.8 Competition Law

As previously mentioned, the R3CEV project is a consortium of financial institutions that came together to see how to move forward with blockchain. This consortium could also become a cartel if the collaboration becomes unlawful, resulting in anti-competitive actions.⁴³⁹

Alistair Maughan, a partner at a London law firm specialising in technology law, also points out that, 'there could be a risk that algorithms are set up in a manner which produces anti-competitive results that are secret or not readily detectible.'⁴⁴⁰

5.3.9 Accountability, Responsibility and Liability

The question regarding who ought to have 'ultimate control' over the ledger is an ironic one at best – the distributed nature of the system is what makes the system special, it is the crux of the technology, shadowing Bitcoin and cryptocurrencies insofar as the frontrunner to the technological advancements originally made by Nakamoto in 2008. This is echoed in Chapter

⁴³⁷ 'Overstockcom to utilize strategic shareholder consulting services firm Georgeson in public offering of blockchain securities' ([Http://investoroverstockcom/mobileview?c=131091&v=203&d=1&id=2155031](http://investoroverstockcom/mobileview?c=131091&v=203&d=1&id=2155031) , 7 April 2016) <<http://investors.overstock.com/mobile.view?c=131091&v=203&d=1&id=2155031> > accessed 30 July 2017

⁴³⁸ Pepper Hamilton, 'Blockchain and Public Securities: Shedding Light on 'Going Dark' ([Http://www.lexology.com/library/detail.aspx?g=c33df1b5-f5bc-4041-9bf0-105ad7ea3f4b](http://www.lexology.com/library/detail.aspx?g=c33df1b5-f5bc-4041-9bf0-105ad7ea3f4b), 27 September 2016) <<http://www.lexology.com/library/detail.aspx?g=c33df1b5-f5bc-4041-9bf0-105ad7ea3f4b>> accessed 30 July 2017

⁴³⁹ Michael Milnes, 'Blockchain: Issues in Competition & Consumer Law' ([Https://www.linkedin.com/pulse/blockchain-issues-competition-consumer-law-michael-milnes](https://www.linkedin.com/pulse/blockchain-issues-competition-consumer-law-michael-milnes), 26 May 2016) <<https://www.linkedin.com/pulse/blockchain-issues-competition-consumer-law-michael-milnes>> accessed 30 July 2017

⁴⁴⁰ Alistair Maughan, 'Blockchain - Legal and regulatory issues around distributed ledger technology' ([Http://www.ciocouk/opinion/legal-briefing/blockchain-legal-regulatory-issues-around-blockchain-3638814/](http://www.ciocouk/opinion/legal-briefing/blockchain-legal-regulatory-issues-around-blockchain-3638814/) , 20 April 2016) <<http://www.cio.co.uk/opinion/legal-briefing/blockchain-legal-regulatory-issues-around-blockchain-3638814/> > accessed 30 July 2017

Four where the control of the ledger from a technological point of view is discussed – the same applies to the legality and accountability of the ledger, since it is necessarily distributed, it makes it nearly impossible to regulate the ledger or the users of the ledger, creating a ripple-effect of legal issues that would need to be tackled.⁴⁴¹

5.3.10 Regulatory Change

The introduction of blockchain technology could have extensive impact on financial services, driving significant regulatory change across multiple sectors. The technology would enable the movement of assets securely and privately without the need for an intermediary such as a bank or government. This would radically change the existing protocols in the industry.⁴⁴²

Additionally, blockchain technology may be used to validate revenue and calculate tax due, allowing for a more transparent governance of corporations. In today's world, where transactions are recorded in real time, it is likely that illicit and illegal businesses will struggle to operate. We are only just beginning to explore the possibilities of this technology. It would seem logical for governments and legislators to clearly identify the risks and challenges of blockchain technology, staying one step ahead of the blockchain roadmap when formulating legislation that is forward thinking and technologically neutral.

5.3.11 Smart Contracts

Smart contracts have been discussed in Chapter Three where the challenges and opportunities of blockchain technology in this context were explored at length.

⁴⁴¹ *ibid*

⁴⁴² Grossman (n285)

CONCLUSION

Blockchain technology is the future. We are only just beginning to explore its possibilities. The future will not wait for us to catch up and it is imperative that we consider the possibility of blockchain based software in the formulation of our legislation. Within this thesis, the author has attempted to clearly identify the risks and challenges of blockchain technology. This is imperative to ensure that our legislators remain one step ahead of the technological advances when formulating legislation that is proactive, forward thinking, and technologically neutral. Without this in-depth analysis of the infinite applications of the blockchain, and its inherent challenges, we risk legislating from a reactive position of fear rather than from a position of authority.

The White Paper recently published by the MGA,⁴⁴³ seems to indicate that the implementation of cryptocurrencies is in the pipeline and this provides the perfect opportunity for us to ensure that Malta becomes a hub for blockchain. The formulation of our legislation in this regard requires divergent thinking, perception and a clear minded vision of Malta's future.

“The Authority is cognizant that the rise of cryptocurrencies is inevitable. Conscious of the need to remain at the forefront of innovation and to keep up with new developments in technology and the industry, as well as being fully aware that the system at the back of such transactions provides the industry with fast and cost-effective alternatives to traditional payment mechanisms, the Authority is committed to allow the use of crypto-currencies by its licensees in the immediate future. The Malta Gaming Authority is mindful that there are also risks which have to be addressed in order to ensure that such developments do not prejudice the protection of players, the importance of the prevention of crime and the reputation of the Maltese jurisdiction. To this effect, the Malta Gaming Authority has commissioned a study to assist in the development of a commensurate framework, inclusive of all necessary safeguards, with due regard to the 4th Anti-Money Laundering Directive which is also currently being revised to include further provisions specific to crypto-currencies. Within this ambit, the Authority shall engage in a public consultation exercise, detailing the main findings of the study on a proposed framework for implementation, the fourth quarter of 2017.”⁴⁴⁴

⁴⁴³ MGA (n5)

⁴⁴⁴ *ibid*

The gaming industry has provided a valuable contribution to our nation's GDP⁴⁴⁵ and we need to ensure that our laws are formulated to provide adequate safeguards to further enhance this industry, making Malta more attractive to international companies implementing the use of cryptocurrencies and blockchain based software. We need to spearhead the implementation of legislation into this new technology so that Malta remains at the forefront of the gaming, capital market and financial industries.

The Chairman of the MGA, Mr. Joseph Cuschieri, is conscious of the fact that Malta cannot afford to lose its competitive edge and must continue to enhance its reputation as a forward-looking jurisdiction which is friendly to compliant businesses.⁴⁴⁶

This thesis seeks to examine the pros and cons of the implementation of blockchain technology and cryptocurrencies into our current legislative framework. The time is opportune for us to take a strong position at the forefront of these technological advances. Much more research and discussion is warranted, and it is the author's aim to elicit interest and create awareness regarding this opportune time for us to take the next step forward.

As stated in Chapter 1.6, one way states are attempting to progress with regard these technologies is through the introduction of regulatory sandboxes, which “implement a set of rules that allow trailblazers to test their products and business models in a live environment with minimal legal requirements.”⁴⁴⁷ Many countries like the UK, Russia, Canada, Switzerland and Australia are already making use of this system.⁴⁴⁸ The author believes that this concept would be a welcome introduction to Malta, as it allows for experimentation with minimal risk.

Maltese legislation needs to be at the nexus of this technology, taking a page out of Satoshi Nakamoto's book and creating a framework that stays ahead of the technology. Technology is malleable and it is up to us to mould it into the right shape that ensures a positive future for law and industry in Malta.

⁴⁴⁵ GDP (n289)

⁴⁴⁶ Capital Market Resources (n350)

⁴⁴⁷ Dan Cummings, 'Regulatory Sandboxes: A Practice For Innovation That Is Trending Worldwide' (<https://www.ethnews.com/regulatory-sandboxes-a-practice-for-innovation-that-is-trending-worldwide> , 1 March 2017) <<https://www.ethnews.com/>> accessed 30 July 2017

⁴⁴⁸ *ibid*

BIBLIOGRAPHY

THESES

Galea, Jonathan, 'The Effect of Bitcoin on Money Laundering Law', LL.D Thesis, University of Malta 2015

Mula, Mariah, 'The Fourth EU Anti-Money Laundering Directive, LL.B. Honours Thesis, University of Malta 2016

Sare Kathleen, 'The Use of Cryptocurrencies in Gaming: The Legal and Regulatory Considerations', LL.D Thesis, University of Malta 2016

BOOKS

Babatunde Fagoyinbo J , *The Armed Forces: Instrument of Peace, Strength, Development and Prosperity* (May 2013)

Goodhart C A E, Two Concepts of Money by Charles A.E.' <<https://www.scribd.com/doc/67161350/Two-Concepts-of-Money-by-Charles-A-E-Goodhart>> accessed 31 July 2017

Tapscott D and Tapscott, *Blockchain Revolution How the Technology Behind Bitcoin is Changing Money, Business and The World* (Penguin Random House 2016)

Orwell G, 1984 (Secker & Warburg 8 June 1949)

Oxford Dictionary of Law (7th edn, Oxford University Press 2009)

WORKING PAPERS

Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' [October 31, 2008] Metzger, Dowdeswell & Co Website

Pierre Rochard, 'The Bitcoin Central Bank's Perfect Monetary Policy ' ([Http://nakamotoinstitute.org/mempool/the-bitcoin-central-banks-perfect-monetary-](http://nakamotoinstitute.org/mempool/the-bitcoin-central-banks-perfect-monetary-)

policy/#selection-117-1723, 15 December 2013) <<http://nakamotoinstitute.org/>> accessed 30 July 2017

Nick Szabo, 'The God Protocols ' ([Http://nakamotoinstitute.org/the-god-protocols/](http://nakamotoinstitute.org/the-god-protocols/), 1997) <<http://nakamotoinstitute.org/>> accessed 30 July 2017

Hughes E., *A Cypherpunk's Manifesto* (1993)

Luther W. J. and White L. H., 'Can Bitcoin Become a Major Currency?' [2014] GMU Working Paper in Economics No. 14-17. Available at SSRN: <https://ssrn.com/abstract=2446604> or <http://dx.doi.org/10.2139/ssrn.2446604>

Mga.org.mt, 'The Malta Gaming Authority Publishes a White Paper Proposing Major Reforms to Malta's Gaming Legal Framework' (*Malta Gaming Authority*, 12 July 2017)<<http://www.mga.org.mt/malta-gaming-authority-publishes-white-paper-proposing-major-reforms-maltas-gaming-legal-framework/>> accessed 31 July 2017

Malta Gaming Authority, *A White Paper to Future Proof Malta's Gaming Legal Framework* (1st edn, 2017)

Marian O. Y., 'A Conceptual Framework for the Regulation of Cryptocurrencies' [2014] 82 University of Chicago Law Review Dialogue 53. Available at SSRN: <https://ssrn.com/abstract=2509857>

Ospan A, Skrzypski K and Hatch C, 'Quanta Lottery White Paper Draft v0.4.5' <<http://www.quanta.im/wp-content/themes/quanta/assets/img/Quantalotterywhitepaperdraftv0.4.5.pdf>> accessed 31 July 2017

OTHER

Tapscott, D. [TED] (2016, June). "How the blockchain is changing money and business" Retrieved from: <https://www.ted.com/talks/don_tapscott_how_the_blockchain_is_changing_money_and_business#t-9390> accessed 2nd February 2017

‘Mark Pascall Presents an Introduction Smart Contracts, Ethereum and the Blockchain - YouTube’ <<https://www.youtube.com/watch?v=lBiBoRlagK0>> accessed 31 July 2017

‘Ethereum and Smart Contracts - YouTube’ <https://www.youtube.com/watch?v=Lp7Qzys_yB8> accessed 31 July 2017

‘Bettina Warburg: How the Blockchain Will Radically Transform the Economy | TED Talk | TED.com’

<https://www.ted.com/talks/bettina_warburg_how_the_blockchain_will_radically_transform_the_economy/transcript?language=en> accessed 31 July 2017

‘Blockchain Demystified | Daniel Gasteiger | TEDxLausanne - YouTube’ <<https://www.youtube.com/watch?v=40ikEV6xGg4>> accessed 31 July 2017

‘Marc Goodman: A Vision of Crimes in the Future | TED Talk Subtitles and Transcript | TED.com’

<https://www.ted.com/talks/marc_goodman_a_vision_of_crimes_in_the_future/transcript?language=en#t-87462> accessed 31 July 2017

EU PUBLICATIONS

‘Revision of the Fourth Anti-Money-Laundering Directive - Think Tank’ <http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI%282017%29607260> accessed 31 July 2017

‘European Commission - PRESS RELEASES - Press Release - Questions and Answers: Anti-Money Laundering Directive’ <http://europa.eu/rapid/press-release_MEMO-16-2381_en.htm> accessed 31 July 2017

‘Financial Crime - European Commission’ <http://ec.europa.eu/justice/civil/financial-crime/index_en.htm> accessed 31 July 2017

ONLINE JOURNALS

‘The University of Chicago Law Review |’ <<https://lawreview.uchicago.edu/page/conceptual-framework-regulation-cryptocurrencies>> accessed 31 July 2017

‘The Law and Legality of Smart Contracts – The Georgetown Law Technology Review’ <<https://www.georgetownlawtechreview.org/the-law-and-legality-of-smart-contracts/GLTR-04-2017/>> accessed 31 July 2017

ONLINE ARTICLES, WEBSITES AND BLOGS

Gatt Gege, ‘Nebulous Law Presents an Affront to Basic Online Rights – Gege Gatt’ <<http://www.gegegatt.com/internet-freedoms-malta/>> accessed 31 July 2017

Hellström V., 'PSD2 - the directive that will change banking as we know it' (*Evrycom*) <<https://www.evry.com/en/news/articles/psd2-the-directive-that-will-change-banking-as-we-know-it/>> accessed 31 July 2017

Altcointoday.com, 'Updated Law Will Oblige Travelers Entering US to Declare Digital Currency Holdings' (*Altcoin Today*, 10 June 2017) <<http://www.altcointoday.com/law-will-oblige-travelers-entering-us-to-declare-digital-currency-holdings/>> accessed 31 July 2017

Iwamura M. and Kitamura Y. and Matsumoto T., ‘Is Bitcoin the Only Cryptocurrency in the Town? Economics of Cryptocurrency And Friedrich A. Hayek’ [2014]. Available at SSRN: <https://ssrn.com/abstract=2405790> or <http://dx.doi.org/10.2139/ssrn.2405790> accessed 31 July 2017

De Filippi P., ‘Bitcoin: A Regulatory Nightmare to a Libertarian Dream’ [2014] 3(2) Internet Policy Review. Available at SSRN: <https://ssrn.com/abstract=2468695> accessed 31 July 2017

Chaparro F., 'Ethereum's share of the cryptocurrency market has exploded' (*Business Insider*, 13 July 2017) <<http://www.businessinsider.com/ethereum-price-sends-marketcap-sky-high-vs-bitcoin-price-marketcap-2017-7>> accessed 31 July 2017

Buterin V., 'Bitcoin Network Shaken by Blockchain Fork' (*Bitcoin Magazine*, 12 March 2013) <<https://bitcoinmagazine.com/articles/bitcoin-network-shaken-by-blockchain-fork-1363144448/>> accessed 31 July 2017

Kinsella S., 'Bitcoin: Experts clash over the crypto-currency' (*Stephen Kinsella*, 28 November 2013) <<http://www.stephenkinsella.net/2013/11/28/bitcoin-experts-clash-over-the-crypto-currency/>> accessed 31 July 2017

Coindesk.com, (*Coindesk*) <<https://www.coindesk.com/price/>> accessed 31 July 2017

Suberg W., 'Bitcoin ETF Reconsidered by SEC, Ethereum ETF Version May Be Approved' (*The Cointelegraph*, 26 April 2017) <<https://cointelegraph.com/news/bitcoin-etf-reconsidered-by-sec-ethereum-etf-version-may-be-approved>> accessed 31 July 2017

Higgins S., 'The SEC is Now Weighing an Ethereum ETF Proposal' (*Coindesk*, 25 April 2017) <<https://www.coindesk.com/sec-now-weighing-ethereum-etf-proposal/>> accessed 31 July 2017

Plassaras N., 'Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF' [2013] Chicago Journal of International Law. Available at SSRN: <https://ssrn.com/abstract=2248419> accessed 31 July 2017

Kaplanov N. M., 'Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation' [2012] Temple University Legal Studies Research Paper. Available at SSRN: <https://ssrn.com/abstract=2115203> or <http://dx.doi.org/10.2139/ssrn.2115203> accessed 31 July 2017

Vlastelica R., 'Bitcoin needs government regulation to rise further, Morgan Stanley says' (*Market Watch*, 15 June 2017) <<http://www.marketwatch.com/story/bitcoin-needs-government-regulation-to-rise-further-morgan-stanley-says-2017-06-13>> accessed 31 July 2017

Whpartners.eu, 'Malta's new gaming law: Consultation document and draft law published' (*WH Partners - Leading Law Firm Malta*, 12 July 2017) <<http://whpartners.eu/news/maltas-new-gaming-law-consultation-document-draft-law-published/>> accessed 31 July 2017

Encyclopædia Britannica, 'Fiat money' (*Encyclopædia Britannica*) <<https://www.britannica.com/topic/fiat-money>> accessed 31 July 2017

Bitcoin' (*IGaming Business*, 30 January 2014) <<http://www.igamingbusiness.com/news/verajohn-becomes-first-regulated-online-casino-accept-bitcoin>> accessed 31 July 2017

Cssf.lu, 'Communique: Virtual Currencies' (*Commission de Surveillance du Secteur Financier*, 14 February 2014)

<http://www.cssf.lu/fileadmin/files/Publications/Communiqués/Communiqués_2014/Communique__virtual_currencies_140214.pdf> accessed 31 July 2017

Nakamotoinstitute.org, 'Literature' (*Satoshi Nakamoto Institute*, x) <<http://nakamotoinstitute.org/literature/>> accessed 31 July 2017

Hughes S. J, and Middlebrook S. T., 'Regulating Cryptocurrencies in the United States: Current Issues and Future Directions' [2014] 40(813) William Mitchell Law Review

Rosenblum P., 'Bitcoin: The Currency Of The Future?' (*Forbes*, 27 January 2014) <<https://www.forbes.com/sites/paularosenblum/2014/01/27/bitcoin-the-currency-of-the-future/#5895d30c28b9>> accessed 31 July 2017

Bjerg O., 'How is bitcoin money?' [2016] 33(1) Theory, Culture & Society 53-72.

DUIVESTEIN S, 'Bitcoin Is The World's Most Dangerous Idea' (*The Next Web*) <https://thenextweb.com/insider/2015/04/16/bitcoin-is-the-worlds-most-dangerous-idea/#.tnw_uyy7mZWa> accessed 31 July 2017

'Blockchain Raises Fundamental Questions' <<https://www.ft.com/content/a0a4f42e-a4b1-11e5-a91e-162b86790c58>> accessed 31 July 2017

'Central Bank Embrace of Blockchain Is All About Control | Mises Institute' <<https://mises.org/library/central-bank-embrace-blockchain-all-about-control>> accessed 31 July 2017

'The 7 Foundational Principles' <www.privacybydesign.ca> accessed 31 July 2017

'Threat or Opportunity? Blythe Masters Talks Blockchain Jobs Impact - CoinDesk' <<https://www.coindesk.com/threat-opportunity-blythe-masters-addresses-blockchain-jobs-impact/>> accessed 31 July 2017

McConnell P, 'When Will Regulators Wake up to the Dangers of Blockchain? | Pulse | LinkedIn' <<https://www.linkedin.com/pulse/when-regulators-wake-up-dangers-blockchain-patrick-mcconnell>> accessed 31 July 2017

‘Will Blockchain Technology and Smart Contracts Steal Jobs from People? - NEWSBTC’
<<http://www.newsbtc.com/2016/07/31/smart-contracts-automation-employment/>> accessed 31 July 2017

Teixeira D., 'UNODC launches training to tackle cryptocurrency-enabled Organized Crime' (*UNODC*) <<https://www.unodc.org/unodc/en/frontpage/2017/May/unodc-launches-training-to-tackle-money-laundering-and-bitcoin-banking-fraud.html>> accessed 31 July 2017

Hillbom E and Tillström T, ‘Applications of Smart-Contracts and Smart-Property Utilizing Blockchains’ <http://www.the-blockchain.com/docs/Applications_of_smart-contracts_and_smart-property_utilizing_blockchains.pdf> accessed 31 July 2017

‘Press Release - Blockchain Committee - Malta Stock Exchange’
<<https://borzamalta.com.mt/article-press-release-blockchain>> accessed 31 July 2017

‘The Blockchain Will Do to the Financial System What the Internet Did to Media’
<<https://hbr.org/2017/03/the-blockchain-will-do-to-banks-and-law-firms-what-the-internet-did-to-media>> accessed 31 July 2017

‘The Ultimate Guide to Blockchain Smart Contracts’
<<http://www.blockchaintechnologies.com/blockchain-smart-contracts>> accessed 31 July 2017

‘Ross Ulbricht Reflects on Life in Prison; New Evidence of Police Tampering’
<<https://bitcoinmagazine.com/articles/ross-ulbricht-reflects-on-life-in-prison/>> accessed 31 July 2017

‘BlockCloud: Re-Inventing Cloud with Blockchains’
<<https://guardtime.com/blog/blockcloud-re-inventing-cloud-with-blockchains>> accessed 31 July 2017

‘What Are Smart Contracts? A Beginner’s Guide to Smart Contracts’
<<https://blockgeeks.com/guides/smart-contracts/>> accessed 31 July 2017

‘What Is Ethereum? A Step-by-Step Beginners Guide [Ultimate Guide]’
<<https://blockgeeks.com/guides/what-is-ethereum/>> accessed 31 July 2017

John Ream, Yang Chu DS, ‘Upgrading Blockchains: Smart Contract Use Cases in Industry | Deloitte University Press’ <<https://dupress.deloitte.com/dup-us-en/focus/signals-for-strategists/using-blockchain-for-smart-contracts.html>> accessed 31 July 2017

‘European Court of Justice Considers the Exchange of Traditional Currencies for Bitcoins Exempt from VAT’ <<https://www.stibbe.com/en/news/2016/january/european-court-of-justice-considers-the-exchange-of-traditional-currencies-for-bitcoins-exempt-from>> accessed 31 July 2017

‘Bitcoin Is Exempt from VAT, Rules European Court of Justice’ <<https://www.coindesk.com/bitcoin-is-exempt-from-vat-says-european-court-of-justice/>> accessed 31 July 2017

‘Bitcoin Is Exempt from VAT, Rules European Court of Justice’ <<https://www.coindesk.com/bitcoin-is-exempt-from-vat-says-european-court-of-justice/>> accessed 31 July 2017

‘A Legal Perspective of the European Court Ruling Exempting Bitcoin from VAT Tax - CryptoCoinsNews’ <<https://www.cryptocoinsnews.com/legal-perspective-european-court-ruling-exempting-bitcoin-vat-tax/>> accessed 31 July 2017

‘Gaming on the Blockchain – the Trillion Dollar Jackpot’ <<http://www.ibtimes.co.uk/gaming-blockchain-trillion-dollar-jackpot-part-1-1542297>> accessed 31 July 2017

‘Could Blockchain Gaming Inspire More People To Use Bitcoin?’ <<https://www.forbes.com/sites/rogeraitken/2016/12/21/could-spells-of-genesis-blockchain-gaming-incite-broader-digital-currency-use/#5193040c26c4>> accessed 31 July 2017

‘Startup Will Use Blockchain Tech to Disrupt Online Gaming’ <<https://www.coindesk.com/one-startup-will-use-blockchain-disrupt-online-gaming/>> accessed 31 July 2017

Department of the Treasury Financial Crimes Enforcement Network, ‘Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies’ <<https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf>> accessed 31 July 2017

“Legitimate” Bitcoin’s Value Soars after Senate Hearing - BBC News’
<<http://www.bbc.com/news/technology-24986264>> accessed 31 July 2017

‘Top 10 Countries in Which Bitcoin Is Banned’ <<https://www.cryptocoinsnews.com/top-10-countries-bitcoin-banned/>> accessed 31 July 2017

‘The Russian Bitcoin Ban Plan Is on Indefinite Hold - CryptoCoinsNews’
<<https://www.cryptocoinsnews.com/the-russian-bitcoin-ban-is-on-indefinite-hold/>> accessed 31 July 2017

‘Bitcoin’s Legality Around The World’
<<https://www.forbes.com/sites/kashmirhill/2014/01/31/bitcoins-legality-around-the-world/#4f737b7e3ccd>> accessed 31 July 2017

‘Legal Issues of Accepting Bitcoin That You Should Know About • LawKick Blog’
<<http://blog.lawkick.com/legal-issues-of-accepting-bitcoin/>> accessed 31 July 2017

‘Why Bitcoin Is Not Regulated | HuffPost’ <http://www.huffingtonpost.com/john-rampton/why-bitcoin-is-not-regula_b_9458864.html> accessed 31 July 2017

‘Technological Breakthroughs - Megatrends - PwC UK’
<<http://www.pwc.co.uk/issues/megatrends/technological-breakthroughs.html>> accessed 31 July 2017

‘Aiming to Make Malta the Silicon Valley of Gaming - MaltaToday.com.mt’
<http://www.maltatoday.com.mt/business/business_news/68155/aiming_to_make_malta_the_silicon_valley_of_gaming#.WX6gdtOGNE5> accessed 31 July 2017

‘Bitcoin Currency - Real, Virtual or Illegal?’
<<http://www.gamingtechlaw.com/2014/04/bitcoin-real-virtual-or-illegal-currency.html>>
accessed 31 July 2017

‘How Do Smart Contracts Work? – Bitcoin and Ethereum’ <<https://ark-invest.com/research/smart-contracts-work>> accessed 31 July 2017

John Ream, Yang Chu DS, ‘Upgrading Blockchains: Smart Contract Use Cases in Industry | Deloitte University Press’ <<https://dupress.deloitte.com/dup-us-en/focus/signals-for-strategists/using-blockchain-for-smart-contracts.html>> accessed 31 July 2017

‘How Do Smart Contracts Work? – Bitcoin and Ethereum’ <<https://ark-invest.com/research/smart-contracts-work>> accessed 31 July 2017

‘A Gentle Introduction to Smart Contracts | Bits on Blocks’ <<https://bitsonblocks.net/2016/02/01/a-gentle-introduction-to-smart-contracts/>> accessed 31 July 2017

‘CIO Explainer: What Is Blockchain? - CIO Journal. - WSJ’ <<https://blogs.wsj.com/cio/2016/02/02/cio-explainer-what-is-blockchain/>> accessed 31 July 2017

‘We Must Regulate Bitcoin. Problem Is, We Don’t Understand It | WIRED’ <<https://www.wired.com/2016/03/must-understand-bitcoin-regulate/>> accessed 31 July 2017

‘Regulating Bitcoin: How New Frameworks Could Be a Catalyst for Cryptocurrencies’ <<http://www.telegraph.co.uk/business/2017/04/16/regulating-bitcoin-new-frameworks-could-catalyst-cryptocurrencies/>> accessed 31 July 2017

‘Written Testimony of U.S. Secret Service for a Senate Committee on Homeland Security and Governmental Affairs Hearing Titled “Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies” | Homeland Security’ <<https://www.dhs.gov/news/2013/11/18/written-testimony-us-secret-service-senate-committee-homeland-security-and>> accessed 31 July 2017

Barrdear J and Kumhof M, ‘The Macroeconomics of Central Bank Issued Digital Currencies The Macroeconomics of Central Bank Issued Digital Currencies (on-Line)’ <www.bankofengland.co.uk/research/Pages/workingpapers/default.aspx> accessed 31 July 2017

‘Digital Currencies: Response to the Call for Information’ <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf> accessed 31 July 2017

‘Nick Szabo’s Latest Post On the Industrial Revolution’ <<https://www.cryptocoinsnews.com/nick-szabos-latest-post-industrial-revolution/>> accessed 31 July 2017

‘Blockchain in 2017: The Year of Smart Contracts | PCMag.com’
<<https://www.pcmag.com/article/350088/blockchain-in-2017-the-year-of-smart-contracts>>
accessed 31 July 2017

‘The Ultimate Guide to Blockchain Smart Contracts’
<<http://www.blockchaintechnologies.com/blockchain-smart-contracts>> accessed 31 July 2017

‘Thinking about Using Decentralized Ledger “Blockchain Technology” for Centralized Ledgers? Think Again. | LedgerX’ <<https://ledgerx.com/thinking-about-using-decentralized-ledger-blockchain-technology-for-centralized-ledgers-think-again/>> accessed 31 July 2017

‘Bitcoin: Decentralized Virtual Currency - The Data Center Journal’
<<http://www.datacenterjournal.com/bitcoin-decentralized-virtual-currency/>> accessed 31 July 2017

‘Op-Ed: What Is the True Meaning of “Decentralization” in Blockchain Technology? — Bitcoin Magazine’ <<https://bitcoinmagazine.com/articles/guest-post-what-is-the-true-meaning-of-decentralization-in-blockchain-technology-1474558340/>> accessed 31 July 2017

‘Decentralization Archives - CoinDesk’ <<https://www.coindesk.com/tag/decentralization/>>
accessed 31 July 2017

‘US States Working on Blockchain Legislation in 2017» Brave New Coin’
<<https://bravenewcoin.com/news/us-states-working-on-blockchain-legislation-in-2017/>>
accessed 31 July 2017

‘Decentralization & Governance: Can Bitcoin Have the Best of Both? - CoinDesk’
<<https://www.coindesk.com/decentralized-proven-otherwise/>> accessed 31 July 2017

‘Is Bitcoin Truly Decentralized? Yes – and Here Is Why It’s Important — Bitcoin Magazine’
<<https://bitcoinmagazine.com/articles/bitcoin-truly-decentralized-yes-important-1421967133/>> accessed 31 July 2017

‘Augur May Become the Greatest Gambling Platform in History. Is There Anything the Government Can Do to Stop It? - Hit & Run: Reason.com’

<<http://reason.com/blog/2015/08/11/augur-gambling-prediction-ethereum>> accessed 31 July 2017

‘Attorneys Author First-Ever Book on Blockchain Technology and the Law - Blockchain News’ <<http://www.the-blockchain.com/2016/11/15/attorneys-author-first-ever-book-blockchain-technology-law/>> accessed 31 July 2017

‘Gambling Industry – How Blockchain Can Make It More Transparent | Fintech Schweiz Digital Finance News – FintechNewsCH’ <http://fintechnews.ch/blockchain_bitcoin/transparent-gambling-blockchain-gambling-industry-how-blockchain-can-make-it-more-transparent/3844/> accessed 31 July 2017

‘Startup Will Use Blockchain Tech to Disrupt Online Gaming’ <<https://www.coindesk.com/one-startup-will-use-blockchain-disrupt-online-gaming/>> accessed 31 July 2017

‘Malta Is Gearing up to Greenlight Bitcoin Gambling - CoinDesk’ <https://www.coindesk.com/immediate-future-malta-gearing-greenlight-bitcoin-gambling/?utm_content=bufferde180&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer> accessed 31 July 2017

‘Are Smart Contracts Smart? A Critical Look at Basic Blockchain Questions - CoinDesk’ <<https://www.coindesk.com/when-is-a-smart-contract-actually-a-contract/>> accessed 31 July 2017

‘UNODC Launches Training to Tackle Cryptocurrency-Enabled Organized Crime’ <<https://www.unodc.org/unodc/en/frontpage/2017/May/unodc-launches-training-to-tackle-money-laundering-and-bitcoin-banking-fraud.html>> accessed 31 July 2017

Harvey T, ‘Cryptocurrencies Opening Fraud Gates’ <<http://www.fraud-magazine.com/article.aspx?id=4294982435>> accessed 31 July 2017

‘PSD2 - the Directive That Will Change Banking as We Know It’ <<https://www.evry.com/en/news/articles/psd2-the-directive-that-will-change-banking-as-we-know-it/>> accessed 31 July 2017

Whitehead Holly, ‘AML, Compliance and Financial Crime Blogs and Articles from ICT: Five Key Points of the Upcoming Fifth Anti Money Laundering Directive (5AMLD)’

<[https://www.int-comp.com/ict-views/posts/2017/04/10/five-key-points-of-the-upcoming-fifth-anti-money-laundering-directive-\(5amlld\)/](https://www.int-comp.com/ict-views/posts/2017/04/10/five-key-points-of-the-upcoming-fifth-anti-money-laundering-directive-(5amlld)/)> accessed 31 July 2017

Baille S, 'The ECB Just Killed Bitcoin in Europe – This Is Why – Salvador Baille' <<https://salvadorbaille.com/2016/10/20/the-ecb-just-killed-bitcoin-in-europe-this-is-why/>> accessed 31 July 2017

'European Central Bank Pushes for Tighter Digital Currency Control - CoinDesk' <<https://www.coindesk.com/ecb-control-digital-currencies-bitcoin/>> accessed 31 July 2017

'Press Release: ERP Integration to Distributed Ledger and Blockchain - Press Release' <<https://www.coindesk.com/press-releases/press-release-erp-integration-distributed-ledger-blockchain/>> accessed 31 July 2017

'Ether Review Legal Discussion #1 — Challenges in Blockchain Law' <<https://etherreview.info/ether-review-legal-discussion-1-challenges-in-blockchain-law-b96c56b73de9>> accessed 31 July 2017

'How Blockchain Is Decentralizing Gambling' <<https://www.techinasia.com/talk/blockchain-decentralizing-gambling>> accessed 31 July 2017

'Blockchain Is the Future of Insurance but What Are the Legal Risks?' <<http://www.gamingtechlaw.com/2017/03/blockchain-insurance-legal-risks.html>> accessed 31 July 2017

Ryder B, 'Governments May Be Big Backers of the Blockchain' <<https://www.economist.com/news/business/21722869-anti-establishment-technology-faces-ironic-turn-fortune-governments-may-be-big-backers?fsrc=scn/fb/te/bl/ed/landgrabgovernmentsmaybebigbackersoftheblockchain>> accessed 31 July 2017

'The European Union Wants to Identify Bitcoin Users - Altcoin Today' <<http://www.altcointoday.com/european-union-wants-identify-bitcoin-users/>> accessed 31 July 2017

'Stitches in Time: Why the Blockchain Needs (a Few) More Lawyers – Cryptolawyer.net' <<http://cryptolawyer.net/2015/11/stitches-in-time-why-the-blockchain-needs-a-few-more-lawyers/>> accessed 31 July 2017

‘The Future of Financial Infrastructure An Ambitious Look at How Blockchain Can Reshape Financial Services An Industry Project of the Financial Services Community | Prepared in Collaboration with Deloitte’ ‘What Are Bitcoin Nodes and Why Do We Need Them?’ <<https://www.coindesk.com/bitcoin-nodes-need/>> accessed 31 July 2017

Sironi P, *FinTech Innovation: From Robo-Advisors to Goal Based Investing and Gamification* (Wiley 2016)
<https://books.google.com.mt/books?id=xS2pDAAAQBAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q=blockchain&f=false> accessed 31 July 2017

Vandervort D, ‘Challenges and Opportunities Associated with a Bitcoin-Based Transaction Rating System’ <http://fc14.ifca.ai/bitcoin/papers/bitcoin14_submission_5.pdf> accessed 31 July 2017

‘Blockchain Faces Maze of Regulatory Complexities, Questions and Challenges | Thomson Reuters’ <<https://blogs.thomsonreuters.com/answerson/blockchain-faces-maze-of-u-s-regulatory-complexities-questions-and-challenges/>> accessed 31 July 2017

‘Blockchain 101 With Andreas Antonopoulos: How Bitcoin Makes Each Of Us As Powerful As A Bank’ <<https://www.forbes.com/sites/laurashin/2016/08/23/blockchain-101-with-andreas-antonopoulos-how-bitcoin-makes-each-of-us-as-powerful-as-a-bank/#3bf02d7366d3>> accessed 31 July 2017

‘Updated Law Will Oblige Travelers Entering US to Declare Digital Currency Holdings’ <<http://www.altcointoday.com/law-will-oblige-travelers-entering-us-to-declare-digital-currency-holdings/>> accessed 31 July 2017

‘Regulation Is Only Hope For Bitcoin: Morgan Stanley’ <https://cointelegraph.com/news/regulation-is-only-hope-for-bitcoin-morgan-stanley?utm_source=dlvr.it&utm_medium=facebook> accessed 31 July 2017

‘Blockchain: Issues in Competition & Consumer Law | Michael Milnes | Pulse | LinkedIn’ <<https://www.linkedin.com/pulse/blockchain-issues-competition-consumer-law-michael-milnes>> accessed 31 July 2017

‘Bitcoin Tech May Be the Future, but It Raises Serious Antitrust Questions | TheHill’ <<http://thehill.com/blogs/pundits-blog/technology/335140-is-bitcoin-tech-the-future-or-will-they-violate-antitrust-laws>> accessed 31 July 2017

‘SEC.gov | Home’ <<https://www.sec.gov/>> accessed 31 July 2017

‘Blockchain and Public Securities: Shedding Light on “Going Dark” - Lexology’ <<http://www.lexology.com/library/detail.aspx?g=c33df1b5-f5bc-4041-9bf0-105ad7ea3f4b>> accessed 31 July 2017

‘Colored Coins Paint Sophisticated Future for Bitcoin - CoinDesk’ <<https://www.coindesk.com/colored-coins-paint-sophisticated-future-for-bitcoin/>> accessed 31 July 2017

‘What Are Coloured Coins and Meta Coins? | CryptoCompare.com’ <<https://www.cryptocompare.com/coins/guides/what-are-coloured-coins-and-meta-coins/>> accessed 31 July 2017

‘Colored Coins, What They Are and How They Work On The Bitcoin Blockchain - Bitcoinist.com’ <<http://bitcoinist.com/colored-coins-work-bitcoin-blockchain/>> accessed 31 July 2017

‘Black Tuesday For Crypto Markets As \$10 Bln Wiped In 24 Hours, Ethereum Down 20%+’ <https://cointelegraph.com/news/black-tuesday-for-crypto-markets-as-10-bln-wiped-in-24-hours-ethereum-down-20?utm_source=dlvr.it&utm_medium=facebook> accessed 31 July 2017

‘Will Ethereum Based Smart Contracts Automate Contract Lawyers?’ <<http://www.trustnodes.com/2017/04/04/will-ethereum-based-smart-contracts-automate-contract-lawyers>> accessed 31 July 2017

‘Money Laundering and Terrorist Financing: Council Agrees Its Negotiating Stance - Consilium’ <<http://www.consilium.europa.eu/en/press/press-releases/2016/12/20-money-laundering-and-terrorist-financing/>> accessed 31 July 2017

‘ECB Wants To Curb Bitcoin Use Over Fears It May “Lose Control Over Money Supply” | Zero Hedge’ <<http://www.zerohedge.com/news/2016-10-19/ecb-wants-curb-bitcoin-use-over-fears-it-may-lose-control-over-money-supply>> accessed 31 July 2017

‘Is Bitcoin Money? | Anita Ramasastry | Verdict | Legal Analysis and Commentary from Justia’ <<https://verdict.justia.com/2014/09/09/bitcoin-money>> accessed 31 July 2017

‘Bitcoin Needs Government Regulation to Rise Further, Morgan Stanley Says - MarketWatch’ <<http://www.marketwatch.com/story/bitcoin-needs-government-regulation-to-rise-further-morgan-stanley-says-2017-06-13>> accessed 31 July 2017

‘Legal Implications of Expanded Use of Blockchain Technology — Financier Worldwide’ <<https://www.financierworldwide.com/legal-implications-of-expanded-use-of-blockchain-technology/#.WX6XcdOGNE7>> accessed 31 July 2017

‘Ether Review Legal Discussion #1 — Challenges in Blockchain Law’ <<https://etherreview.info/ether-review-legal-discussion-1-challenges-in-blockchain-law-b96c56b73de9>> accessed 31 July 2017

MGA, ‘Guidelines | Technical Infrastructure Hosting Gaming and Control Systems Remote Gaming’ <<http://www.mga.org.mt/wp-content/uploads/Guidelines-Technical-Infrastructure-hosting-Gaming-and-Control-Systems-Remote-Gaming.pdf>> accessed 31 July 2017

‘Bitcoin vs. Big Government - Reason.com’ <<http://reason.com/archives/2013/04/09/bitcoin-vs-big-government>> accessed 31 July 2017

‘Blockchain: Five Profound Legal Impacts | Cornelius Grossmann | Pulse | LinkedIn’ <<https://www.linkedin.com/pulse/blockchain-five-profound-legal-impacts-cornelius-grossmann?articleId=6214393509496131584>> accessed 31 July 2017

‘Blockchain - Legal and Regulatory Issues around Distributed Ledger Technology | Legal Briefing | Opinion | CIO UK’ <<http://www.cio.co.uk/opinion/legal-briefing/blockchain-legal-regulatory-issues-around-blockchain-3638814/>> accessed 31 July 2017

‘EY - Building a Better Working World’ <<https://betterworkingworld.ey.com/better-questions/blockchain-five-legal-impacts>> accessed 31 July 2017

‘Decentralized Gambling: Laws, Morals, and Ethics - ETHNews.com’ <<https://www.ethnews.com/decentralized-gambling-laws-morals-and-ethics>> accessed 31 July 2017

‘Distributed Ledgers Part I: Bitcoin Is Dead | FiniCulture’ <<http://finiculture.com/distributed-ledgers-part-i-bitcoin-is-dead/>> accessed 31 July 2017

‘Who Controls the Blockchain?’ <<https://hbr.org/2017/04/who-controls-the-blockchain>> accessed 31 July 2017

‘The Governance of Blockchains – The Control’ <<https://thecontrol.co/the-governance-of-blockchains-5ba17a4f5da6>> accessed 31 July 2017

‘The Evolution of Blockchain Governance – Peercoin Pulse – Medium’ <<https://medium.com/@PeercoinPulse/the-evolution-of-blockchain-governance-6ecb793acc1>> accessed 31 July 2017

Atzori M, ‘Blockchain Technology and Decentralized Governance: Is the State Still Necessary?’ <[http://www.the-blockchain.com/docs/Blockchain Technology and Decentralized Governance - Is the State Still Necessary.pdf](http://www.the-blockchain.com/docs/Blockchain%20Technology%20and%20Decentralized%20Governance%20-%20Is%20the%20State%20Still%20Necessary.pdf)> accessed 31 July 2017

‘NSA Leak Confirms Skynet Is for Real - ScienceAlert’ <<http://www.sciencealert.com/nsa-leak-confirms-skynet-is-for-real>> accessed 31 July 2017

‘How Blockchain Will Affect Financial Services Employment’ <<http://news.efinancialcareers.com/us-en/269710/how-blockchain-will-affect-financial-services-employment>> accessed 31 July 2017

‘Under the Microscope: Economic and Environmental Costs of Bitcoin Mining’ <<https://www.coindesk.com/microscope-economic-environmental-costs-bitcoin-mining/>> accessed 31 July 2017

‘How Small Bitcoin Miners Lose on the Crypto-Currency Boom-Bust Cycle | New Republic’ <<https://newrepublic.com/article/121089/how-small-bitcoin-miners-lose-crypto-currency-boom-bust-cycle>> accessed 31 July 2017

‘Leveraging the Remote Gaming Advantage’ <<http://www.mga.org.mt/wp-content/uploads/Leveraging-the-Gaming-Advantage.pdf>> accessed 31 July 2017

‘Central Banks Beat Bitcoin at Own Game with Rival Supercurrency’ <<http://www.telegraph.co.uk/business/2016/03/13/central-banks-beat-bitcoin-at-own-game-with-rival-supercurrency/>> accessed 31 July 2017

‘Europe Lays Out Roadmap to Restrict Payments in Cash and Cryptocurrencies - Bitcoin News’ <<https://news.bitcoin.com/europe-roadmap-restrict-payments-cash-cryptocurrencies/>> accessed 31 July 2017

‘The European Union Wants to Identify Bitcoin Users - CryptoCoinsNews’
<<https://www.cryptocoinsnews.com/the-european-union-wants-to-identify-bitcoin-users/>>
accessed 31 July 2017

Bryan D and Rafferty M, ‘Financial Derivatives: The New Gold?’ (2006) 10 *Competition & Change* 265 <<http://journals.sagepub.com/doi/10.1179/102452906X114375>> accessed 31 July 2017

Ali R, ‘Innovations in Payment Technologies and the Emergence of Digital Currencies of the Bank’s Financial Market Infrastructure Directorate, John Barrdear of the Bank’s Monetary Assessment and Strategy Division, and Roger Clews and James Southgate of the Bank’s Markets Directorate’
<<http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3digitalcurrenciesbitcoin1.pdf>> accessed 31 July 2017