THE EFFECT OF BITCOIN ON MONEY LAUNDERING LAW

JONATHAN GALEA

Thesis submitted in partial fulfilment of the
Degree of Doctor of Laws

Faculty of Laws

University of Malta

May 2015

DECLARATION OF AUTHORSHIP

I, **Jonathan Galea**, declare that this thesis entitled *The Effect of Bitcoin on Money Laundering* Law, and the work presented in it is my own.

I confirm that:

- The word count of the thesis is 35,000.
- The work was done in partial fulfilment of the degree of Doctor of Laws at the Faculty of Laws at the University of Malta.
- Where any part of this thesis has previously been submitted for a degree or any other qualifications at this University or any other institution, this has been clearly stated.
- Where I have consulted the published works of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all sources used for the purpose of this work.
- I have not commissioned this work, whether in whole or in part, to a third party and that this work is my own work.
- I have read the University of Malta’s guidelines on plagiarism.

Signed:

Jonathan Galea

ABSTRACT

This thesis sets out to determine the influence of Bitcoin on the current Anti-Money Laundering law in Malta, which is largely derived from European Union Directives. The Directives in turn are based on the Financial Action Task Force Recommendations, and hence what shall be stated in this thesis may be, *mutatis mutandis*, applicable to other jurisdictions as well.

Bitcoin is an innovative technological advancement in payment systems, with its most intriguing features being that it is completely virtual and lacks the oversight of a central authority. Perhaps the most worrying feature for legislators is that it is pseudonymous, thus hiding the identities of the persons transacting if there is no oversight. There have been a few incidents to date where Bitcoin and other Virtual Currencies were used with illicit intent. Therefore, with the advent of Bitcoin, it is imperative to ascertain whether the existing Anti-Money Laundering framework is enough to curb abuse through the utilisation of such a 'currency', or whether a revamped system is required.

A comparative analysis is indispensable for this thesis, as currently there is no ad-hoc legislation on Bitcoin in Malta, and very few foreign legislative attempts on regulating Bitcoin for that matter. Moreover, a simplified technological overview of the workings of Bitcoin is important as well since it vastly differs from *fiat* currencies in some aspects. The thesis shall ultimately propose changes required both in the Bitcoin infrastructure itself as well as in the current Anti-Money Laundering framework in Malta, with the former requiring intervention from the Bitcoin community itself rather than a mere localised effort. Moreover, it is important to remember that notwithstanding copious amounts of research, both theoretical and practical, conducted before and during the writing of this thesis, ultimately the subject revolves around a technology which is still in its infancy, and may exhibit future features which would be hitherto unascertainable.

Bitcoin – Virtual Currencies – Money Laundering – Blockchain – Customer Identification

First of all, I'd like to dedicate this thesis to my mother and father, who made their riskiest bet ever against all odds, sacrificing and staking everything on my receiving a proper education. Your wager has succeeded. I am proud to call you my parents.

Secondly, I'd like to dedicate it as well to Vincenza, who fought the hardest battle of them all and put on a brave face throughout. You have truly lived up to your name and emerged victorious, and have served as my best source of inspiration.

Last but not least, I'd like to dedicate this work to those angels who have been killed in the Peshawar massacre and the Kenyan University of Garissa attack. Here's to a future where no one is put to death while drinking from the fountain of knowledge.

Table of Contents

TABLE OF STATUTES AND TREATIES

Malta

Prevention of Money Laundering Act, Chapter 373 of the Laws of Malta

Prevention of Money Laundering and Funding of Terrorism Regulations, S.L. 373.01

Dangerous Drugs Ordinance, Chapter 101 of the Laws of Malta

Criminal Code, Chapter 9 of the Laws of Malta

Central Bank of Malta Act, Chapter 204 of the Laws of Malta, Article 44

Financial Institutions Act, Chapter 376 of the Laws of Malta

Act III of 2015 - Various Laws (Prevention of Money Laundering and Funding of Terrorism) (Amendment) Act, 2015 [Government Gazette of Malta No. 19,385 – 20.02.2015]

L.N. 464 of 2014 - Prevention of Money Laundering and Funding of Terrorism (Amendment) Regulations, 2014 [Government Gazette of Malta No. 19,358 – 16 December 2014]

European Union

Consolidated Version of the Treaty on the Functioning of the European Union [2007] OJ C326/47

Council Directive (EC) 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering [1991] OJ L166/77

Council Directive (EC) 2001/97 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering [2001] OJ L344/76

Council Directive (EC) 2005/60 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing [2005] OJ L309/15

Proposal for a Council Directive (EC) 2013/0025 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing [2013]

Electronic Money Directive (2009/110/EC) on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC [2009] OJ L267/7

European Parliament and Council Regulation 1781/2006 on information on the payer accompanying transfers of funds [2006] OJ L345/1

European Parliament and Council Directive 2014/42/EU on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union [2014] OJ L127/39

Germany

Banking Act of the Federal Republic of Germany (Kreditwesengesetz, KWG)

Criminal Code in the version promulgated on 13 November 1998, Federal Law Gazette [Bundesgesetzblatt] I p. 3322, last amended by Article 3 of the Law of 2 October 2009, Federal Law Gazette I p. 3214

Isle of Man

Proceeds Of Crime (Business In The Regulated Sector) Order 2015, Article 1(mm)

Japan

The Act on Prevention of Transfer of Criminal Proceeds (Act no. 22 of 2007)

The Act on Punishment of Organized Crimes and Control of Crime Proceeds (Act no. 136 of 1999)

United States

Assembly Bill 129, California Assembly, 23 June 2014

Bank Secrecy Act, 26 October 1970

Securities Exchange Act, 6 June 1934

U.S. Code of Crimes and Criminal Procedure, Title 18

U.S. Code, Title 31, Chapter 53

International Conventions

United Nations Vienna Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (adopted 20 December 1988, entered into force 11 November 1990)

TABLE OF JUDGEMENTS

Malta

Il-Pulizija vs. Carlos Frias Mateo, Court of Magistrates (Criminal Judicature), 5 August 2011 [Referenza Numru: 1010/2009]

Il-Pulizija vs. Carlos Frias Mateo, Court of Criminal Appeal (Inferior), 19 January 2012 [Appell Kriminali Numru: 356/2011]

Mario Camilleri & Pierre Camilleri vs. L-Avukat Ġenerali, First Hall, Civil Court (Constitutional Jurisdiction) 15 November 2010 [Rikors Numru: 18/2007]

Egbomon Morgan Ehi vs. L-Avukat Ġenerali, Constitutional Court, 16 March 2011 [Appell Ċivili Numru: 21/2009/1]

United States

Securities and Exchange Commission v. Trenton T. Shavers and Bitcoins Savings and Trust, United States District Court (Eastern District of Texas: Sherman Division), 23 July 2013, Case No. 4:13-CV-416

United States of America v. E-Gold Ltd, Gold & Silver Reserve, Inc., Douglas L. Jackson, Barry K. Downey, and Reid A. Jackson, United States District Court for the District of Columbia, 20 November 2008, Case No. 1:07-CR-00109-RMC

United States of America v. Liberty Reserve S.A., Arthur Budovsky a/k/a "Arthur Belanchuk" a/k/a "Eric Paltz", Vladimir Kats a/k/a "Ragnar, Ahmed Yassine Abdelghani a/k/a Alex, Allan Esteban Hidalgo Jimenez a/k/a Allan Garcia, Azzeddine El Amine, Mark Marmilev a/k/a "Marko", and Maxim Chukharev, United States District Court for the Southern District of New York [sub-judice]

United States of America v. Robert M. Faiella, a/k/a "BTCKing", and Charlie Shrem, United States District Court for the Southern District of New York, 20 January 2015

United States of America vs. Ross William Ulbricht, aka "Dread Pirate Roberts", aka "DPR", aka "Silk Road", Southern District of New York Court [sub-judice]

ACKNOWLEDGEMENTS

First of all, I would like to thank my parents Brian and Pauline, and my brother Kristian for their steadfast and unwavering support throughout these years.

Secondly, I would like to thank my tutors Dr. Antonio Ghio and Dr. Leonard Caruana for supervising my work, as well as Dr. Anton Bartolo and Mr. Antonio Ghirlando for graciously accepting my requests for an interview and giving me insightful advice.

Last but not least, I would like to express my thanks to all those persons who have made these past six years a truly memorable period.

ABBREVIATIONS

1MLD = First Money Laundering Directive

2MLD = Second Money Laundering Directive

3MLD = Third Money Laundering Directive

AG – Attorney General

AML – Anti-Money Laundering

BaFin - German Federal Financial Supervisory Authority

BTC – Bitcoin

CDD – Customer Due Diligence

CBMA – Central Bank of Malta Act

EBA – European Banking Authority

ECB – European Central Bank

EG – E-Gold

EU – European Union

FATF – Financial Action Task Force

FIAU – Financial Intelligence Analysis Unit

FIU – Financial Intelligence Unit

FC – *Fiat* Currency

FTR – Prevention of Money Laundering and Funding of Terrorism Regulations

HMT – British HM Treasury

IT – Information Technology

KYC – Know Your Customer

LR – Liberty Reserve

MOU – Memorandum of Understanding

MFSA – Malta Financial Services Authority

MLD – Money Laundering Directive

MONEYVAL - Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism

P4MLD = Proposal for a Fourth Money Laundering Directive

PMLA – Prevention of Money Laundering Act

SR – Silk Road

UK – United Kingdom of Great Britain and Northern Ireland

UN – United Nations

US – United States of America

VC – Virtual Currency

GLOSSARY

Address – an address is a unique string of letters and numbers assigned to a particular Bitcoin wallet, to which Bitcoin can be sent or from which Bitcoin can be received

AML Framework – the rules, regulations and practices making up the anti-money laundering regime

Bitcoin – a decentralised cryptocurrency which solely exists in the virtual domain and can be converted into *fiat* currencies and vice-versa[1]

Virtual currency – any other cryptocurrency apart from Bitcoin which can be converted into *fiat* currencies and vice-versa

Bitcoin network – the network of miners which consolidate the infrastructure via which BTC transactions are processed and confirmed onto the blockchain

Block – a record of all the transactions which were effected in the time period between the last found block and the solution of the current block

Blockchain – the list of all the blocks mined since the conception of Bitcoin, each identifiable by a unique successive number

Block Reward – the reward, in BTC, earned by the miner which first solves the block being mined

Block Confirmation – once a block is solved, the solution is relayed across the Bitcoin network, whereby consensus is achieved once 51% of the miners agree that the solution found is the applicable one, hence 'rubber-stamping' that block, verifying it and confirming it onto the Blockchain

Dark net - the underground websites accessible only via Tor

[1] Refer to Chapters 1.1 & 1.2 for a detailed explanation of Bitcoin and how it works

Encumbrance - the locking script which secures the transaction when it is sent through the BTC network. It acts as a highly-complex unique password on the transaction, and can only be unlocked by the recipient to whom it is addressed

Exchanges/VC exchanges– websites which offer an exchange service from *fiat* currencies to virtual currencies and/or vice-versa, whether at a cost or not

Fiat currencies – the traditional/conventional currencies which are considered as legal tender and hence issued by a particular State, such as the U.S. Dollar and the Euro

IP address - a unique address identifying the machine, such as a laptop, which is connected to the Internet. It also indicates the originating region of the connection

Mining – the process in which computational devices are used to solve complex mathematical formulae for that particular block; whichever 'miner' solves the mathematical problem first gets the block reward in the form of newly 'minted' Bitcoins, and validates all the transactions which took place during the time taken for that block to be solved, which on average is ten minutes for Bitcoin blocks

Network attack – otherwise known as a '51% attack', it represents a scenario where 51% or more of the miners control the network, and hence can verify dummy or fake transactions and add them to the block. Since the mined blocks require verification by 51% or more of the network, this would potentially lead to the collapse of the BTC network as the controlling miners could in theory produce as many BTCs as they want and verify them themselves

Node – a device with access to the Internet which has Bitcoin software installed on it and acts as a bridge connected to the BTC network

Password – an extra layer of security protecting the BTC wallet whereby the user encrypts access to such wallet with a password of choice

Password cracking/hacking - Password cracking is the process of recovering a password, usually by 'brute-forcing' which entails feeding as many passwords as possible until the right one is inputted.

Private Key – a unique encrypted code allowing the wallet user access to his/her Bitcoin stored virtually on the Bitcoin blockchain

Proxy server - a server that relays a user's connection through its own, hence providing only its own 'identity' to the sites it visits, masking the identity of the machine originally requesting access to the visited web page

Public Key – a code derived from the private key via an irreversible mathematical process which acts as a public identifier for a particular wallet

Onion routing – it functions similarly to a proxy server; however, it uses a network of nodes via encrypted mechanisms, layering the original connection in layers of anonymity in the process and ensuring a more elevated level of security than simple proxy servers

Signature – an algorithm derived from the private key of a particular wallet, verifying that a transaction was authorised from that particular wallet. A transaction is included onto the blockchain once the signature and accompanying public key are co-validated as having sourced from the corresponding Bitcoin wallet

Tor Browser – a software program which enables a user to access the Internet via encrypted and anonymous connections, hence hiding the identity of the user. It utilises Onion routing to establish such connections

Tumbler – a software program which mixes several transactions originating from different addresses, making it difficult to pinpoint the origin of a single transaction. It is also known as a coin-mixing service

VC-VC exchanges – websites which offer an exchange service solely and exclusively from one virtual currency to another

Wallet – A file in which the private keys are stored, hence allowing access to a user's Bitcoin/s. A Bitcoin wallet is normally accessible by a user through a local (offline) or online software program with a graphical user interface

Web servers - programs which 'serve' the files forming part of a Web page to the computer or device asking for access to such Web page. The Web Servers are usually run on dedicated machines which store data allowing these processes to take place, and may include, inter alia, user accounts information, passwords, etc.

INTRODUCTION

Over the past few years, a technological phenomenon has rapidly been developing, namely that of virtual currencies (VCs). VCs differ from *fiat/*physical currencies (FCs) such as the U.S. Dollar and the Euro, mainly on the point that the latter are backed by governments which declare such currencies to be accepted as legal tender and have a value associated to them[2]. On the other hand, VCs currently lack such State backing, with their values being determined purely on demand and supply[3]. Nonetheless, both have a common denominator, which is that of not having any intrinsic value in the currency itself, but rather used as a means of representation of value.

VCs themselves are split into cryptocurrencies and non-cryptocurrencies. The main distinction between them is that non-cryptocurrencies are centralised while cryptocurrencies may be centralised or decentralised and, as the name implies, heavily rely on cryptography as security means, thus giving them an edge over the nearly-extinct non-cryptocurrencies[4]. This thesis will focus on the most popular cryptocurrency in circulation, which is Bitcoin (BTC). BTC has been conceived in 2009[5] and has steadily risen in popularity, with 1 BTC reaching a value of over $1000 in November 2013[6] and fluctuating ever since according to various factors, including tentative legislation by some countries[7]. Other derivatives have developed by countless numbers with some gaining traction[8], but what is applicable to BTC is, by and large, applicable to most of the other VCs as well.

[2] 'Definition of *fiat* money' (*Investopedia*) <http://www.investopedia.com/terms/f/fiatmoney.asp>

[3] Alec Liu, 'Why Bitcoins are just like Gold'(*Motherboard,* 21 March 2013) <http://motherboard.vice.com/blog/why-bitcoins-are-just-like-gold> accessed 20 September 2014

[4] D.K. Subramanian, 'Digital Currency' [2013] FF 2, 6

[5] Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System'(*Bitcoin.org* 2009) <http://bitcoin.org/bitcoin.pdf> accessed 8 August 2013

[6] Ben Rooney, 'Bitcoin worth almost as much as gold'(*CNN Money,* 2013) <http://money.cnn.com/2013/11/29/investing/bitcoin-gold/> accessed 20 September 2014

[7] Refer to Chapter 3.1

[8] Samuel Gibbs, 'Nine Bitcoin alternatives for future currency investments'(*The Guardian,* 28 November 2013) <http://www.theguardian.com/technology/2013/nov/28/bitcoin-alternatives-future-currency-investments> accessed 20 September 2014

Unlike FCs, BTC are not regulated by any bank, and the time required for a transaction to be completed is much shorter than that involved in the transfer of FCs[9]. BTC users also enjoy a debatable level of anonymity, although all the transactions conducted are visible and available on a public ledger, making it more a matter of pseudonymity rather than anonymity as shall be discussed in Chapter 1.1.

The connection to Money Laundering

The advantage of pseudonymity coupled with the fact that BTC are, as of yet, unregulated as a currency by any bank, might potentially encourage the widespread use of BTC in black markets. The most famous incident to date is the Silk Road case[10], concerning an 'underground' website accessible only via Onion routing which conceals the identities of the users. Drugs, along with other illegal objects, were being traded on the website, and the currency of choice for the transactions was BTC. The case will be dealt with in much greater detail in the thesis; suffice it to say that millions' worth of BTC were seized by the American government following the closing-down of the website, leading to a dramatic drop in its value which ironically in turn led to a huge upsurge in the purchase of BTC[11].

Consequently, some legislators starting becoming concerned about the potential of BTC for money-laundering and insist that the advent of VCs will be invaluable for criminals to conceal their transactions and to launder money[12], while others state that through preventive and proactive measures, these fears will remain unfounded[13]. That will be the main subject of the thesis.

[9] Ibid.

[10] Refer to Chapter 3.4.1

[11] Robert McMillan, 'Bitcoin Values Plummet $500M, Then Recover, After Silk Road Bust'(*Wired*, 2 October 2013) <http://www.wired.com/2013/10/bitcoin-market-drops-600-million-on-silk-road-bust/> accessed 22 September 2014

[12] Rebecca Falconer, 'World powers react to the Bitcoin boom'(*Al Jazeera*, 7 December 2013) <http://www.aljazeera.com/indepth/features/2013/12/world-powers-react-bitcoin-boom-2013127115950323990.html> accessed 22 September 2014

[13] Matt Clinch, 'Bitcoin recognized by Germany as 'private money'' (*CNBC*, 19 August 2013) <http://www.cnbc.com/id/100971898> accessed 22 September 2014

Objective of the thesis

The subject of the thesis will revolve around the issue on whether current AML (anti-money laundering) legislation is enough to prevent rampant abuse of BTC in money-laundering practices, as well as whether BTC in its current state can coexist with the AML framework. The focus will be on the criminal aspect rather than the IT one, although both will intertwine inevitably at intervals. At this current point in time, the main worry of most States is in fact the criminal potential for BTC and other VCs. The author shall **analyse the current Maltese AML Framework and the current BTC infrastructure, and shall strive to determine whether any changes are needed for the two to co-exist.**

Potential difficulties

Two of the biggest problems faced in completing the thesis were the current lack of legislation and the widespread misconceptions of what BTC really represents. The former is slowly being developed and hence a comparative study is indispensable to truly answer the previously mentioned questions, while the latter can only be addressed through a simplified explanation of how BTC works. In order to counter both of these problems, the author has deeply researched how BTC and other VCs work, including both theoretical research and practical exercises by mining and transacting in BTC, as well as conducting surveys in order to gain a better understanding of the practical side of money laundering legislation[14]. Moreover, due to BTC being such a novel subject, continuous updates are being issued, making it difficult to ensure that all the latest information has been included in the thesis. In order to partly counter this problem, the author felt it necessary to implement an information-collection cut-off date set at the 1st of May, 2015, which is the latest date possible to ensure adequate time for ulterior revisions of the thesis before submission.

A considerable dose of IT terminologies and explanations were inevitable, and although the main focus of the thesis was on AML legislation and legal issues, the tackling of the thesis necessitated an IT background and heavy research on part of the author. Limiting the subject strictly to the effect of BTC on AML legislation was not an easy task, especially due to the heavy IT influence; the simplification of the workings of BTC proved to be a difficult job, especially when considering the complex mathematical formulae and intricate programming

[14] Refer to Surveys in Chapter 4.3.1

involved. Great care was taken in order to ascertain that the technological aspect did not eclipse the legal aspect, tackling each one in turn and consequently marrying both concepts in Chapter 4.

It is worth pointing out that BTC and other VCs are still a largely untapped and unknown source of technological innovation, and this thesis seeks to tackle a single facet, namely the money laundering aspect. For the sake of brevity, the author has to omit from including an analysis of whether BTC generally classifies and ticks the requirements of a currency, limiting himself to analysing solely whether BTC may classify as a currency under Maltese legislation.

Summary of Chapters

'Chapter 1: Bitcoin' focuses on the most important technical aspects of BTC which are pertinent to the thesis, and shall give an overview of its advantages and disadvantages.

'Chapter 2: The Anti-Money Laundering Regime' is an overview of the current international, EU and Maltese AML regimes which are intertwined and connected.

'Chapter 3: The legal standing of Bitcoin especially with regards to Money Laundering' is a comparative analysis of how BTC is treated in several handpicked jurisdictions, with a close look being taken at research papers, opinions and cases as well.

'Chapter 4: Critical Overview of the Bitcoin Infrastructure vis-à-vis AML policies and the current Anti-Money Laundering Regime in Malta' is the culmination of the thesis, and involves researched points through surveys and personal experience of the author. The suggestions to changes in both the BTC network and the Maltese AML framework are incorporated herein.

Last point

Finally, the author feels it necessary to point out that what is said about BTC vis-à-vis the AML framework can, by and large, be applicable to most VCs currently on the market. Most VCs share many of BTC's attributes, such as pseudonymity and non-reversibility of the transactions, and hence most of the references to BTC can be substituted with another VC while still retaining the original sense of what is being said. Therefore, any reference to BTC in this thesis may also be construed as a reference to VCs, namely convertible decentralised cryptocurrencies, which, as the name implies, can be converted into FCs and vice-versa. Also, any reference to "the author" signifies a reference to Jonathan Galea, unless otherwise expressly stated.

CHAPTER 1 – BITCOIN

In essence, BTC is a peer-to-peer payment system deriving from an open-source software[15]. BTCs are created through a process which is known as 'mining'; this involves solving complex mathematical computations through computer power, which rewards successful calculations in BTC, once such work is proven through a computational algorithm. In essence, this is the process required for the creation of a new 'block'. The value of BTC depends on demand and supply, and BTC can either be acquired through the mining process or by exchanging them with a FC through exchange services found on the Internet. In order to truly gain a better understanding of the possible impact of BTC upon the AML framework, a short technical explanation of the underlying technology of BTC is indispensable.

1.1 - A BRIEF TECHNICAL EXPLANATION OF BITCOIN

BTC is a fully digital asset and has no tangible or material form. It is a decentralised convertible VC, differing from other VCs such as Facebook credits [16] and Amazon points[17], which are centralised and non-convertible. It is built on a peer-to-peer network, where all the constituents of the BTC network secure it and consensus on the latest block found is achieved once 51% or more of the BTC miners agree that the latest block has indeed been found and the calculation has been solved. BTC may be seen as permitting each and every person becoming his or her own private banker since no central authority is needed to mint new units, and conduct transactions without the need of an intermediary. The transactions are also highly secured via cryptography and the details of every transaction are encrypted, which is why BTC is also known as a 'cryptocurrency'.

[15] Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System'

[16] David Cohen, 'Farewell, Facebook Credits'(*Adweek*, 13 September 2013) <http://www.adweek.com/socialtimes/farewell-facebook-credits/428240> accessed 29 October 2014

[17] 'Shop with Points' (*Amazon* website) <http://www.amazon.com/b?node=2634438011> accessed 29 October 2014

BTC are created through the mining process, whereby new BTC are created every time a new block is found after a complex calculation is solved via the computational power of a miner. The 'winning' miner transmits the finding of the block throughout the whole BTC network to notify other miners that the latest block has been found, and the race starts over again to find the next block. The winning miner receives a reward for finding the latest block; such reward comes in the form of newly minted, or created, BTC and also gathers the transaction fees of all the transactions put through while the latest block was being searched for. On average, a new block is found every ten minutes[18]. There is a finite amount of BTC, with the total number of BTC being 21 million. It is calculated that the last BTC block will be mined in 2140, after which miners will rely on transaction fees to recoup the costs as no more BTC blocks will be mineable[19].

BTC is built on the so-called block-chain technology. A block is made up of the transactions conducted and completed in the ten-minute window it takes to find the next and newest block; once the newest block is found, the transactions are then confirmed by every BTC miner on the network, confirming their validity and their authenticity and acting as an official stamp of approval on those transactions conducted in that block. Every block mined since the conception of BTC can be traced on the public ledger, and each block is built on the preceding one, confirming the solved calculations of the previous blocks. In fact, most BTC connoisseurs acknowledge that a BTC transaction is deemed to be fully irreversible once it achieves six confirmations[20]; in other words, once six consecutive newer blocks are found, it would require an abnormal amount of computational power to reverse or alter all the transactions found in six blocks. The transactions are hence 'stamped' by every BTC miner in the network, ensuring the security of the network and one of the most salient advantages of a peer-to-peer network.

The transactions work in the following manner: Charles has 4 BTC stored in his BTC wallet. He wants to send 1 BTC to Mary. Through his BTC wallet, Charles transfers 1 BTC to Mary's public wallet address; the transfer is digitally signed with Charles' private keys[21] and

[18] A.M. Antonopoulos, *Mastering Bitcoin* (1st, O'Reilly Media, California, U.S.A. December 2014) pg. 175

[19] Ibid., pg. 2

[20] Alex Gorale, 'Are Bitcoin Zero Confirmation Transactions Safe?'(*CryptoCoinsNews*, 2 January 2015) <https://www.cryptocoinsnews.com/zero-confirmation-transactions-safe/> accessed 4 April 2015

[21] The concept of traditional ownership does not apply to BTC, as one cannot not physically own BTC – one uses a set of private keys to access the amount of BTC matching to such private keys. If the private keys are

'encumbered' with a script lock which can only be unlocked by the addressee of the transaction, which in this case is Mary[22]. The transaction is made identifiable with a public key; the private key is not shown as it is solely utilisable by the person accessing his/her BTC on the network, and is heavily encrypted for security purposes. As the transaction is transferred throughout the BTC network via a so-called node, it will only stop until it reaches Mary's wallet which has the correct code/script to unlock it and thus receive the payment of 1 BTC. The code is unique to the transaction and hence cannot be availed of by someone else.

It is the first VC to solve the double-spend problem which plagued other decentralised VCs. 'Double-spend', simply put, means using the same set of coins or currency to conduct a transaction twice. This problem became salient with the use of digital currencies as one could theoretically 'spend' a set amount by sending the digital file containing the coins to another person, while keeping a copy of the file himself and spend it again elsewhere, if there is no valid means of confirming and executing a transaction. Traditionally, the double-spend issue was solved by the use of a central authority which monitored and validated the transactions, ergo the centralisation of the currency. BTC managed to solve the problem with the use of a public ledger which keeps a record of all the transactions, and new transactions are checked against the whole ledger to verify that they have not been executed or spent before[23].

The common perception of BTC is that it is a completely anonymous currency; however, this is definitely not the case. Thanks to the public ledger which lists all the transactions taking place and the impossibility of hiding a transaction from the ledger as otherwise it wouldn't be recognised on the BTC network, a BTC transaction could theoretically be traced back to the person who authorised it, as a BTC address is public and the address can be pinpointed to a particular person, especially if he/she has shared such address before[24]. The process of

lost, which are found in the files constituting the wallet, then access to the BTC on the blockchain is permanently lost; they are not 'destroyed', but they cannot be accessed by the user anymore.

[22] Ibid., pg. 124

[23] Daniel Cawrey, 'Is Double Spending Unconfirmed Transactions a Concern for Bitcoin?'(*CoinDesk*, 23 April 2014) <http://www.coindesk.com/double-spending-unconfirmed-transactions-concern-bitcoin/> accessed 29 October 2014

[24] Tom Simonite, 'Mapping the Bitcoin Economy Could Reveal Users' Identities'(*Technology Review*, 5 September 2013) <http://www.technologyreview.com/news/518816/mapping-the-bitcoin-economy-could-reveal-users-identities> accessed 29 October 2014

linking a BTC address to a particular person is facilitated by the fact that BTC exchanges in certain jurisdictions are bound to abide by KYC requirements and have to store certain information of their users; hence, the BTC exchange can provide information about BTC addresses linked to a user and provide the user's data to the investigating authorities. Rather than calling BTC 'anonymous', the proper term for it would be 'pseudonymous' as the user's identity is hidden behind a string of numbers and letters but recorded on a publicly available ledger.

The problem might lie in identifying users who transact using private BTC wallets, more so with the use of tools which further shroud users in anonymity, such as the Tor browser[25], which adds a major hurdle to the tracking process. However, as a deeper analysis of the Silkroad case in Chapter 3.4.1 will show, the anonymity added to BTC transactions thanks to the utilization of the Tor browser does not make a user invulnerable to identification.

1.2 - AN OVERVIEW OF THE ADVANTAGES AND DISADVANTAGES OF BTC

Like every other means of representation of value, BTC has its own unique benefits and flaws. According to the author's point of view, the advantages outweigh the disadvantages numerically, but a few disadvantages risk damaging BTC as a currency beyond mainstream usability, especially at such an early stage in its existence.

[25] Ian Paul, 'How to use the Tor Browser to surf the web anonymously'(PC World, 23 September 2014) <http://www.pcworld.com/article/2686467/how-to-use-the-tor-browser-to-surf-the-web-anonymously.html> accessed 29 October 2014

1.2.1 - Advantages

Global access to a common currency

According to a recent study conducted by the Bill and Melinda Gates Foundation, more than 2.5 billion adults around the world do not have a bank account[26]. The reasons for such a disparity are various, and include "high cost, physical distance, and lack of proper documentation, though there are significant differences across regions and individual characteristics"[27]. Therefore, such persons have to either transact in cash, or barter, or resort to international money transfer services such as Moneygram. BTC presents a ray of light as all one requires to transact in BTC is either a computer or a mobile phone. Indeed, there are roughly six billion mobile phone subscriptions worldwide, vastly outnumbering the number of persons who own a bank account, and thus it can be conceded that BTC would provide access to the global economy for an enormous number of unbanked individuals. BTC transactions can take place via SMS wallets as well, removing the necessity of an Internet connection. A genuine example of a country in which a move to BTC would make sense is Kenya; in a 2014 study, it was discovered that there are about 8-10 million unique bank accounts in the country, with the number of mobile phone users far outweighing them at 20-21 million[28]. BTC has a global reach, without the need for exchange rates.

Transaction costs and time

Banks and other entities such as PayPal which offer an intermediary service charge a premium for their services, which is often 4-5% of the total amount of the transaction as is the case for PayPal international transfers[29]. BTC has a sound advantage in this area; the current fee for each transaction is 0.0001 BTC, which, at the time of writing, amounts to

[26] Karen Weise, 'Why Half the World Doesn't Have Bank Accounts'(*Business Week*, 25 April 2012) <http://www.businessweek.com/articles/2012-04-25/why-half-the-world-doesnt-have-bank-accounts> accessed 4 November 2014

[27] Asli Demirguc-Kunt & Leora Klapper, 'Measuring financial inclusion: the Global Findex Database, Volume 1' (*The World Bank*, 19 April 2012) <http://www-wds.worldbank.org/external/default/WDSContentServer/IW3P/IB/2012/04/19/000158349_20120419083611/Rendered/PDF/WPS6025.pdf> accessed 4 November 2014

[28] Kyla Yeoman, 'M-Pesa helps world's poorest go to the bank using mobile phones'(*The Christian Science Monitor,* 6 January 2014) <http://www.csmonitor.com/World/Making-a-difference/Change-Agent/2014/0106/M-Pesa-helps-world-s-poorest-go-to-the-bank-using-mobile-phones> accessed 4 November 2014

[29] PayPal User Agreement <https://www.paypal.com/mt/webapps/mpp/ua/useragreement-full#8> accessed 11 January 2015

€0.0227[30]. The transaction fee may vary slightly depending on the size of the transaction which it occupies on the blockchain; normally, a larger size is attributed to a larger amount of BTC being transferred. Still, a €0.02 fee per transaction on average is a very low fee when compared to the more exuberant fees charged on the more traditional money transfer services, especially when taking place on an international scale since currency conversion fees need to be factored into the equation. However, such fees may increase with potential costs such as licensing fees possibly being factored in the future.

The time for a transaction to be completed is also much quicker than that for the other services mentioned. Granted, PayPal acknowledges the transfer almost instantaneously, but it may take quite a longer period for it to be available for withdrawal as is the case in certain purchases[31]. BTC transactions appear a few seconds after having been sent by the payer, taking at most ten minutes to become confirmed on the blockchain and can then be withdrawn by the payee – quicker than the days required for bank transfers to be completed especially when the transfers concerned are international.

<u>Better security for merchants</u>

BTC transactions, apart from being faster, are also non-reversible. This can be seen as a blessing for merchants who are prone to suffering chargeback fraud, where typically the customer fraudulently claims that he/she has not received the item or has received a faulty product and asks the issuing back to order a chargeback on the payment made, if made via a credit card[32]. While certain measurements undertaken by the merchants help to prevent such fraud, it is not foolproof.

Transactions are also publicly available and hence fully transparent with no hidden costs or charges, which is a plus both for the merchants and for the customers.

[30] Based on the BTC value on the 11th of January, 2015, at €227.42 – *CoinMarketCap* <http://coinmarketcap.com/#EUR> accessed 11 January 2015

[31] "Spook-1690" [PayPal account moniker], 'How long does it take for payment to clear?' (*PayPal,* 7 November 2011) <https://www.paypal-community.com/t5/Selling-on-eBay/how-long-does-it-take-for-payment-to-clear/td-p/372826?profile.language=en-gb> accessed 11 January 2015

[32] 'Chargeback Management Guidelines for Visa Merchants'(*Visa*, 2014) <http://usa.visa.com/download/merchants/chargeback-management-guidelines-for-visa-merchants.pdf> accessed 11 January 2015

Innovation

The innovative stimulus brought about by BTC does not stop at simply bringing about a new currency, but extends far beyond that. The blockchain technology has a myriad of other potential uses, such as implementing a smart contract system where contracts are validated across the peer-to-peer network, without the need of notaries and other public officials to rubber-stamp their approval so as to apply public faith[33]. As Antonopoulos aptly put it in his book:

> *"Many human activities that previously required centralized institutions or organizations to function as authoritative or trusted points of control can now be decentralized. The invention of the blockchain and consensus system will significantly reduce the cost of organization and coordination on large scale systems, while removing opportunities for concentration of power, corruption and regulatory capture"*[34].

1.2.2 - Disadvantages

Volatility

At the time of writing, BTC lacks the stability of FCs and has been termed as "2014's worst currency" by Bloomberg[35]. It has peaked at $1,130 in late-2013, and currently stands at $236.48, or €200.75[36], signifying a huge plunge in the value and making it a poor investment proposition. However, this did not slow down the rate of adoption by merchants; on the contrary, investment in VCs has increased and the number of merchants accepting Bitcoin as a payment method includes companies such as Dell and Microsoft[37]. This is because

[33] Vitalik Buterin, 'Ethereum: A Next-Generation Generalized Smart Contract and Decentralized Application Platform'(*VButerin,* 2014) <http://vbuterin.com/ethereum.html> accessed 13 January 2015

[34] A.M. Antonopoulos, *Mastering Bitcoin* (1st, O'Reilly Media, California, U.S.A. December 2014) pg. 231

[35] Mark Gilbert, 'And 2014's Worst Currency Was...Bitcoin' (*Bloomberg*, 23 December 2014) <http://www.bloombergview.com/articles/2014-12-23/and-2014s-worst-currency-wasbitcoin> accessed 13 January 2015

[36] Based on the BTC value on the 13th January, 2015, at €200.75. Interestingly enough, just two days ago the value was around €27 higher per BTC, as can be attested by reference to footnote no. 27. <http://coinmarketcap.com/#EUR>

[37] CoinDesk, 'State of Bitcoin 2015: Ecosystem Grows Despite Price Decline'(*CoinDesk,* 7 January 2015) <http://www.coindesk.com/state-bitcoin-2015-ecosystem-grows-despite-price-decline/> accessed 13 January 2015

merchants can price their products in terms of a traditional currency and accept the equivalent amount in BTC.

Security issues

BTC entails a few security issues which may make potential users hesitant. First of all, if a user loses access to his local BTC wallet because of a forgotten password, the stored BTC are practically impossible to access, and the same applies if a user loses the hard-disk or other storage medium on which the BTC are stored. Secondly, online wallets may have better recovery options in case of lost passwords, but are vulnerable to hacking attempts[38]. These risks however are present in FCs as well; if a user loses his cash, it is irretrievable, and the same goes for a hacked online bank account.

Security issues also extend to transactions; the irreversible nature of BTC transactions, while helping merchants avoid chargeback fraud, means that customers may end up with no viable remedy should anything go wrong and would solely depend on the merchant's goodwill to put things right. This may change with regulation, but at the moment, consumers are hesitant in dealing in BTC unless transacting with a reputable company with adequate consumer protection regulations in place.

Regulation and public perception

As with most technological advances, the law may take a while to catch up. BTC is still largely unregulated in most jurisdictions, and generic laws may be outdated or inapplicable vis-à-vis BTC. This presents certain problems, such as the refusal of a bank to finance merchants if they accept BTC, or a lack of a taxation regime when one's income is mainly in BTC. The only solution to this is the creation of a new regulatory framework which should not be stifling as it would hamper BTC's growth.

Furthermore, there should be widespread education on what BTC consists of as BTC is either misunderstood or deemed to be a helping tool for criminals and nothing else[39]. Regulation

[38] Alex Hern, 'A history of Bitcoin hacks'(*The Guardian*, 18 March 2014) <http://www.theguardian.com/technology/2014/mar/18/history-of-bitcoin-hacks-alternative-currency> accessed 13 January 2015

[39] Richard Lyons, 'The Primary Legal and Regulatory Hurdles to Widespread Digital Currency Usage'(*Digital Currency Council,* 16 September 2014) <http://www.digitalcurrencycouncil.com/legal/the-primary-legal-and-regulatory-hurdles-to-widespread-digital-currency-usage/> accessed 13 January 2015

and better supervision would help ensure that the use of BTC would fare on the legitimate rather than on the illegitimate side, and it would not make much sense to ban something simply because it is being used for illicit motives; cash would have long been banned were that the case.

Bottom line

BTC is still a technology very much in its infancy, and a lot still needs to be discovered on its potential uses and downfalls. The underlying details and mathematical formulae involved are extremely complex, and what has been illustrated above only scratches upon its surface. Such complexities, coupled with the demanding features of AML legislation, present a laborious task for legislators to sew BTC into the fabric of the AML framework. The current AML framework shall be viewed in the next chapter, and step by step the author shall try and ultimately determine the best approaches to be taken in order to legislate upon BTC prudently while retaining its day-to-day usability.

CHAPTER 2 - THE CURRENT REGIME OF MONEY LAUNDERING

The current AML law in Malta is, by and large, derived from the EU Directives, which in turn are derived from the FATF Recommendations. Therefore, it is worth delving into each of the three abovementioned works in order to gain a better understanding of the current framework, so as to be able to better tackle the question forming the subject of the thesis.

2.1 – THE INTERNATIONAL ASPECT

The first international effort towards suppressing money laundering took place in 1988 with the adoption of the *United Nations Vienna Convention*[40] by the participating States, wherein the States agreed to adopt measures towards the confiscation of proceeds from illicit drug trafficking.

However, the real breakthrough was the creation of the Financial Action Task Force (FATF) established in 1989[41] after the G7 meeting in that same year. Thanks to the FATF, a standardised set of Recommendations have been created to thwart the surmounting threat of money laundering. These forty Recommendations have been adopted by States worldwide so as to have a standardised set of laws in place.

The latest amendments to the Recommendations took place in 2012, where the focus was on refining the 'risk-based approach', improving transparency regarding the ownership and control of legal persons and legal arrangements, as well as requiring more clarity on the parties to wire transfers, stressing the need for better international cooperation and operational standards, strengthening the requirements imposed on financial institutions to

[40] United Nations Vienna Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (adopted 20 December 1988, entered into force 11 November 1990)

[41] *About Us,* FATF website <http://www.fatf-gafi.org/pages/aboutus/> accessed 20 January 2015

identify politically exposed persons and the inclusion of tax crimes in the list of predicate offences[42].

Although the name "Recommendations" implies a non-obligatory nature of such rules, most States have adopted such Recommendations *en bloc* with little modifications. While such Recommendations were and are still relevant for most developed countries across the world, the same cannot be said for countries with an underdeveloped or non-existent financial sector. An example can be taken from Southern African countries such as Namibia, Swaziland, and Botswana, where it is known that "in this region [Southern Africa], most people do not have addresses, a basic problem for completing the forms necessary to establish a bank account or enter the financial system"[43]. Indeed, the problem is not pertinent to Southern Africa only but can be said to be widespread and of major international concern, as "over 70 percent of adults in the developing world (2.7 billion people) do not have access to the formal financial system"[44].

Notwithstanding this gaping loophole in the application of the FATF Recommendations, the Recommendations per se cannot be said to be ineffective when applied properly in fully-functional economies. The AML regime of the 40 Recommendations boils down to two fundamental sections: prevention and enforcement[45]. Prevention is further subdivided into four areas: customer due diligence (also referred to as 'Know your Customer', or KYC), reporting, regulation and supervision, while enforcement mainly comprises sanctions. It can be said that preventive measures, as opposed to sanctions, are largely homogenous and mostly adopted by credit and financial institutions, which can afford to implement the Anti-Money Laundering (AML) rules without suffering severe financial prejudice, which may unfortunately not be the case for smaller and/or underfinanced businesses or traders. Additionally, it is also argued that it is in the banks' own interests to implement AML rules

[42] 'Revision of the FATF recommendations, 2012', FATF <http://www.fatf-gafi.org/media/fatf/documents/Press%20handout%20FATF%20Recommendations%202012.pdf> accessed 20 January 2015

[43] Consultative Group Assisting the Poor, *Financial Access Report 2009 – Measuring Access to Financial Services Around the World* (2009) pg. 18

[44] Ibid., pg. 12

[45] E.M. Truman & P. Reuter, *Chasing Dirty Money* (1st ed., Peterson Institute, Washington 2004) pg. 46-48

since “public confidence in banks, and hence their stability, can be undermined by adverse publicity as a result of inadvertent association by banks with criminals”[46].

One particular indirect enforcement measure for countries to adhere to this international AML regime is the inclusion of non-complying States to the so-called “FATF Blacklist”, wherein States which do not meet the requirements set out in the Recommendations are listed and hence acting as a persuasive force since such listing would deter other States from cooperating in financial ventures with such listed States.

2.2 – THE EU ASPECT

For the most part, EU legislation in this regard followed the Recommendations as enacted and revised throughout the years, with timely amendments to EU Directives being made shortly after any revisions to the Recommendations as aforesaid. However, EU legislation provides a deeper regulatory insight and fleshes out the metaphorical regulatory skeleton which the Recommendations provided.

2.2.1 - First Money Laundering Directive

The first formal EU effort towards combating money laundering arrived in 1991 with the introduction of the Directive on the Prevention of the Use of the Financial System for the Purpose of Money Laundering[47] (1MLD). The Directive defined the concepts of credit institutions, financial institutions and money laundering, and particularly in the latter category departing from the definition given in the 1988 United Nations Convention abovementioned[48]. The Directive introduced the KYC obligations whereupon credit and financial institutions had to start identifying customers when opening an account, or when starting a business relationship, or in the case of any transactions for the amount of €15,000

[46] Basel Committee, *Prevention of Criminal Use of the Banking System for the Purpose of Money-Laundering* (1988) <http://www.bis.org/publ/bcbsc137.pdf> accessed 14 January 2015

[47] Council Directive (EC) 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering [1991] OJ L166/77

[48] Ibid., Article 1

or more, even when conducted in several operations[49], and to conduct proper examinations when transactions of whatever amount were suspected of being connected to money laundering[50]. Credit and financial institutions were also obliged to keep appropriate records[51] and to establish compliance procedures applicable in business relationships with clients as well as to take appropriate measures so that the employees are aware of the provisions of the Directive[52].

2.2.2 - Second Money Laundering Directive

This Directive proved to be an emancipating measure undertaken to curb the crime of money laundering in the EU, and paved the way for regulation on a worldwide scale, even though it was initially intended with respect to proceeds from drug-related crimes. The latter shortcoming was addressed in the Amending Directive (2MLD) which arrived in 2001[53], wherein criminal activity was defined as "any kind of criminal involvement in the commission of a serious crime"[54], and went on further to define "criminal activity" as comprising, *inter alia*, one or more of the following listed offences: human trafficking for sexual or labour exploitation by criminal organization, serious fraud against the EU budget, corruption and "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"[55].

These were added on to the already-listed offences relating to drug activity. The most interesting addition was the last provision which included offences that generate "substantial" proceeds and are punishable by a severe sentence of imprisonment. This widened the scope of the amended Directive considerably, but at the same time it generated a lot of debate as to what "substantial proceeds" and "severe sentence of imprisonment" meant. Another important change brought about by the 2MLD was the

[49] Ibid., Articles 3(1), 3(2)
[50] Ibid, Article 5
[51] Ibid., Article 4
[52] Ibid., Article 11
[53] Council Directive (EC) 2001/97 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering [2001] OJ L344/76
[54] Ibid., Article 1(E)
[55] Ibid.

inclusion of a wider range of subject persons, as well as rendering it applicable to auditors, external accountants, tax advisors, real estate agents, notaries, lawyers, other independent legal professionals, casinos, and dealers and auctioneers when dealing with goods whose value exceeds €15,000 and payment is made in cash[56]. The requirement for customer identification arose whenever the above-mentioned persons entered into business relationships for the first time or when dealing with transactions involving a sum of more than €15,000, whether the transaction was carried out in a single transaction or in several linked transactions[57].

2.2.3 - Third Money Laundering Directive

Several years passed until the next fundamental step towards combating money laundering arrived in 2005 with the advent of the Third Money Laundering Directive[58] (3MLD) which abrogated the two preceding Directives. Although in substance the 3MLD retained most of the principles enunciated by the previous Directives, it introduced important changes, with some of the most important ones being the implementation of stronger measures to combat terrorist financing and a novel proposition of a risk-based approach. Most of these changes were based on the FATF's revisions of the Recommendations in 2003[59] and the inclusion of an added Recommendation in 2004 in relation to cash couriers in terrorist financing[60]. The definition of money laundering was also slightly altered from the previous Directives, and read as follows:

> *"(a) 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;*

[56] Ibid., Article 2

[57] Ibid., Article 3

[58] Council Directive (EC) 2005/60 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing [2005] OJ L309/15

[59] Financial Action Task Force, *The Forty Recommendations* (20 June 2003) < http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202003.pdf> accessed 20 January 2015

[60] FATF, *IX Special Recommendations* (October 2001) <http://www.fatf-gafi.org/topics/fatfrecommendations/documents/ixspecialrecommendations.html> accessed 20 January 2015

> *(b) 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;*
>
> *(c) 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;*
>
> *(d) 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"*[61]*.*

The definition of "serious crimes" was changed in the 3MLD; besides the original list of offences, express reference was made to Terrorist Offences as enunciated in Council Framework Decision 2002/475/JHA of 13 June 2002[62]. More importantly, the so-called "general provision" relating to serious crimes was drastically altered and was made 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"*[63].

This change was much needed in order to remove the ambiguity and subjectivity which surrounded the previous definition. However, such a change did not completely solve the problem, as there still is a somewhat severe discrepancy between States which punish offences with a maximum of more than one year, and States which punish offences with a minimum of more than six months, resulting in different predicate offences being condemnable in some States but not others. This problem is further exacerbated by Article 1(3) which states that "money laundering shall be regarded as such even where the activities which generated the property to be laundered were carried out in the territory of another

[61] Council Directive 2005/60/EC, Article 1(2)
[62] Ibid., Article 3(5)(a)
[63] Ibid., Article 3(5)(f)

Member State or in that of a third country[64]", and which was already present in the preceding Directive.

This "therefore creates a situation whereby a person in one Member State may perform an act that is not a criminal offence at all there, but a bank or other financial intermediary in another Member State, which invests the proceeds for him, may commit a serious criminal offence[65]", and results in a backfire emanating from the principle of subsidiarity, preventing harmonisation rather than promoting it.

Customer Due Diligence (CDD) requirements were also altered, with particular emphasis on the application of enhanced due diligence where there is a suspicion of money laundering or terrorist financing and where there are doubts about the veracity or adequacy of previously obtained customer identification data[66], hence emphasising the risk-based approach mentioned before. Such an approach further extends to simplified due diligence as well; customers "representing a low risk of money laundering or terrorist financing"[67] need not have enhanced CDD applied in their respect.

Subject persons are now also required to conduct constant monitoring of the business relationships established as part of the CDD measures listed in Article 8 of the Directive, hence bringing in constant supervision of transactions regardless of whether they are being transacted by first-time or repeat customers or persons, and departing from the position in the previous Directive which gave paramount importance to CDD in the establishment of business relationships and substantial transactions but did not give much heed to other instances of business relationships.

Finally, Article 6 of the 3MLD includes an interesting provision which prohibits the keeping of anonymous accounts and/or passbooks by credit and financial institutions, unless the users of such accounts/passbooks are first subjected to CDD measures before using such accounts/passbooks[68]. Indeed, Austria risked becoming blacklisted by the FATF in consequence to its institutions' acceptance and running of completely anonymous passbook

[64] Ibid., Article 1(3)

[65] R.C.H. Alexander, *Insider Dealing and Money Laundering in the EU: Law and Regulation* (1st edition, Ashgate Publishing Limited, Surrey 2007) pg. 149

[66] Council Directive 2005/60/EC Articles 7(c), 7(d)

[67] Ibid., Article 11(4)

[68] Ibid., Article 6

(*sparbuch*) without any need for proof of identification by the users[69], and the inclusion of Article 6 may have been triggered by this incident.

2.2.4 - Proposal for a Fourth Money Laundering Directive

A Proposal for a Fourth Money Laundering Directive (P4MLD)[70] repealing the previous Directives has been tabled in 2013, following the 2012 amendments of the FATF Recommendations, with various welcome changes in CDD procedures and broadening the scope of the Directive, among other changes. The P4MLD extends the applicability of the Directive to providers of gambling services[71] and reduces the €15,000 threshold for dealers and traders to €7,500[72]. An exception is listed in the Directive for those who engage in low-risk transactions and satisfy the six listed criteria[73]. Additionally, tax crimes have also been included in the scope of the Directive and listed expressly as a predicate offence[74]. An emphasis on Data Protection has also been injected in order to balance the rights of persons transacting and the need to have sufficient information to curb money laundering[75].

Another major change impinges upon CDD; the P4MLD no longer incorporates outright exclusions for low-risk transactions as under the 3MLD, but requires that CDD is still carried out for such transactions, albeit a simplified form of CDD, and "sufficient monitoring of the transaction or business relationship" is required at all times[76]. Thus, the risk-based approach will become more prominent with these changes; indeed, the P4MLD also vouches for the removal of the so-called "white list" which included third countries with AML systems equivalent or superior to those present in the EU, therefore obliging subject persons to perform CDD whenever required on all cross-border transactions irrelevantly of their origin[77]. Enhanced CDD will be required by providers of gambling services when carrying out occasional transactions amounting to €2,000 or more, as well as natural or legal persons

[69] J.C. Sharman, *The Money Laundry: Regulating Criminal Finance in the Global Economy* (1st, Cornell University Press, New York 2011) pgs. 117, 119

[70] Proposal for a Council Directive (EC) 2013/0025 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing [2013]

[71] Ibid., Article 2(1)(3f)

[72] Ibid., Article 2(1)(3e)

[73] Ibid., Article 2(2)

[74] Ibid., Article 3(4)(f)

[75] Ibid., Article 38

[76] Ibid., Article 13

[77] Ibid., Article 17

trading in goods when the €7,500 threshold is surpassed. Finally the P4MLD outright prohibits credit institutions from entering into or continuing a correspondent banking relationship with a shell bank which is defined as:

> *"A credit institution, or an institution engaged in equivalent activities, incorporated in a jurisdiction in which it has no physical presence, involving meaningful mind and management, and which is unaffiliated with a regulated financial group.*[78]*"*

The author feels it necessary to point out that the fact that only cash transactions of €7,500 or more are covered, rather than all transactions irrespective of the payment method, may be exploited illicitly. Although it is true that such a provision may be due to the fact that if payment is made via bank transfer or credit card, the required CDD procedure would be carried out by the bank rather than by the trader, there still exists the risk of such a loophole being exploited especially if the card issuer is a shell bank or a bank instituted in a country with lax AML policies. Also, although the preamble of the P4MLD states that an effort has been made towards harmonising the effects and implementation of such Directive, the list of predicate offences still has the worrying divergence which existed under the 3MLD where predicate offences include offences punishable by diverging terms of deprivation of liberty depending on the Member States' domestic legislation[79], hence fuelling the problem regarding cases where an act may be considered as a predicate offence in one Member State but not in another[80].

[78] Ibid., Article 23

[79] Ibid., Article 3(4)(f)

[80] Ibid., Article 1(3)

2.3 – THE MALTESE ASPECT

The primary legislation concerning money laundering is the Prevention of Money Laundering Act (PMLA)[81], which has been enacted in 1994 and has regularly been amended over the years. The PMLA lays out the AML framework in Malta, establishing the definitions of the offence and modes of commission of the offence itself, while also setting up the FIAU. In 2008, a new set of regulations under Chapter 373 was enacted, titled "Prevention of Money Laundering and Funding of Terrorism Regulations[82]" (FTR) which aimed to incorporate the enforcement of CDD procedures, the list of subject persons, the duty to report suspicious transactions and other provisions stemming from the 3MLD.

On an international plane, apart from the implementation of the EU directives, Malta has also ratified the 1999 United Nations Convention for the Suppression of Terrorism Financing, the 1988 UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances and the 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime. The local financial institutions have also adopted renowned international reports and recommendations, which include the International Organisation of Securities Commissions' 1992 report, the Basel Committee Statement of Principles and the FATF's 40 Recommendations on Money Laundering.

2.3.1 – The Prevention of Money Laundering Act

The greater part of the PMLA reflects what has been iterated in Chapter 2.2 regarding European legislation on money laundering, and therefore for brevity's sake this part of the chapter will focus on where the local legislation diverges from the European Directives. The first and foremost important difference is the definition of a "criminal offence", as the PMLA goes a step further than the 3MLD and includes "any criminal offence"[83] within the ambit of the AML regime. Keeping in mind that the words "criminal offence" are used vis-à-vis the predicate offence, it can be argued that the Maltese legislator might have deliberately

[81] Prevention of Money Laundering Act, Chapter 373 of the Laws of Malta
[82] Prevention of Money Laundering and Funding of Terrorism Regulations, S.L. 373.01
[83] Chapter 373, Second Schedule

opted for an extremely obtuse definition in order to cater for future unforeseeable developments.

The definition of money laundering is mostly derived from the 3MLD, with one important difference: a mere suspicion that the property is derived directly or indirectly from the proceeds of criminal activity is sufficient[84], rather than outright knowledge as stipulated in the 3MLD. Another diverging definition is that of the word "property", with the Maltese version entering into much more detail than the one provided in the 3MLD. While the latter is kept at a very general level by simply defining it as "assets of every kind"[85] and then listing several non-restrictive criteria to define it, the PMLA defines property generally and then introduces a non-exhaustive list of what such property may consist of, with the first entry in the list being of special importance to the subject of the thesis as it mentions:

> *"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"*[86] [added emphasis of the author].

Although such a definition is not exhaustive and the four sub-paragraphs are inclusive rather than exclusive, it would be interesting to determine whether Bitcoin would fall within the definition of "any currency" as stipulated in the PMLA. If BTC is considered as a currency, then it would fall within the ambit of the first part of the definition, even if it is not considered as legal tender in Malta; on the other hand, if it is not considered as a virtual currency, it might be considered as a negotiable instrument and hence still regulated by the same provision. If it does not fall within either of these categories, then it would still be caught under the general definition of "property".

Perhaps the most important element present in the PMLA and absent in the 3MLD is the possibility of the conviction of the offence of money laundering without the need to prove the underlying or predicate offence[87]. Indeed, all the prosecution needs to prove is that the accused has a source of income which does not tally to his official or registered legal income;

[84] Chapter 373, Article 2

[85] Council Directive 2005/60/EC , Article 3(3)

[86] Chapter 373, Article 2

[87] Ibid., Article 2(2)(a)

subsequently, the burden of proof is shifted onto the accused who needs to prove that such monies were not the product or proceeds of a criminal offence and were legitimately obtained[88]. Therefore, the accused cannot plead the lack of conviction of an underlying offence in order to be acquitted of the offence of money laundering, and such an approach is also favourable towards the prevention of abuse of BTC in such a scenario as the owner would still need to prove the legitimate sources of funds.

A notable change brought about by an amending Act in 2015[89] was the inclusion of "property that may have derived directly or indirectly from, or constitutes the proceeds of, criminal activity" when reporting or analysing reports of suspicious transactions, which reports previously only concerned "transactions or activities suspected to involve money laundering or funding of terrorism"[90]. Although one may question the necessity of such a change, due to the fact that the definition of "money laundering" in the PMLA already includes "property that may have derived directly or indirectly from, or constitutes the proceeds of, criminal activity", there is a valid reason for such an inclusion. Property could be handled by a person who is not aware that such property is the proceeds of or has been derived, directly or indirectly, from criminal activity. Due to the way in which the law was drafted prior to the amendment, the reporting and analysis of such transactions could only be made if there was a suspicion that the said transactions could involve money laundering or the funding of terrorism; in other words, such terms denoted the necessity of *mala fede* on part of the transactor. Thanks to the amendments, transactions which possibly involve the proceeds of criminal activity as termed in the articles of the PMLA can also be reported and/or analysed, according to the situation, even though there is, as of yet, no hint of money laundering involved, or the said transaction has not yet entered the stage of money laundering.

[88] Ibid., Article 3(3) which refers to Article 22, Paragraph (1C)(b) of the Dangerous Drugs Ordinance, Chapter 101 of the Laws of Malta:
"In proceedings for an offence under paragraph (a), where the prosecution produces evidence that no reasonable explanation was given by the person charged or accused showing that such money, property or proceeds was not money, property or proceeds described in the said paragraph, the burden of showing the lawful origin of such money, property or proceeds shall lie with the person charged or accused".

[89] Act III of 2015

[90] An example of this is the amended Article 16, Sub-paragraph 1(a) of the PMLA which previously read as "..."to receive reports of transactions suspected to involve money laundering or funding of terrorism" and, after the amendment, reads as "...to receive reports of transactions or activities suspected to involve money laundering or funding of terrorism or property that may have derived directly or indirectly from, or constitutes the proceeds of, criminal activity".

The PMLA also provides for the possibility of investigating and monitoring orders, whereby the Attorney General (AG) can, upon a reasonable suspicion either order the suspect to hand over any material to the persons mentioned in the order for further investigation, or order a bank to monitor the suspect's transactions[91]. The AG can also order an attachment order to the assets of the accused[92], and may also order the freezing of the assets of the accused[93]; such freezing can also be ordered if the AG receives a request by a judicial or prosecuting authority outside Malta regarding the accused who is located in Malta and who is accused of an act or omission which would constitute an offence under Article 3 of the PMLA[94]. Such a provision is fundamental for the curbing of abuse of BTC in transnational money-laundering offences, although the freezing of digital assets may be problematic even with the recent Directive on the freezing and confiscation of the proceeds of crime within the EU[95].

In the same manner as the 3MLD provides for a Financial Intelligence Unit, the PMLA establishes the Financial Intelligence Analysis Unit (FIAU) which is be responsible for the "collection, collation, processing, analysis, and dissemination of information with a view to combating money laundering and funding of terrorism", amid other functions[96]. The supervisory powers of the FIAU have been widely broadened since the implementation of the 3MLD[97], with Act III of 2015 further widening such powers; the FIAU can now carry out on-site examinations of subject persons so as to establish compliance[98], and can override legal and contractual obligations to which the subject person is obliged when issuing directives[99] or orders such as the delaying of transactions[100]. However, much still needs to be done in order to increase the effectiveness of the FIAU to the necessary standard, as shall be discussed in Chapter 4.3.2.

[91] Chapter 373, Articles 4(1), 4B(1)

[92] Ibid., Article 4(6)

[93] Ibid., Article 5(1)

[94] Ibid., Article 10(1)

[95] European Parliament and Council Directive 2014/42/EU on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union [2014] OJ L127/39

[96] Ibid., Article 16(1).

[97] MONEYVAL, *Report on Fourth Assessment Visit – Executive Summary* (2012) <http://www.coe.int/t/dghl/monitoring/moneyval/Evaluations/round4/MLT4_MER_MONEYVAL%282012%293_en.pdf> accessed 2 February 2015

[98] Chapter 373, Article 26(2)(c)

[99] Ibid., Article 30C

[100] Ibid., Article 28(4)

2.3.2 – The Prevention of Money Laundering and Funding of Terrorism Regulations

The FTR were enacted in order to fully implement the provisions of the 3MLD which were not yet part of the PMLA, as explained in the opening section of the FTR itself[101]. Therefore it largely replicates the 3MLD, with a few exceptions, the most noteworthy one for the purpose of the thesis being the inclusion of a definition of "subject person" in the FTR, which defines it as "any legal or natural person carrying out either relevant financial business or relevant activity"[102]. This definition is restricted by the listing of various applicable relevant activities throughout the FTR. Subject persons have several AML obligations, including, *inter alia*, the imposition of CDD, the keeping of records and maintaining internal reporting procedures whenever establishing a business relationship or carrying out an occasional transaction where applicable, especially if the transaction is taking place on a non-face-to-face basis[103]. Another provision of major importance states that the FTR shall also apply where any relevant financial business or relevant activity is undertaken or performed through the Internet or other electronic means[104].

The risk-based approach is predominant in the FTR, where subject entities have to determine the risk posed by an applicant for business or persons already in a business relationship on the basis of several criteria, which include "the customer background, country of origin, business activities, products, linked accounts or activities and public or other high profile positions"[105]. Such a risk-based approach does not only pertain to subject persons but also to authorities such as the FIAU, which has to allocate its resources to the areas which present the highest risk, as it is virtually impossible to supervise and inspect each and every subject person[106]. Moreover, after the introduction of L.N. 464 of 2014, the general provision relating to applicants for business which are legal persons and which present a low risk of money laundering or funding of terrorism has been abolished[107], meaning that simplified

[101] S.L. 373.01, Regulation 1(2)
[102] Ibid., Regulation 2(1)
[103] Ibid., Regulations 4(1)(a), 4(1)(b)
[104] Ibid., Regulation 2(3)
[105] Ibid., Regulation 7(9)(b)
[106] *Report on Fourth Assessment Visit – Executive Summary*, pg. 8
[107] L.N. 464 of 2014, Regulation 8

CDD cannot be applied vis-à-vis such legal persons, hence having to go through the applicable CDD or enhanced CDD if necessary.

However, there is a glaring loophole vis-à-vis VCs which has not yet been addressed and which was mentioned in the EBA's opinion issued in 2014. VC-*fiat* exchanges and vice-versa are not specifically regulated by the EU directives or by the Maltese FTR; they only fall within the ambit of such regulations if the exchange engages in a cash transaction amounting to €15,000 or more. Most transactions are normally less than that amount, and hence are not included as relevant financial business or relevant activity as defined in the FTR. While it is true that the FTR imposes enhanced CDD in cases where there is a suspicion that the person making the transaction may be engaging in money laundering[108], it still remains something of a grey area on whether such exchanges are 'obliged entities' which are duty-bound to supervise transactions and report where necessary, hence the need for an express inclusion in the FTR.

2.3.3 – Jurisprudence

The AML provisions under Maltese law have been fleshed out by rules and regulations applicable to the banking sector. However, another source of AML law which is extremely important is local case-law, albeit the amount of cases which delve into money laundering being few and far between when compared to other more common crimes. In the case *The Police vs. Carlos Frias Mateo*[109], the Court of Magistrates (CoM) had stated that "mhux kull akkwist, mhux kull konverżjoni ta' trasferiment ta' proprjeta', mhux kull ħabi jew wiri ta' proprjeta' neċessarjament jammonta għall-money laundering, anki jekk l-akkużat ikun kriminal inkallit"[110], meaning that the judicial authorities have to tread warily whenever faced by a person accused of money laundering.

In the same case but at the appeal stage, the Court of Criminal Appeal[111] had also underlined the fact that although the crime of money laundering is theoretically described as consisting of three separate and distinct stages, in practice these are not *sine qua non*

[108] Ibid., Regulation 10(5)

[109] *Il-Pulizija vs. Carlos Frias Mateo*, Court of Magistrates(Criminal Judicature), 5 August 2011

[110] "Not every purchase, not every conversion of a transfer of property, not every concealment or exhibition of property necessarily amounts to money laundering, even if the accused is a renowned criminal".

[111] *Il-Pulizija vs. Carlos Frias Mateo*, Court of Criminal Appeal(Inferior), 19 January 2012

requirements for the offence to subsist and more often than not one of these elements is missing. It also highlighted the element of reversal of the burden of proof onto the accused to prove the licit origin of the property, as it was extremely difficult in certain instances for investigators and prosecutors to prove the origin of such property. However, the Court also stated that the prosecution has to prove, at least at a *prima facie* level, the connection between the property involved and the possibility of criminal activity connected to the accused; there is no need to prove a prior conviction as the prosecution merely needs to show that the amount of money involved **does not conform to the lifestyle of the accused**, and hence that there is no logical and plausible explanation as to the provenience of the money.

The inversion of the burden of proof onto the accused, once the *prima facie* level of proof has been presented by the prosecution, was contested as being in breach of the fundamental human rights of the accused, in the cases *Mario Camilleri et vs. The Attorney General*[112] and *Egbomon Morgan Ehi vs. The Attorney General*[113]. In both cases, the Courts in their Constitutional jurisdiction enounced that the shift in the burden of proof was merely with respect to the explanation vis-à-vis the provenance of the funds in question, and not vis-à-vis the offence of money laundering itself, which still needs to be proved beyond reasonable doubt by the prosecution. The Court, in the *Camilleri Mario* case, noted that such a reversal had been embraced by the EU and that several other EU MS had adopted the same position. Therefore, the presumption in Article 3(3) of the PMLA was deemed as "rebuttable and is not in itself unreasonable"[114], and that the shifting in the burden of proof did not breach the rights of the accused and retained the "fair balance" required in a trial.

Such reversal of the burden of proof is of fundamental importance were BTC to be used in money laundering offences. Although not as anonymous as cash, BTC transactions can still be rendered anonymous with the right tools, and hence if the prosecution is to have any conceivable chance of proving money laundering when the suspicious transactions are made in BTC, it stands to reason that it should be up to the accused to prove the legitimate source of such BTC.

[112] *Mario Camilleri & Pierre Camilleri vs. L-Avukat Ġenerali*, First Hall, Civil Court(Constitutional Jurisdiction) 15 November 2010

[113] *Egbomon Morgan Ehi vs. L-Avukat Ġenerali*, Constitutional Court, 16 March 2011

[114] *Mario Camilleri et vs. L-Avukat Ġenerali*, pg. 22

Bottom Line

With the law subject to much interpretation due to its open-ended nature, one should consult with case law in order to better understand the elements and consequences of the crime of money laundering. However, as already stated above, case-law is still scarce on the matter, and no mention of BTC has been made in the law, let alone in cases. It is for this reason that a close look shall be given at foreign law and cases on the matter, both in relation to BTC itself and also in connection to the crime of money laundering.

CHAPTER 3 - THE LEGAL STANDING OF BITCOIN ESPECIALLY WITH REGARDS TO MONEY LAUNDERING

The need for regulation vis-à-vis BTC and other VCs is increasing daily. While excessive regulation is not desirable as it stifles BTC's growth, a complete lack of regulation does not fare much better. Unfortunately, most States are still reluctant to take a stand with regards to BTC, either because of a lack of understanding of the subject, or because of apathy, or a mixture of both. In the first part of the chapter, several jurisdictions shall be examined in order to assess their stand on BTC, with particular emphasis on the money laundering aspect. In the second part, the existent BTC/VC-afflicted cases of money laundering will be examined in detail.

3.1 - THE POSITION OF BTC IN SEVERAL JURISDICTIONS

3.1.1 - Malta

Malta has not yet taken an official position vis-à-vis BTC or legislated thereupon. BTC is neither treated as a currency nor as a commodity, and is regulated by the general laws pertaining to taxation and money laundering. This free-for-all approach has attracted a few businesses originating from foreign jurisdictions which already have regulations pertaining to BTC in place, but it also acts as a double-edged sword as it could moreover attract illicit activity. The apathy present vis-à-vis BTC has led to Malta becoming ranked in the 131st position out of 177 in the list of countries most likely to adopt BTC[115].

[115] 'Malta lags behind on Bitcoin opportunities'(*Times of Malta*, 14 August 2014) <http://www.timesofmalta.com/articles/view/20140814/business-news/Malta-lags-behind-on-Bitcoin-opportunities.531822> accessed 4 February 2015

3.1.2 - Isle of Man

The Tynwald[116] has recently passed an amendment regarding VC businesses, including them in the list of businesses in the regulated sector, ergo businesses which are subject to AML requirements. The relevant article of the law[117] describes the said businesses as follows:

> *"the business of issuing, transmitting, transferring, providing safe custody or storage of, administering, managing, lending, buying, selling, exchanging or otherwise trading or intermediating convertible virtual currencies, including crypto-currencies or similar concepts where the concept is accepted by persons as a means of payment for goods or services, a unit of account, a store of value or a commodity;"*

This is quite a wide-ranging definition and does not only include VC exchanges but also wallet service providers, VC loaners and even the issuance of VCs; the author is of the opinion that the last-mentioned activity encompasses centralised VCs and not decentralised ones as no authority is responsible for the issuance in the latter. However, it omits from defining BTC or other VCs as a currency or otherwise, instead roping in different classifications so as to avoid possible legal loopholes. One may argue that it may be too soon to regulate VCs in such a wide manner, especially as the Isle of Man was on the forefront of adopting BTC in the past[118].

3.1.3 - Germany

Germany treats BTC as a financial instrument in the form of a unit of account, and has also been dubbed as a form of 'private money'[119]; it is not recognized as legal tender. However, it is subject to sales tax unless the sale is made after a period of retention exceeding a year[120]. In other words, in order not to be subject to sales tax, one should hold on to the BTCs for a

[116] Isle of Man Parliament

[117] Proceeds Of Crime (Business In The Regulated Sector) Order 2015, Article 1(mm)

[118] Robert Paul Davis, 'Isle of Man Welcomes Digital Currency Exchanges "No License Required"'(*Coindesk*, 28 March 2014) <http://www.coindesk.com/isle-man-welcomes-digital-currency-exchanges-license-required/> accessed 4 February 2015

[119] ''Private Money': Bitcoins Gain Ground in Germany'(*Spiegel Online International*, 20 August 2013) <http://www.spiegel.de/international/business/germany-declares-bitcoins-to-be-a-unit-of-account-a-917525.html> accessed 4 February 2015

[120] David Gilson, 'German government relieves capital gains tax on Bitcoin positions'(*CoinDesk*, 27 June 2013) <http://www.coindesk.com/german-government-relieves-capital-gains-tax-on-bitcoin-positions/> accessed 4 February 2015

year and then sell them. BTC service providers require a trading license from BaFin in order to operate. With regards to the money laundering aspect, it is treated under the auspices of the general AML law found in the German Criminal Code[121] and the German Banking Act[122]; with regards to the latter, the "sale and purchase of financial instruments on an own account basis for others"[123] is treated as a financial activity subject to AML regulation. Therefore, if a business sells or purchases BTC, since it is treated as a financial instrument, then it is caught under the said Banking Act and becomes a subject person thereunder.

3.1.4 - United Kingdom

The UK Parliament has also declared BTC as 'private money' and furthermore declared an exemption from VAT charges on income derived from mining, BTC exchange to/from Sterling and other currencies and other activities; however, "VAT will be due in the normal way from suppliers of any goods or services sold in exchange for Bitcoin or other similar cryptocurrency"[124]. Again, BTC is not currently treated or mentioned separately in the AML law, and worryingly enough, BTC exchanges and other service providers are not required to register under AML regulations[125], which may be seen as a glaring loophole ready to be exploited. Nevertheless, most service providers dealing in BTC do strive to comply with AML and KYC requirements out of their own volition[126].

In March 2015, the British HM Treasury (HMT) issued a response to the call for information on VCs[127]. The HMT commented positively on the underlying technology utilised by BTC,

[121] German Criminal Code, Section 261 <http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p2095> accessed 4 February 2015

[122] Banking Act of the Federal Republic of Germany (Kreditwesengesetz, KWG) <http://www.cftc.gov/ucm/groups/public/@otherif/documents/ifdocs/eurexmcobankingact.pdf> accessed 4 February 2015

[123] Ibid., Section 1, Article 2(4)

[124] HM Revenue and Customs, *Revenue and Customs Brief 9 (2014): Bitcoin and other cryptocurrencies*, 3 March 2014 <https://www.gov.uk/government/publications/revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies/revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies> accessed 6 February 2015

[125] Emily Spaven, 'HMRC: UK bitcoin exchanges don't have to register under money laundering regulations'(*CoinDesk*, 8 July 2013) <http://www.coindesk.com/hmrc-uk-bitcoin-exchanges-dont-have-to-register-under-money-laundering-regulations/> accessed 6 February 2015

[126] Eitan Jankelewitz, 'Bitcoin regulation in the UK'(*CoinDesk*, 16 February 2014) <http://www.coindesk.com/bitcoin-regulation-uk/> accessed 6 February 2015

[127] HM Treasury, *Digital currencies: response to the call for information* (2015) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf> accessed 31 March 2015

namely that of the blockchain and the public ledger[128]. Interestingly, it has also stated that the British government intended to start applying AML legislation to VC exchanges in the UK in the future, therefore addressing the shortcoming mentioned above. Moreover, the HMT stressed the importance of the investigation and confiscation regime with regard to VCs, asking for "effective skills, tools and legislation to identify and prosecute criminal activity relating to digital currencies"[129].

The HMT noted that positive attributes of VCs such as low transaction costs, faster settlement times and easy cross-border transfers of funds made them attractive to criminals as well, especially when coupled with pseudonymity. However, it added that there is "little evidence to indicate use by established money laundering specialists or that digital currencies played a role in terrorist financing", and opined that such use is mostly for low-value transactions, with "serious organised money launderers [favouring] conventional payment methods instead"[130].

The importance of the application of KYC procedures to VC exchanges was stressed upon, as well as the introduction of a new bespoke legal framework to regulate VCs in general[131]. In the author's opinion, it is still too soon to consider introducing such a specialised framework, especially since the effect of BTC and other VCs both on the economy and on AML legislation are not yet completely clear to anyone; the technology is still too fresh and has to develop further before such a consideration is made. Interestingly enough, the HMT also mentioned the possibility of regulation of VC ATMs[132]; the author is of the opinion that ideally the VC ATM operators should be regulated by other existing legislation, such as that regulating financial institutions, rather than have a specific piece of legislation for VC ATM operators per se.

In conclusion, the paper stated:

> *"The government considers that digital currencies, when used legitimately, offer an innovative, alternative payment option, which competes with existing payment*

[128] Ibid., pg. 3
[129] Ibid., pg. 4
[130] Ibid., pg. 11
[131] Ibid., pg. 12
[132] Ibid., pg. 13

> *models and has particularly clear short-term advantages for micro-payments, overseas remittances and crossborder trade"*[133].

Therefore, it is clear that the British government is considering VCs in a positive manner and acknowledges their potential use, after ascertaining that their integration in the AML framework is possible with further research.

3.1.5 - Bangladesh

Although it is far from being one of the major global economies, Bangladesh has perhaps the strictest anti-BTC regime in place, as mere usage of BTC could lead to a punishment of up to 12 years imprisonment[134]. This is due to the fact that Bangladesh has very restrictive AML laws, albeit ironically having a severely impoverished economy with a large amount of the population not owning a bank account[135]. This is the best example of how **not** to proceed in legislating vis-à-vis BTC, in the author's opinion.

3.1.6 - China

The People's Bank of China (PBOC) issued a statement in late 2013 declaring BTC as a non-currency without any legal status, and shortly thereafter prohibited financial institutions from trading in BTC as fears were high regarding the possibility of the widespread use of BTC in money laundering[136]. Subsequently, there were fears that China could outright ban the use of BTC completely as it extended the ban to payment service providers and which led to a crash in the price of BTC[137]. However, the fears were unconfirmed and to this very date, BTC trading by individuals is allowed. In fact, China might slowly reverse its initial stand as recently a Chinese PBOC official commented that there is no why as to why BTC should not

[133] Ibid., pg. 19

[134] AFP, 'Bangladesh warns of jail for Bitcoin traders'(*AsiaOne Business*, 15 September 2014) <http://business.asiaone.com/news/bangladesh-warns-jail-bitcoin-traders> accessed 7 February 2015

[135] Ibid.

[136] 'China Bans Financial Companies From Bitcoin Transactions'(*Bloomberg News*, 5 December 2013) <http://www.bloomberg.com/news/2013-12-05/china-s-pboc-bans-financial-companies-from-bitcoin-transactions.html> accessed 7 February 2015

[137] Ibid.

co-exist with FCs[138]. The general AML rules in place in China are also applicable for BTC transactions, requiring subject persons to perform KYC procedures[139].

3.1.7 - Japan

In February, 2014, BTC was the main point of discussion in the Japanese House of Councillors (known as *sangiin*)[140]. A Parliamentary Member asked, *inter alia*, about the legal status of BTC in Japan and its potential effects for usage in crime. The Japanese Government stated that BTC lacks "the backing of any government or central bank for its credit"[141], could not be considered as a currency and that it was still too early to legislate on BTC. Unfortunately, the rest of the replies provided by the Government were poorly informed, and could not provide the total number of BTC in circulation and the market cap at that time, which is publicly available information and easily accessible[142].

The Government also held that the general AML rules apply for BTC[143] and that specified business operations have to follow KYC rules for certain trades, regardless if BTC are used or not. Also, it stated that it is a crime to knowingly receive crime proceeds, whether made in yen, dollars, BTC, gold or any other means which may be qualified as 'proceeds' from a crime[144], and therefore BTC is also provided for in the general law. An interesting side-note made by the Japanese Government is that BTC would not need to be covered by forgery laws as it is impossible to forge a BTC[145].

[138] Jon Southurst, 'Chinese Official: Bitcoin Can 'Co-exist' with fiat currencies'(*CoinDesk*, 15 December 2014) <http://www.coindesk.com/chinese-official-bitcoin-can-co-exist-fiat-currencies/> accessed 7 February 2015

[139] You Yunting, 'How the Chinese Government Regulates Risk Prevention for Bitcoin Transactions'(DeBund Law Office, 2015) <http://www.debund.com/info/eee3f9062e22495c96dc12881bb0b125> accessed 7 February 2015

[140] K.F. Lenz, *Japanese Bitcoin Law* (1st edition, CreateSpace Independent Publishing Platform, Charleston 2014) pg. 22

[141] Ibid., pg. 23

[142] Namely on http://www.coinmarketcap.com

[143] The Act on Punishment of Organized Crimes and Control of Crime Proceeds (Act no. 136 of 1999) and the Act on Prevention of Transfer of Criminal Proceeds (Act no. 22 of 2007)

[144] *Japanese Bitcoin Law*, pg. 172

[145] Ibid., pg. 54

3.1.8 – United States

The initial reaction to BTC was a mixed one; the U.S. Treasury issued a warning in late 2013 warning traders and investors of the illicit uses of BTC and that non-compliance with AML rules would lead to criminal sanctioning[146], and Senator Joe Manchin called for a BTC ban as he said that the only two purposes of BTC are either to transact in illegal goods and services or to use it in speculative gambling[147]. In reply to this, Congressman Jared Polis defended BTC and held that if the U.S. were to ban BTC because of its association with money launderers, then the U.S. Dollar would have to be banned as well as it is used for the same purposes, perhaps with better effect[148]. In the same period, ongoing discussions were being held in order to determine whether BTC constituted a threat or whether it was an innovative piece of technology that could prove to be beneficial. A Senate Committee enacted after the Silk Road incident delved into great detail regarding the bigger picture of BTC; both the findings of the Committee and an overview of the Silk Road incident will be discussed in detail later on in Chapters 3.4.1 and 3.4.2.

The Internal Revenue Service (IRS) treats BTC as property for tax purposes, although such a classification has been questioned due to the nature of BTC, as it is seen being more akin to a currency than property[149], and there are conflicting views on the subject. Indeed, the Financial Crimes Enforcement Network (FinCEN) seems to be treating BTC as a currency, as it issued a letter classifying BTC exchangers and administrators as money transmitters, even if there is no transfer between the company running the exchange and the customers, as is the case when it simply provides a matching service between the sellers and buyers of VCs; the test to qualify such persons as money transmitters is an activity-based test[150]. A move

[146] Brett Wolf, 'U.S. Treasury cautions Bitcoin businesses on legal duties'(*Reuters*, 17 December 2013) <http://www.reuters.com/article/2013/12/17/us-bitcoin-letters-idUSBRE9BG1DC20131217> accessed 9 February 2015

[147] Brian Fung, 'Sen. Joe Manchin calls for a Bitcoin ban as regulators seek 'accelerated push''(*Washington Post*, 26 February 2014) <http://www.washingtonpost.com/blogs/the-switch/wp/2014/02/26/sen-joe-manchin-calls-for-a-bitcoin-ban-as-regulators-seek-accelerated-push/> accessed 9 February 2015

[148] Gregory Ferenstein, 'Congressman Calls To Ban U.S. Dollar In Response To Plea For Bitcoin Ban' (*TechCrunch*, 5 March 2014) <http://techcrunch.com/2014/03/05/congressman-calls-to-ban-u-s-dollar-in-response-to-bitcoin-ban/?utm_campaign=fb&ncid=fb> accessed 9 February 2015

[149] Daniel Cawrey, 'Could Bitcoin Become a Policy Issue for US Congress?'(*CoinDesk*, 25 October 2014) <http://www.coindesk.com/bitcoin-become-policy-issue-us-congress/> accessed 9 February 2015

[150] FinCen, *Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform*, Letter nr. FIN-2014-R011 (27 October 2014) <http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R011.pdf> accessed 9 February 2015

towards embracing BTC as a currency was further accentuated by the Californian lawmakers' decision to repeal an outdated law which prohibited companies from using any currency other than the U.S. dollar, and *in obiter* commenting that such a measure was taken so as to promote the use of BTC[151]. A Texan court also ruled BTC as falling under the definition of a currency, and declared that Bitcoin investment funds and transactions fall under the jurisdiction of the Securities Exchange Act[152].

With regards to AML provisions, the general consensus was that the Bank Secrecy Act has been deemed as sufficient to withstand any major problems which BTC might present at such an early stage[153]. BTC is moreover caught under Title 18 of the U.S. Code of Crimes and Criminal Procedure[154], wherein it is stated that financial transactions that involve proceeds of illegal or terrorist activities or that are designed to finance such activities is prohibited. KYC requirements and reporting obligations are imposed on money services businesses under the Currency and Foreign Transaction Reporting Act, and this has been made applicable to BTC exchanges and other companies which convert BTC to U.S. and vice-versa, thanks to an interpretative guidance issued by FinCEN in 2013. However, the question still stands whether such regulations apply to businesses dealing solely in BTC-to-BTC transactions.

[151] *Assembly Bill 129*, California Assembly, 23 June 2014 <http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB129&search_keywords=>

[152] *Securities and Exchange Commission v. Trenton T. Shavers and Bitcoins Savings and Trust*, United States District Court (Eastern District of Texas: Sherman Division), 23 July 2013, Case No. 4:13-CV-416 <https://www.sec.gov/litigation/complaints/2013/comp-pr2013-132.pdf>

[153] Senate Committee on Homeland Security and Governmental Affairs, *Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies* (2013) - Testimony by Jennifer Shasky Calvery, Director of Financial Crimes Enforcement Network, pg. 2

[154] Paragraphs 1956, 1957

3.2 - NEW YORK'S BITLICENSE

One of the first proposed comprehensive legislative acts on VCs has been issued by the State of New York, dubbed as the "NY BitLicense"[155]. These proposed amendments aim to regulate businesses which engage in "Virtual Currency Business Activity", namely receiving VCs for the financial purpose of transmitting such VCs, storing/holding VCs on behalf of third parties, buying and selling VCs as a customer business, exchanging VCs as a customer business and controlling, administering or issuing a VC[156], exempting persons who solely utilise VCs for the "purchase or sale of goods or services or for investment purposes"[157]. The term "Virtual Currencies" has been broadly defined as "any type of digital unit that is used as a medium of exchange or a form of digitally stored value"[158], excluding VCs that cannot be converted into *FCs*.

Amid several requirements such as capital requirements, compliance policies, and customer assets protection systems, the BitLicense provides for record-keeping procedures too. Licensees are required to, *inter alia,* keep records of each and every transaction, including information about the amount, date, time, description of the transactions as well as the names, physical addresses, account numbers of the parties to the transaction that are customers or accountholders of the licensee, and, if practicable, of the parties who are not such customers or accountholders[159]. This would ensure the transparency of the transaction as well as that of the parties to the transaction, hence removing the pseudonymity normally associated with BTC/VC transactions. The records need to be kept for a minimum period of seven years, and have to be made immediately available for access by the Financial Department upon request[160].

[155] Stan Higgins, 'New York Reveals BitLicense Framework for Bitcoin Businesses'(*CoinDesk*, 17 July 2014) <http://www.coindesk.com/new-york-reveals-bitlicense-framework-bitcoin-businesses/> accessed 12 February 2015

[156] New York State Department of Financial Services, *Proposed Amendments to Title 23, Chapter 1* (2015), Section 200.2 (q)

[157] Ibid., Section 200.3 (c(2))

[158] Ibid., Section 200.2 (p)

[159] Ibid., Section 200.12 (a)(1)

[160] Ibid., Section 200.12 (a), Section 200.13

Perhaps the most interesting part of the proposed regulations is Section 200.15, which concerns the AML program that the Licensee has to keep in place. Firstly, the Licensee has to conduct an initial and, thereafter, annual risk assessment to consider potential money laundering threats associated with its activities, customers and geographic location[161]. Secondly, internal controls, policies and procedures have to be enacted by the licensee to ensure conformity with AML regulations and training has to be provided to all of the personnel of the licensee regarding their AML obligations. Transactions exceeding $10,000 in one day by one person as well as suspicious transactions have to be immediately reported to the Financial Department[162], and every customer or account holder must be identified appropriately[163]; identification is required for every transaction of $3,000 or more. Another intriguing provision states that "each Licensee shall have in place appropriate policies and procedures to block or reject specific or impermissible transactions that violate federal or state laws, rules, or regulations"[164].

The BitLicense merits an analysis, starting from the last-mentioned provision regarding the blocking or rejection of transactions. In essence, this would mean that the transactions requested by the customers or account holders would not take place in real-time, ergo when they submit the request, but would take place when and if the licensee approves the transaction and transmits it itself. This has several implications; first of all, this would slightly negate the near-instantaneous transactions for which VCs are renowned, depending on the transaction processing time of the licensee. Secondly, this would help deter illicit or suspicious activity as transactions are screened before approval. Overall, this is a welcome provision which would greatly alleviate one of the headaches of BTC/VC transactions.

The licensing costs are, in the author's opinion, too high and would discourage entrepreneurs from adopting BTC or other VCs for their businesses, especially the smaller ones. For a technology which is still in its infancy and which would benefit from all the research and practical application that it can get at this stage, the licensing costs should be kept at a minimum. The costs have also been criticised by BTC advocates such as Circle and

[161] Ibid., Section 200.15 (b)
[162] Ibid., Section 200.15 (d)(2), (d)(3)
[163] Ibid., Section 200.15 (h)(1)
[164] Ibid., Section 200.15 (j)

Ripple Labs, and a petition has been initiated to further revise such amendments to render them more startup-friendly[165].

Finally, it is inadvisable to include the issuers/administrators of VCs and VC-to-VC exchanges within the ambit of any regulations for now. First of all, with regard to the former entities, the use of VCs in transactions would still be regulated vis-à-vis exchanges, wallet services providers and other businesses and therefore the regulation of issuers/administrators of VCs would be superfluous. With regard to both such issuers/administrators and VC-to-VC exchanges, regulation would simply serve to hamper innovation and technological developments as both regulation and compliance costs would dissuade persons from developing newer technologies or novel VC trading mechanisms. As long as the gateways between FCs and VCs are adequately protected against money laundering possibilities, one should not worry about any inherent problems which VCs by themselves might pose, especially at such an early stage where BTC adoption is still very low, let alone adoption of other VCs.

3.3 – OPINIONS AND RESEARCH PAPERS ON HOW BITCOIN MAY AFFECT THE AML REGIME

3.3.1 - FATF Paper on BTC and other Virtual Currencies

In June, 2014, FATF issued a research paper on VCs, analysing the potential risks for money laundering and funding of terrorism[166]. The document was not focused solely on BTC, and analysed past incidents concerning VCs in money laundering cases.

In the paper, the FATF declared that "decentralised systems are particularly vulnerable to anonymity risks"[167], citing the fact that there is no central authority to direct the VC and

[165] Pete Rizzo, 'Bitcoin Advocates Back Petition for BitLicense Safe Harbor Provision'(*CoinDesk*, 1 April 2015) <http://www.coindesk.com/bitcoin-petition-bitlicense-safe-harbor/> accessed 6 April 2015

[166] FATF, *Virtual Currencies: Key definitions and Potential AML/CFT risks* (June 2014) <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 15 February 2015

[167] Ibid., pg. 9

picking BTC as an example to show how a pseudonymous VC may hinder investigative authorities. However, the author does not agree with this conclusion drawn by the FATF. Suffice it to say that centralised VCs may pose a greater threat to AML policies than decentralised VCs, as the notion of a central authority in control of the distribution and administration of the currency may be subject to less transparency and external supervision, especially if the VC has been specifically created to cater for money laundering, as was the case for the Liberty Reserve Dollar which shall be discussed in Chapter 3.5.2. Furthermore, as has already been stressed over and over again, transactions are transparent and publicly available, with no possibility of ancillary problems such as the manipulation of the public ledger and administrative mismanagement, unlike centralised VCs. It is simply a question of introducing a novel way of classifying and supervising 'clean' transactions and 'dirty' transactions, coupled with the application of KYC procedures; a suggestion on how this can be done shall be presented in Chapter 4.

The FATF also listed the global reach of VCs as another threat to AML[168]. In the author's opinion, this is akin to discrediting what is possibly one of the VCs' largest advantages, ergo the possibility of a near-instantaneous global transaction with low fees, especially for micro-payments which are exorbitantly charged when using other traditional forms of payment such as PayPal. It is part of human nature to convert a beneficial object to wrongful uses, and ultimately it becomes a case of whether the beneficial side outweighs the wrongful one. Moreover, this can also be treated as a wake-up call for regulatory entities worldwide to work on an overhaul of the AML system, focusing particularly on global cooperation. The mere threat of a blacklist has not sufficiently worked, as countries with a defective economic and banking sector who adopt recognised AML policies evade the watchful eye of the FATF and yet are still rotten underneath, and ripe for abuse from money launderers. The lack of a cohesive framework of regulation should not impede BTC and other VCs from flourishing; rather, it should serve as an incentive to consider such emerging technologies more seriously.

[168] Ibid., pg. 9

3.3.2 - EBA Opinion on Virtual Currencies

Shortly after the FATF issued their opinion on VCs, the EBA (European Banking Authority) published a more detailed opinion on VCs, highlighting the individual merits and disadvantages of VCs[169]. Some of the points iterated are either superfluous to the subject of the thesis or identical to those of the FATF's, and hence will not be repeated here.

The EBA called for an inclusion of VC-*fiat* exchanges onto the list of 'obliged entities' which are subject to KYC requirements and other AML regulations[170]. The 3MLD only provides for such entities in a generic manner, requiring any business dealing in cash transactions of over €15,000 to perform the required CDD tests; exchangers more often than not deal in amounts less than that stipulated, and hence fall outside the scope of the 3MLD. This has not been amended so far in the upcoming 4MLD either. However, even if such an amendment were to be made, a problem would still potentially remain as exclusively VC-VC exchanges as was *Mintpal* would remain outside the scope of the Directives, as such exchanges do not deal in cash or FCs. In order for such exchanges to be considered for inclusion in the future, the first and foremost hurdle to be surmounted is to determine the exact status of VCs, whether they are to be treated as a legal tender or otherwise, and so on, which questions are beyond the scope of the thesis.

The EBA conceded that a complete overhaul of the existing legal framework is not necessary, as "VC schemes tend to have properties that are very similar to those provided by conventional payment service providers, as regulated and supervised by the EBA"[171]; this does not mean that the current laws are sufficient, as already demonstrated, but neither should it present an insurmountable obstacle to law-makers as long as there is a sufficient understanding of what VCs metaphorically bring to the table. The EBA also stressed the fact that VCs are not electronic money, since it does not tally to the definition provided in the Electronic Money Directive[172] and "does not have a fixed value in a FC"[173], therefore falling

[169] EBA Opinion EBA/op/2014/08 On Virtual Currencies [2014] <https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf> accessed 20 February 2015

[170] Ibid., pg. 44, para. 178

[171] Ibid., pg. 8, para. 9

[172] Article 2, Paragraph 2 of the Electronic Money Directive (2009/110/EC) defines electronic money as "electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions as defined in point 5 of Article

outside the scope of such a Directive as well. Moreover, VCs are not recognised as legal tender in any Member State.

Moving on to the risks posed by VCs in the AML area, similar risks to those cited by the FATF were presented, with anonymity and the global reach of transactions being the paramount perceived risks; these risks have already been segmented and analysed in the preceding section on the FATF's opinion. Other risks, such as the usage of VCs to hide the origins of criminal proceeds and the manipulation of market participants[174], are already risks which are inherent in traditional payment systems. One other risk which is worth mentioning is the possibility of the creation of a VC by criminals solely for money laundering and other illicit purposes, which would hence focus on desirable features such as complete anonymity; however, this is not pertinent to BTC as it is decentralised.

Overall, most of the risks iterated in the EBA opinion are either risks which are shared with those inherent in traditional payment systems or risks which can only be overcome through new regulation and international judiciary cooperation, such as the freezing and seizure of digital wallets. Other 'risks' such as the possibility of a regulatory failure in this regard[175] can certainly be avoided through information and consultation with interested parties. The EBA stressed on the importance of CDD procedures such as:

> *"the collection and verification of basic identity information; matching names against lists of known parties (such as 'politically exposed persons'); determining the customer's risk in terms of likeliness to commit money laundering, terrorist finance or identity theft; and monitoring a customer's transactions against their expected behaviour and recorded profile, as well as that of the customer's peers."*[176]

Ideally, this should also apply to VC-VC exchanges as well in order not to leave an obvious loophole in the system. The author does not agree with the EBA which discouraged credit institutions, payment institutions, and e-money institutions from buying, holding or selling

4 of Directive 2007/64/EC, and which is accepted by a natural or legal person other than the electronic money issuer"

[173] EBA/op/2014/08, pg. 11

[174] Ibid., pg. 34, paras. 121-122

[175] Ibid., pg. 36, Para. 140

[176] Ibid., pg. 40, Para. 156

VCs, as it is too much of a draconian measure, even if with the intent of 'shielding' regulated financial services from VCs[177].

The EBA concluded its Opinion by once again stating that international cooperation is a must in this area, additionally asking whether such proposed measures can sufficiently be obtained by the MS alone or whether it should be achieved at an EU level. In the author's opinion, in order to strive for true international cooperation, one should aim for homogeneity in the law, while at the same time catering for the needs of each State; therefore the best regulatory tool would be a Directive. A Regulation would be too stringent and would risk running counter to certain fundamental provisions in the laws of individual MS, while a Directive would ensure harmonisation in the important areas, such as AML issues, while leaving certain details in the hands of the MS.

3.3.3 - ECB Analysis on Virtual Currencies

The ECB (European Central Bank) had issued a preliminary analysis on BTC and other VCs in October 2012[178], wherein it treated VCs as a form of money and cautioned financial and credit institutions about their use and adoption, stating that they were completely unregulated and basically *terra incognita*. Earlier on this year, the ECB issued an updated analysis[179] due to the various developments which had taken place in the past few years, especially since several EU States have taken timid steps towards regulating BTC and other VCs.

The ECB made it a point in this recent analysis that BTC and other VCs are not, in actual fact, currencies according to the ECB's standards. Neither can they legally be regarded as such, mainly as they are not recognised as legal tender anywhere in the world and are not issued by any central bank, credit institution or e-money institution[180]. However, the ECB did concede that "within their user community, virtual currencies resemble money"[181]. This seems to imply that VCs are not regarded as money simply because they have not yet been

[177] Ibid., pg. 44, Para. 177

[178] European Central Bank, *Virtual Currency Schemes* (October 2012) <http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> accessed 21 February 2015

[179] European Central Bank, *Virtual Currency Schemes – a further analysis* (February 2015) <http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> accessed 21 February 2015

[180] Ibid., pg. 4

[181] Ibid., pg. 6

endorsed by any State and/or because their usage is still too low to merit proper recognition as such.

The ECB conceded that BTC does present a revolution in payment system methods, and has very important attributes such as the possibility of open-source development of the software, which means that new projects can be initiated if the majority of contributors agree on the proposition, as well as the fact that the network is supported by a multitude of individuals, ergo the miners, instead of a centralised single entity, offering better security and more resistance to attacks on the network[182].

Several issues were raised by the ECB and flagged as problems: these included the alleged lack of transparency in the information provided to the user on the workings of BTC and other VCs, the need for an IT background in order to transact in BTC, lack of regulation and pseudonymity[183]; however, the author humbly submits that such problems are overdramatised. There are BTC 'light' wallets which can be downloaded and installed as any other simple PC program, and which certainly do not require a profound knowledge of IT. The workings of BTC can be sufficiently and easily explained to those who are merely interested in sending and receiving money, while the current lack of regulation can be solely attributed to legislators taking an overly-wary approach vis-à-vis VCs. Finally, the alleged problem of pseudonymity can easily be countered by a proper set of regulations applying KYC and CDD to BTC businesses and service providers, as shall be seen in Chapter 4.3.3. The ECB also mentioned the problem of inter-jurisdictional laws and regulations which differ especially in the AML sphere, but this is a problem which also afflicts traditional payment system methods. In the author's opinion, the only true problems of BTC are the current volatility in price and the rate of adoption, both of which are interlinked.

The ECB finally affirmed that several changes had taken place since its first analysis, namely that some form of regulation had started taking place in EU Member States such as Germany and Sweden, as well as confirming that VCs are not money, and defined them 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"[184]. It

[182] Ibid., pgs. 19-20
[183] Ibid., pgs. 20-23
[184] Ibid., pg. 26

expressed disappointment at European legislators for not following the EBA's recommendation that VC exchanges become obliged entities in the PMLD4[185], especially since the ECB believes that "an increase in the usage of VCs is conceivable"[186]. On the whole, the ECB retained its cautious approach, but it still considers VCs to be of worthy importance, especially if they develop and move out of the early/beta stage.

3.4 - JURISPRUDENCE ON BTC VIS-À-VIS MONEY LAUNDERING PRACTICES

3.4.1 – The Silk Road Case

The first large-scale money laundering case involving BTC is the notorious Silk Road (SR) case[187], which is still *sub-judice*. The facts are briefly as follows: Ross William Ulbricht, who used the nickname "Dread Pirate Roberts" on the Silkroad website, is currently undergoing trial and is accused for running, operating and administering the said SR website which was an underground e-commerce marketplace for illicit drugs and other substances, as well as malicious hacking software, forged documents such as licenses and passports, and assassin-hiring services, among other items[188]. An interested party could only access SR through the Tor browser by inputting a specific "Onion" URL address, hence increasing the anonymity of the users accessing the website as the Tor browser hides the IP addresses of its users. SR accounts could easily be created and required no user identity verification, and registered SR members rarely divulged information about themselves.

An extra layer of anonymity was added through the use of BTC; transactions could only be done via BTC, to the extent that even the SR employees were paid in BTC[189]. Users had to deposit BTC into their SR account and then transact with the sellers; in order to exchange

[185] Ibid., pg. 29

[186] Ibid., pg. 26

[187] Sealed Complaint 13 MAG 2328, *United States of America vs. Ross William Ulbricht, aka "Dread Pirate Roberts", aka "DPR", aka "Silk Road"*, Southern District of New York Court, filed on 27 September 2013 <https://www.cs.columbia.edu/~smb/UlbrichtCriminalComplaint.pdf> accessed 24 February 2015

[188] Ibid., pg. 9, Para. 19

[189] Ibid., pg. 20, para. 28

their BTC back into FC, such BTC had to be withdrawn and exchanged via a BTC-*fiat* exchange. Albeit charging high commission rates ranging from 8 to 15%[190], SR proved to be popular with drug dealers and other criminals, as the transactions were faster and safer than if they were to be conducted via other online payment systems.

As mentioned, Ulbricht was the alleged owner and administrator of the SR website, and one of the charges was that of "money laundering conspiracy" and laundering of proceeds from criminal activity, as stipulated under Title 18 of the U.S. Code of Crimes and Criminal Procedure[191]. The criminal complaint specifically additionally stipulated that Ulbricht facilitated the laundering of the proceeds of sales through the use of BTC, which was, perhaps erroneously, described as an "anonymous form of digital currency[192]". Furthermore, privileged vendors on the SR website could only be accessed by typing in their personal address and accessing their page directly, adding yet another layer of protection.

An interesting point to note is that Ulbricht also allegedly implemented a BTC 'tumbler' to the SR payment system, which mixed the addresses of the incoming and outgoing transactions with those of dummy transactions, hence making it very difficult to trace transactions back to their respective owners[193]. It is worth elaborating on this point as first of all, it shows that the implementation of a tumbler shows a specific and unequivocal intent to facilitate the laundering of criminal proceeds as it adds a thick layer of anonymity. Secondly, the addition of a tumbler is a feature extraneous to BTC; BTC is pseudonymous in nature, while a tumbler is specifically made to be anonymous. Much as wearing a glove hides fingerprints on a physical cash note, a tumbler hides the provenance of a BTC transaction, albeit not in a total manner as a 'tumbled' transaction can be traced back to the address of origin[194]. This shows that BTC is only as anonymous as the user wants it to be, much like transactions in FCs.

[190] Ibid., pg. 14, para 21(h)
[191] Ibid., pgs. 3-4, paras. 9, 10
[192] Ibid., pg. 5, para 12(a)
[193] Ibid., pg. 5, para 12(b)
[194] It can be tracked by accumulating all the addresses in the "mixed group", including the dummy ones, and individualising the real address. It is more difficult than it sounds, but it shows that even a tumbler is not foolproof.

In fact, Christopher Tarbell[195] noted that BTC is not intrinsically illegal and has its own legitimate uses. Tarbell also explained that the SR website was acting as a BTC bank to its users, who deposited their BTC into accounts stored onto the website's servers and utilised addresses which were unique to their accounts[196]. This point begs the question – what if a bank aimed to provide legitimate services to its users? Could it reach the same level of adoption as that of the SR website? The author is of the opinion that not only is that possible, but it should be the way forward for banks in order to stay on the forefront of technology and pave the way for BTC to become mainstream. The banks would retain their function as reporters for AML purposes, and would also have additional security should there ever be financial and economic problems in the FCs sphere.

The initial evidence gathered to link Ulbricht to the "DPR" moniker shows that even though one may use an extensive range of anonymity tools and precautions, a single mistake allows investigators to track the perpetrator. In Ulbricht's case, the fatal mistake was the use of his personal *'gmail'*[197] account to register an alias named "altoid" to promote the SR website on several online forums and to recruit IT professionals for the same website. Although further evidence still needs to be presented during the course of the case, such a small mistake may well prove to be his undoing. Unless a criminal is scrupulously attentive in his methods, faring on the Internet rarely results in complete anonymity, especially since most activities on the Internet remain stored permanently in one form or another[198].

During the initial stage of the proceedings, Ulbricht admitted to creating the SR website, but "claimed he handed over control of it to someone who went by the handle Dread Pirate Roberts"[199]. However, former FBI agent Ilhwan Yum testified against Ulbricht and stated that the FBI had traced $13.4 million worth of BTC to Ulbricht's laptop in what he termed "direct,

[195] Tarbell is a special agent of the Federal Bureau of Investigation (FBI), and the criminal complaint was instituted by him

[196] Ibid., pg. 13, para. 21(d)

[197] A web-based email service by Google

[198] 'Data on the internet is permanent after 20 minutes'(*InfoSecurity*, 21 April 2011) <http://www.infosecurity-magazine.com/news/data-on-the-internet-is-permanent-after-20-minutes/> accessed 25 February 2015

[199] 'Prosecutors attempt to link Ross Ulbricht email address to Silk Road'(*Circa Media Organisation*, 30 January 2015) <http://cir.ca/news/silk-road-seized> accessed 25 February 2015

one-to-one transfers"; Yum further testified that BTC is not untraceable or anonymous by default[200], which is in line with what has been stated earlier on in this chapter.

The salient effects of the SR incident on BTC ironically proved to be good publicity and a spike in BTC adoption by new users who heard of BTC for the first time through the media. However, a worrying indirect effect is that any person interested in creating a copy of SR is now well informed of any potential pitfalls, thus increasing the necessity of BTC-specific regulations so as to further push BTC into the mainstream sphere[201].

3.4.2 - Senate Committee on the Silk Road Incident

In the wake of the Silk Road scandal, a Senate Committee hearing was held in order to evaluate the bigger picture of BTC[202], with several representatives of relevant areas ranging from BTC businesses to law enforcement officers expressing their informed views on the matter.

Jeremy Allaire - CEO of Circle

BTC advocates such as Jeremy Allaire[203] held that BTC is the way forward in electronic payments and money transfers, and presents far less of a problem in money laundering than cash systems, which are also very costly to operate[204]. Allaire called for regulation in this area as a lack thereof could lead to widespread abuse and would taint BTC's originally intended purpose of a global currency[205].

Ernie Allen - President of *The International Centre for Missing and Exploited Children*

Other more sceptical commentators such as Ernie Allen stated that BTC might prove to be a viable means of transacting for criminals due to its unbanked and unregulated nature, and quoted the FBI which said:

[200] Andy Greenberg, 'Prosecutors Trace $13.4M in Bitcoins From the Silk Road to Ulbricht's Laptop' (*Wired*, 29 January 2015) <http://www.wired.com/2015/01/prosecutors-trace-13-4-million-bitcoins-silk-road-ulbrichts-laptop/> accessed 25 February 2015

[201] Jonathan Stacke, 'Analysis of Silk Road's Historical Impact on Bitcoin' (*The Genesis Block*, 3 October 2013 <http://thegenesisblock.com/analysis-silk-roads-historical-impact-bitcoin/> accessed 25 February 2015

[202] Senate Committee on Homeland Security and Governmental Affairs, *Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies* (2013)

[203] Circle is a digital currency company that offers services in order to exchange, store, send and receive BTC.

[204] Ibid, Testimony by Jeremy Allaire, pg. 3

[205] Ibid, pg. 5

> *"Since Bitcoin does not have a centralized authority, law enforcement faces difficulties detecting suspicious activity, identifying users, and obtaining transaction records – problems that might attract malicious actors to Bitcoin. Bitcoin might also logically attract money launderers and other criminals who avoid traditional financial systems by using the internet to conduct global money transfers"*[206].

Furthermore, technologies such as the Tor Browser and coin-mixing services further helped criminals to the detriment of law enforcers.

Jerry Brito - Senior Research Fellow at the Mercatus Center of George Mason University

An interesting argument presented by Jerry Brito during the hearing of the Committee is that BTC, as a decentralised VC, can never be as useful for money launderers as a centralised VC. Brito used the VC called "Liberty Dollar" as an example, which was used in the mid-2000s to launder more than $6 billion in proceeds of several crimes which included credit card fraud, child pornography, identity theft and more, stating that it was the payment system of choice for criminals because "it was designed and managed by its creators to avoid "know your customer" and reporting rules and to evade subpoena"[207], unlike BTC where the transactions are all publicly available.

Brito continued by comparing BTC to cash. While cash can be completely anonymous, BTC is pseudonymous by nature; those seeking to cover their tracks would have to use the aforementioned tools such as Tor, and even then such methods are not completely fool-proof as mistakes occur and linking an IP address to an account on a BTC exchange is a relatively easy way to confirm a person's identity[208]. Brito concluded his analysis by advising the U.S. Senate on the dangers of overregulation, stating that such overregulation would simply push BTC towards illegality rather than destroy it[209], and criminals would still be able to buy BTC in cash even if the exchanges were to shut down, much as they were bought prior to hitting the limelight. This point was accentuated with a very accurate statement:

> *"The governmental interests in detecting and preventing money laundering and terrorist financing would be better advanced, not by prohibiting the technology, but*

[206] Ibid., Testimony by Ernie Allen, pg. 6
[207] Ibid., Testimony by Jeremy Brito, pg. 2
[208] Ibid., pg. 8
[209] Ibid., pg. 17

> *by requiring intermediaries to keep records and report suspicious activities, just as traditional financial institutions do. Again, restricting the use of Bitcoin will only ensure that criminals alone will use the technology"*[210].

Jennifer Shasky Calvery - Director of the U.S. Financial Crimes Enforcement Network

Calvery highlighted what makes BTC an attractive proposition for money launderers. The main points were relative anonymity, low transaction fees, global reach, security, irrevocability of the transactions, a lack of a central authority to report on suspicious activity and a lack of regulation worldwide[211]. The last one is merely a matter of proactivity, or at best, reaction on part of legislative authorities to implement specific laws regulating BTC; Calvery herself admitted that "virtual currency is not different from other financial products and services in this regard"[212].

The other points raised merit a short analysis. When compared to cash, such problems pale in comparison; BTC cannot rival cash in anonymity, and merely matches it in irrevocability. Although BTC transactions are relatively secure, it is a moot point as security depends on the diligence of the user rather than the protocol per se. The lack of a central reporting authority is a frivolous problem at best, as the availability of the public ledger allows anyone to report suspicious transactions and introduces an element of transparency which wrong-doers are likely to avoid. Low transaction fees and global reach are the only two elements which might attract criminals, but such advantages are outweighed by the lack of outright anonymity in BTC. Calvery also explained that BTC has yet to gain any significant traction with money launderers, as a very conservative estimate of the amount of money laundered in 2009 showed it to be *circa* $1.6 trillion in U.S. Dollars[213]; BTC's market cap as of the time of writing is a bit over $3 billion[214].

Keeping in mind the fact that the amount quoted for laundered money is in U.S. Dollars and does not include other currencies, and the fact that BTC's market cap includes legitimate

[210] Ibid., pg. 24

[211] Ibid., Testimony by Jennifer Shasky Calvery, pg. 6

[212] Ibid., pg. 6

[213] United Nations Office on Drugs and Crime, *Illicit money: how much is out there?* (2011) <http://www.unodc.org/unodc/en/frontpage/2011/October/illicit-money_-how-much-is-out-there.html> accessed 28 February 2015

[214] $3,290,329,749, accessed 28 February, 2015 <http://coinmarketcap.com/>

transactions, it is obvious that BTC presents no current significant threat in money laundering. Indeed, the author is of the opinion that the current trend of an increase in BTC adoption by marketers as highlighted earlier on together with the downshift in the market cap may indicate the possibility that money launderers are abandoning BTC as a means of laundering, leaving behind legitimate users and 'clean' transactions.

Patrick Murck, General Counsel to the Bitcoin Foundation

Murck pinpointed a very interesting view on how BTC differs from other currencies. While law enforcement investigations on current payment systems follow a "person known, transactions unknown" pattern, BTC would necessitate a "person unknown, transactions known" approach[215]. While coin-mixing services and anonymity tools can hinder investigative authorities, it is by no means impossible to track down a particular user, especially if exchanges follow KYC requirements and in turn become additional reporting authorities. Indeed, Murck said that "the block chain may be so revealing that the problem with Bitcoin is the difficulty law-abiding people have maintaining privacy"[216]. What would be truly harmful to legitimate users would be an unreasonable antipathy towards BTC, as happened in some States which issued cease-and-desist letters and subpoenas to known BTC users and businesses without valid reasons[217].

Mythili Raman, Acting Assist Attorney General in the Criminal Division of the U.S. Department of Justice

Raman reiterated the issues raised by Calvery as to what makes BTC attractive to criminals, and went on to say the following:

> *"a convertible virtual currency with appropriate anti-money laundering and know-your-customer controls, as required by U.S. law, can safeguard its system from exploitation by criminals and terrorists in the same way any other money services business could."*[218]

[215] Ibid., pg. 11
[216] Ibid., pg. 11
[217] Ibid., pg. 13
[218] Ibid., Testimony by Mythili Raman, pg. 4

Raman added that the usage of VCs in furtherance of criminal activities such as drug trafficking, child exploitation and arms running would fall under current criminal law statutes and hence no radical regulatory overhaul is required[219].

The biggest problem according to Raman is the amalgamation of a global regulatory framework to curb abuse in BTC and other VCs[220]. The classic scenario depicting such a problem would be a BTC transaction originating in a regulated jurisdiction to a non-regulated jurisdiction. In FCs transactions, this is curbed through the use of blacklists; a similar approach is recommendable for BTC transactions. Raman noted that the lack of centralised overseeing authorities can hinder the full effectiveness of such a solution; however, supervisory authorities may and are encouraged to embark on a transnational cooperation exercise to mitigate and potentially cancel the problem of the absence of a central overseeing authority[221].

Apart from commenting on the lack of a homogenous set of regulations on BTC, Raman opined:

> *"Even if the system at issue operates in a country with effective regulation and a cooperative relationship with the United States, the legal process for obtaining foreign records is relatively slow when compared to the near-instantaneous speed at which the virtual currency user can send the funds to another jurisdiction."*[222]

While acknowledging that this is a problem which requires a much greater effort in international cooperation, it is also a problem which plagues traditional payments systems. The same applies to another issue raised by Raman, which is the difficulty in the seizure and forfeiture of digital wallets owned by criminal suspects; 'dirty' physical cash often proves to be difficult to seize unless it is placed in a bank account, and likewise, BTC is only relatively easy to seize if it is placed in an exchange or online wallet. Therefore, the fact that BTC and FCs share some of the same deficiencies does not remove any of the merits which BTC has. Rather, **it should push legislators towards a solution since such deficiencies are shared across the board** and are not specific to any particular currency, whether *fiat* or virtual.

[219] Ibid., pg. 4
[220] Ibid., pg. 6
[221] Moreover, refer to the suggestion of 'Bitcoin Embassies' in Chapter 4.2
[222] Ibid., pg. 7

3.4.3 - Robert M. Faiella and Charlie Shrem Case[223]

The seizure and closing down of the SR website has laid bare the underground network of customers and service providers, with one such service provider being Robert M. Faiella who, along with renowned BTC pioneer Charlie Shrem, were recently convicted for offering exchange services for money laundering purposes[224]. Faiella operated an exchange service on the SR website, adopting the moniker "BTCKing", where customers would place an order for BTC and have it placed into their SR account against a fee. Faiella in turn used the services offered by BitInstant, a company partly owned by Shrem, in order to process the deposits paid by the customers in FC as BitInstant offered a fast fund-transfer service to BTC exchanges. Shrem, through a third-party cash processor, sent the money to Faiella's account on a third-party BTC exchange, where in turn Faiella would exchange the cash into BTC and send it to the customers' SR accounts.

BitInstant was a registered money services business and hence was obliged to comply with AML requirements. Shrem was the company's "AML Program Compliance Officer"[225] and was responsible for, *inter alia*, carrying out KYC and CDD procedures and reporting suspicious transactions by customers who would conduct frequent or large transactions in excess of $3000[226]. Shrem initially threatened to ban Faiella, but later cooperated with Faiella and even instructed him on how to evade the deposit restrictions imposed by the third-party cash processor, striking a long-term business with him and offering discounts on large orders while knowing fully well that Faiella was operating an underground BTC exchange service on the SR website [227]. The identities of Faiella's customers were never verified or looked into by Shrem, hence failing in his role as a Compliance Officer. In total, Shrem helped Faiella move over $1 million through BitInstant's system in full knowledge of Faiella's illicit intents[228]. Faiella was later identified by the investigative authorities after he

[223] Sealed Complaint, *United States of America v. Robert M. Faiella, a/k/a "BTCKing", and Charlie Shrem,* United States District Court for the Southern District of New York, Sealed Complaint filed on 24 January 2013.

[224] Jon Southurst, 'Bitcoin Trader Gets Four-Year Jail Term Over Silk Road Connection' (*CoinDesk,* 21 January 2015) <http://www.coindesk.com/charlie-shrem-co-accused-sentenced-4-years-prison/> accessed 28 February 2015

[225] Ibid., pg. 8, para. 21(b)

[226] Ibid., pg. 8, para. 21(c)

[227] Ibid., pg. 19, para. 38(a)

[228] Ibid., pg. 22, para. 46

started utilising his personal bank account for transfers by customers, after Shrem terminated his business relationship with Faiella[229].

Two main points of interest can be derived from this case. Firstly, this was a clear example of how a BTC service provider should **not** be operated, and that AML compliance is paramount to operating a legal business. Shrem actively sought to circumvent the AML requirements of his company and indeed, after the business ties with Faiella were severed, the latter was exposed to identification by the investigative authorities as he had to use a bank account opened in his own name and tied solely with him, illustrating how AML policies may prove to be efficient when exchanges between BTC and FC are involved. Secondly, Gary Alford[230] in his deposition departed slightly from the adjectives describing BTC in the SR case and did not use the word "anonymous" vis-à-vis BTC, stressing the fact that BTC has legitimate uses[231]. Once again, it has been shown that BTC is not inherently illegal and with the correct regulation and measures by service providers, it is suitable for transactions in line with AML requirements; BitInstant was in line with AML requirements and it was only via the personal misconduct of Shrem that the illicit transfer of funds was possible, and in fact Shrem was prosecuted against in his own personal capacity and not of the company's or the other directors.

3.5 - OTHER CASES WHICH CONCERNED VCS AND MONEY LAUNDERING

3.5.1 - E-Gold[232]

E-Gold (EG) was touted as a "digital currency" rather than a "virtual currency", but for all intents and purposes, it was operated in similar fashion to a centralised VC. The main difference was that EG served as a digital representation of gold and was a currency backed

[229] Ibid., pg. 23, para. 47

[230] A special agent with the Criminal Investigation department within the IRS, responsible for the main investigation vis-à-vis Shrem and Faiella.

[231] Ibid., pg. 6, para. 14(e)

[232] Sealed Indictment, *United States of America v. E-Gold Ltd, Gold & Silver Reserve, Inc., Douglas L. Jackson, Barry K. Downey, and Reid A. Jackson*, United States District Court for the District of Columbia, filed in open court on 24 April 2007

up by gold, with the price fluctuating according to the value of gold. It was classified as a "money transmitting business" and therefore necessitated the implementation of an AML program which included "the development of internal policies, procedures, and controls; the designation of a compliance officer; an ongoing employee training program; and an independent audit function to test programs"[233], requirements which were clearly not followed by the EG administration.

The only requirement to open an EG account was a valid e-mail address, with other required information such as name and surname not being subject to ulterior verifications. EG did not include any statement in its Terms and Conditions prohibiting the use of "e-gold" for criminal activity[234]. Such criminal activity included child exploitation, wire fraud and access device fraud. Moreover, EG employees never received any training and had no background in financial matters; both the defendants and the employees were aware that certain accounts were being used for illicit purposes, and no action was taken to block such accounts. On the contrary EG protected these criminals and messaged victims of fraud instructing them to "educate themselves about online fraud". On other occasions, EG imposed restrictions on certain accounts, while still allowing withdrawals from such accounts; conversely, EG sometimes requested the operators of illicit accounts to sign a waiver stating that they were not affiliates of EG and then allowed the normal operation of such accounts[235]. The defendants were found guilty of the charges against them.

In an interview subsequent to the conviction, EG owner Douglas Jackson stated that he was unaware that his website was being used for such purposes, and committed himself to recreating EG in full compliance with AML law, including measures such as proper KYC on new and existing accounts, transaction limits on existing unverified accounts, and blocking accounts originating from high-risk countries such as Nigeria and Russia[236]. Such requirements should have been in place from the start, and are requirements that are obligatory for any legitimate VC business.

[233] U.S. Code, Title 31, Chapter 53, Section 5318(h) <https://www.law.cornell.edu/uscode/text/31/5318> accessed 1 March 2015

[234] *U.S. v. E-Gold ltd et*, pg. 7, paragraph 22

[235] Ibid., pg. 11-12, paras. 32-36

[236] Kim Zetter, 'Bullion and Bandits: The Improbable Rise and Fall of E-Gold' (*Wired*,6 September 2009) <http://www.wired.com/2009/06/e-gold/all/> accessed 2 March 2015

Although EG was not, by any means, an inherently anonymous currency designed for criminals, subsequent measures undertaken by the persons administering the currency rendered it as such, proof that a centralised VC may result as a higher-risk threat than a decentralised VC openly subject to checks and supervision by any person with access to the publicly-available blockchain. Furthermore, exchanges and other VC businesses with the required KYC and CDD procedures in place would help to largely mitigate abuse while still retaining the most desirable features of VCs.

3.5.2 – Liberty Reserve[237]

While EG was not designed from the get-go as a website specifically offering money-laundering services, Liberty Reserve (LR) was created for the primary purpose of helping criminals transfer and launder proceeds from criminal activities in an anonymous manner; it was intentionally created for such a purpose[238]. Previously, the defendants had operated an EG exchange, and Arthur Budovsky had been convicted for operating an unlicensed money transmitting business. What is interesting about the LR case is the *modus operandi* of the prosecutors in ensuring that the defendants' assets were seized, since LR was a centralised virtual currency and therefore what has been applied vis-à-vis the defendants in the LR case may also be applicable to future cases involving BTC or other VCs.

The bank accounts which held FCs were targeted with a post-indictment warrant in order to be forfeited in favour of the U.S. government[239]. Moreover, the domain names of websites involved in the operation of the LR website and affiliated exchanges were targeted with a warrant of seizure as well. The latter moves into the virtual domain, and signifies an important step towards ensuring that the virtual domain is properly regulated. Indeed, the agents working on the investigation of the LR case "also executed one of the first-ever "cloud" -based search warrants, directed to a service provider used to process Liberty

[237] Sealed Indictment, *United States of America v. Liberty Reserve S.A., Arthur Budovsky a/k/a "Arthur Belanchuk" a/k/a "Eric Paltz", Vladimir Kats a/k/a "Ragnar, Ahmed Yassine Abdelghani a/k/a Alex, Allan Esteban Hidalgo Jimenez a/k/a Allan Garcia, Azzeddine El Amine, Mark Marmilev a/k/a "Marko", and Maxim Chukharev*, United States District Court for the Southern District of New York, Indictment filed in open court on 28 May 2013

[238] Ibid., Application for a Post-Indictment Warrant to restrain the defendants from controlling money in several bank accounts and to seize the domain names used by the same defendants in the operation of their illicit business

[239] Ibid., pg. 13, para. 13

Reserve's Internet traffic"[240]. This shows that the investigating authorities can and do have access to the virtual domain and that the lack of physicality present in BTC should not serve as an impediment when investigating similar crimes where BTC is involved.

The prosecutors also sought an injunction against Amazon Web Services in furtherance of their proposed seizure of the LibertyReserve.com domain name, among other domain names. This was done as a domain name is simply a 'public address' in lieu of the real IP address of the website; without such an injunction, the LR operators could still find the IP address of the LR website without the domain name and potentially withdraw funds from it[241].

LR operators added several layers of anonymity to transactions on the LR website. One such measure included the prohibition of users to add/withdraw funds to/from their LR accounts directly; instead, users had to use approved exchanges on which they could buy the LR currency using FC and then transfer it to their account on the LR website[242], and therefore the exchanges played an integral role in the operation of the LR currency. Moreover, users could hide their own LR account numbers when transferring funds against a small fee, making such a transaction virtually untraceable in a system which already did not carry out KYC and CDD checks[243].

The LR operators also actively hid information from the Costa-Rican authorities, where the business was registered, concealing suspicious transactions by creating a computer portal that appeared to give Costa-Rican regulators the ability to access Liberty Reserve transactional information and monitor it for suspicious activity. However, the data that appeared in the portal was, according to internal communications between the defendants, mostly "fake and could be manipulated to hide data that Liberty Reserve did not want regulators to see"[244]. The operators even feigned a closing-down of the website while operating the business through shell companies[245]. This sustains the point made earlier on that a centralised currency may present a greater threat than a decentralised one such as

[240] Ibid., pg. 8, para. 9
[241] Ibid., pg. 18, para. 30
[242] Ibid., pg. 15, para. 19
[243] Ibid., pg. 7, para. 15
[244] Ibid., pg. 10, para. 25
[245] Ibid., pg. 4, para. 8

BTC, since it may not be open for transparent checks and balances by the competent authorities.

Budovsky had renounced to his U.S. citizenship in order to become a Costa-Rican citizen so as not to be subject to the U.S. jurisdiction[246]. This shows that a greater effort is required in international investigative and judicial cooperation should any potential threat presented by BTC in AML issues be prevented; indeed, the LR operation involved law enforcement action from seventeen different countries[247], a textbook example of how efficient international cooperation can be. The LR case is also a clear example as to what a lack of regulation on BTC and other VCs could lead to; over an estimated period of seven years, LR processed an "estimated 55 million separate financial transactions and is believed to have laundered more than $6 billion in criminal proceeds"[248].

Bottom Line

The jurisdictions which have taken tentative steps at legislating BTC/VCs have all done so using a cautious approach, ultimately preferring to stand by and see how the technology will develop, as well as waiting for ulterior guidelines and regulations being issued by supranational entities such as the FATF and the EBA. While such an approach is prudent, it is not advisable to err on the side of caution, as criminals are invariably ahead of the legislators in this regard, as the above cases show. In the following chapter, the author shall delve and expand on several approaches which may be taken by the Maltese, and also other, legislators to curb the negative effects of BTC and other VCs, as well as certain changes which may be made to BTC for the same purpose.

[246] Ibid., pg. 6, para. 13

[247] U.S. Department of Justice, 'Manhattan U.S. Attorney Announces Charges Against Liberty Reserve, One Of World's Largest Digital Currency Companies, And Seven Of Its Principals And Employees For Allegedly Running A $6 Billion Money Laundering Scheme'(*Press Release by the U.S. Department of Justice*, 28 May 2013) <http://www.justice.gov/usao/nys/pressreleases/May13/LibertyReservePR.php?print=1> accessed 2 March 2015

[248] Ibid., Sealed Indictment, pg. 4, para. 10

CHAPTER 4 – CRITICAL OVERVIEW OF THE BITCOIN INFRASTRUCTURE VIS-À-VIS AML POLICIES AND THE CURRENT AML REGIME IN MALTA

This chapter is the fulcrum of the thesis, whereby the author utilises all of the gathered information as well as his personal knowledge on the AML framework and the BTC network to propose several solutions as to how BTC can fully integrate into the Maltese AML framework. Such propositions can also be implemented, *mutatis mutandis,* in other AML frameworks, especially in other EU jurisdictions which adhere to the EU AML Directives. In order to formulate a more informed opinion regarding AML, the author conducted surveys with several persons from different sectors of the AML framework.

4.1 - IS BITCOIN A CURRENCY UNDER MALTESE LAW?

In order to determine BTC's status in the AML regime, one should ideally first determine whether BTC classifies as a currency or not.

Definition of a currency under the CBMA

Under Maltese law, a currency is simply defined as "legal tender in the country outside Malta in which it was issued"[249]. A currency which is legal tender must be accepted as a means of payment if proffered by the debtor to the creditor, and normally a currency which is legal tender is backed by one or more States[250]. In Malta, the primary legal tender is the Euro, with other foreign currencies also accepted as legal tender under the definition given in the Central Bank of Malta Act (CBMA) as they are considered as legal tender in such other foreign countries. It is this requirement which bars BTC from becoming a true currency. As to

[249] Central Bank of Malta Act, Chapter 204 of the Laws of Malta, Article 44

[250] 'Legal Tender Guidelines' (*British Royal Mint* website) <http://www.royalmint.com/aboutus/policies-and-guidelines/legal-tender-guidelines> accessed 21 February 2015

date, no State has yet accepted BTC as legal tender, and therefore it is up to specific businesses and service providers to decide on whether to accept BTC as a means of payment or not. BTC therefore cannot be considered as a true currency under the CBMA. However, interestingly enough, BTC may qualify as a currency for AML purposes under the Maltese law.

Definition of a currency under the PMLA

The PMLA defines what "property" means in the money laundering context, albeit being an inclusive list and not an exhaustive one. The definition reads 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;*[251]

Hence, one of the definitions of property in the PMLA is "*any currency, whether or not the same is legal tender in Malta*"[252] – therefore, if one were to consider BTC as a currency which is not yet accepted as legal tender, it would fall within the auspices of a currency as defined in the PMLA. So far, there has been no Maltese judgement which has determined whether BTC can be considered as a currency or not; indeed, the only judgement which delved into the issue was the U.S. judgement ***"Securities and Exchange Commission v. Trenton T. Shavers and Bitcoins Savings and Trust***", referred to in Chapter 3.1.9, wherein it was decided that BTC

[251] Chapter 373 of the Laws of Malta, Article 2
[252] Chapter 373 of the Laws of Malta, Article 2

is a currency. However, this issue is still open to contention, with alternative considerations positioning BTC as a commodity rather than a currency[253].

If BTC were not to be considered as a currency within the ambit of the PMLA, it would fall within the generic definition of property which is:

property of every kind, nature and description, whether movable or immovable, tangible or intangible*, legal documents or instruments evidencing title to, or interest in, such property or assets*[254] [emphasis of the author]

It is however suggested that BTC should either be recognised as a currency, or at the very least included in the list aforementioned to avoid any ambiguity and potential lacunae in the law; indeed, there should be a provision dedicated to VCs and not just BTC. It would also help BTC gain legal recognition were it to be specifically included in the law, more so were it to be recognised as a currency, even if by way of a judicial decision.

4.2 - AMENDMENTS WHICH NEED TO BE MADE IN ORDER FOR BITCOIN TO FULLY INTEGRATE INTO THE CURRENT SYSTEM

Does BTC satisfy the requirements of AML policies?

In its current and raw state, BTC is not yet ready to be implemented within the legal framework in jurisdictions with a developed or developing economy, for various reasons which shall be tackled shortly. If taken in a legal vacuum, BTC can operate as a viable alternate to FCs, but existing regulations and financial ecosystems are incompatible with BTC in its current state. There are two main sets of changes which can take place: either

[253] John D. McKinnon & Ryan Tracy, 'IRS Says Bitcoin Is Property, Not Currency' (*Wall Street Journal*, 25 March 2014) <http://www.wsj.com/articles/SB10001424052702303949704579461502538024502> accessed 2 March 2015

[254] Ibid.

changes to the BTC infrastructure itself and/or changes to the regulatory framework in order to accommodate BTC.

Suggested changes to the BTC infrastructure

The greatest worry to legislators is the perceived level of anonymity which BTC users enjoy and the lack of a central authority supervising transactions and reporting suspicious activity. Banks act as intermediaries in day-to-day transactions and hence serve as excellent reporting authorities, conducting CDD procedures when there are transactions which merit investigation.

First of all, a point which has been repeated several times throughout the thesis must be made once again for clarity's sake. BTC is not an anonymous currency and every transaction conducted throughout BTC's history is publicly accessible on the transaction ledger. Since BTC is decentralised, there is no central authority which can manipulate the blockchain and misrepresent data to anyone with access to the public ledger, unless there is a 51% attack[255]. It is also conceded that the BTC network hides the true identity of the users who are transacting, as they are represented by a string of letters and numbers, ergo their BTC address. The situation is therefore one where all the transactions are known, yet the users transacting are unknown. This situation can be ameliorated in several ways.

Verified addresses

This idea is similar to the system of verified addresses utilised by PayPal[256]. Any person with a bank account can register an account with PayPal, but in order to remove the initial restrictions set on the account, the account needs to be 'verified' by PayPal, which entails verifying the identity of the person owning the account. This in turn acts both as an adequate

[255] Since the mined blocks require verification by 51% or more of the network, this would lead to the collapse of the BTC network as the controlling miners could in theory produce as many BTCs as they want and verify them themselves. This, however, would mean that BTC become worthless and therefore it is in the miners' best interest to resort to such attacks.

[256] "PayPal is the safer, easier way to pay and get paid online. The service allows anyone to pay in any way they prefer, including through credit cards, bank accounts, PayPal Smart Connect or account balances, without sharing financial information." – About Us (*PayPal)*
<https://www.paypal.com/mt/webapps/mpp/about> accessed 2 March 2015

exercise of standard CDD as well as increasing trust in the system since receiving/sending money to a verified address entails a safer transaction[257].

This verification system can likewise be applied for BTC addresses through the utilisation of the required signatures for transactions. Each and every BTC transaction has to contain a signature from the sender, whereby he/she is confirming and giving the go-ahead to transfer the specific amount of BTC to a new owner. That transaction is then 'encumbered'[258] then transferred throughout the BTC network, until it reaches the receiving address, which should have the 'unlocking' script that solves the encumbrance placed upon it by the sender and allows the BTC sent to be spent by the receiver[259].

If the transaction is originating from a verified account on an exchange/online wallet, the transaction can be signed as 'verified' which means that the BTC are being sent from a person whose identity has been verified by a third party, which, as already said, can be an exchange, online wallet service provider or even a bank. The same verification system can also be utilised for the receiver, whereby the receiving address needs to be verified in order for the encumbrance to be unlocked. The transaction may bounce back to the sender if the receiving address is not verified. Such a system would result in an economic framework which is both safer and faster than the current system based on FCs, as well as aid authorities such as FIAUs to deal with the threat of money laundering, since the public ledger adds a second layer of transparency.

In the same way as certain people prefer paying in cash or other methods such as Moneygram instead of using PayPal, users who prefer transacting in a safer environment would use service providers who utilise the above-explained system while retaining most of BTC's positive attributes such as faster transaction times and no exchange rate charges. The only caveat to such a proposition would be an increase in transaction fees, as the service providers are highly unlikely to provide such a system for free.

[257] "What does a Verified account status mean?"(*PayPal*) <https://www.paypal.com/us/webapps/helpcenter/helphub/article/?solutionId=FAQ1014&topicID=ACCOUNT_TYPES_US&m=TCI> accessed 2 March 2015

[258] Locked with an encumbrance – refer to Glossary.

[259] A.M. Antonopoulos, *Mastering Bitcoin* (1st, O'Reilly Media, California, U.S.A. December 2014) pg. 124

Colour-coded encumbrances with pre-checks (aka 'colour-coding')

This suggestion is similar to the previous one, albeit having a different mode of operation which entails a focus on the locking script. The BTC transaction is encumbered with a locking script that, apart from being only 'unlockable' by a specific address, can only be unlocked by a specific group of addresses, namely those of a specific 'colour'. The idea is to have a set of colours representing the safety of the transaction depending on the addressee. For example, a green encumbrance would mean that the transaction can only be received by someone with a green address, which would signify a high level of safety, such as when sending payment to a high-profile trader. A bank can have a blue address, and would therefore necessitate the payer to send a transaction using a blue encumbrance; the 'blue address' can be obtained via either another bank or any other pre-established service provider. The reverse can also be applied, where a merchant can decide to only accept payments sent from 'favourably-coloured' addresses.

An added benefit of such a system, apart from added safety, is to verify *a priori* the recipient of the transaction by being able to check beforehand the 'colour' of the recipient address and therefore determine the trustworthiness of the receiver. If a trader or any service provider purports to be of a certain level and a check results that it is otherwise, such trader or service provider can be reported. Such a system could help avoid fraud and protect the users of the BTC network, as well as encourage users to use legitimated systems and service providers which adhere to AML regulation.

A similar system is already being used for another VC, Nextcoin[260], which utilises a system of assets or "coloured coins" denoting the type of item or assets being purchased, such as precious metals, company shares, securities and so on[261]. Such a system can be used as a model for the suggestion provided for BTC, and tailored so as to be effective in an AML context.

[260] "Nxt is a radically enhanced cryptocurrency built from scratch, delivering a unique and decentralized financial platform. Not only does it open up new possibilities – from digital money to transfer of shares – but it addresses all of the most serious deficiencies in existing cryptocurrencies" (*Nxt* website) <http://nxt.org/> accessed 13 March 2015

[261] 'Glossary' (*NXT Wiki*) <http://wiki.nxtcrypto.org/wiki/Glossary#Asset> accessed 13 March 2015

Incorporate sender's info in the transaction's signature

Over and above the colour-coding system suggested, the details of the person initiating the transaction may be incorporated into the signature stamping the transaction, with such details being visible by the recipient of the transaction and the entities hosting the wallets of the sender and the recipient, such as banks, exchanges, and so on; the supervisory authorities should have access to such details upon request. The sender's details can be verified by the hosting entities which are required to exercise KYC procedures. This system can work in tandem with the colour-coding system, as wallets with the said incorporated details can be given a more 'favourable colour'. Moreover, it is important that such information cannot be accessed via the public ledger lest the privacy of the transactors be compromised.

Flagging system and decentralised reporting

In order to best utilise the public ledger, it is also recommendable in the author's opinion to extend the principle of decentralisation to the reporting system. Instead of relying solely on a select number of institutions to act as reporting authorities on suspicious transactions, each and every user and participant on the BTC network can flag or indicate transactions which are either suspicious or originating/destined to an address known or suspected to be used for illicit activity. This flagging system would ideally work side-by-side with the traditional reporting system whereby banks act as reporting authorities *par excellence*.

The flagging system can also be used in another manner, where users, especially consumers, can flag a trader or service provider in a positive manner, and thus increase the seller's reputation. Such a system could work conjointly with the coloured addresses system, whereby a seller would gain a more favourably coloured BTC addresses if a certain threshold of recommendations is passed. This would in effect be similar to the feedback system utilised by eBay[262], where customers can leave positive feedback to those sellers who provide a recommendable service.

[262] 'How Feedback works' (*eBay*) <http://pages.ebay.com/help/feedback/howitworks.html> accessed 13 March 2015

Large volume transactions ledger

In order to facilitate the task of supervising each and every transaction passing through the network on the public ledger, a separate public ledger can be created in order to list solely the transactions which exceed a certain pre-established limit, or transactions which can be linked even if not originating from the same BTC address but are being sent from the same IP address[263].

There already exists a so-called "BTC Richlist"[264] which provides the top 100 or top 500 "BTC holders", ergo the wallets most filled with BTC around the world. The author hereby suggests that it would be more prudent to render such a list accessible only to the established supervising authorities in order to minimise the risk of hacking or theft attempts and also to aid such supervising authorities to keep an eye on the largest wallets in circulation.

IP address tagging for large volume transactions

Together with the large volume transactions ledger, it would also be prudent to list the originating IP address of the transaction as well as the receiving IP address, so as to further help the supervision of large volume transactions and, at the very least, determine the country of origin of the BTC transaction. Transactions originating from countries with a poor AML track record would do well to be supervised scrupulously. Naturally such IP addresses would be hidden from public sight and only accessible to the supervising authorities. Transactions of over €1000 should be 'tagged' so as to better satisfy the requirements of Regulation No. 1781/2006/EC, with transactions of over €5000 or a higher established threshold either being 'tagged' differently or listed on a separate ledger.

The Blockchain site[265] which lists all the ongoing transactions in real time and which is also the *de facto* BTC public ledger at the moment simply lists the IP address which relays the transaction, not the originating and/or receiving IP addresses.

While it is true that proxies can be used to 'hide' the true IP address of the persons transacting, it would only be a small added hurdle to investigators as proxies can easily be backtracked in order to reveal the true IP addresses[266].

[263] Refer to the suggestion "IP address tagging for large volume transactions"
[264] Bitcoin Rich List <http://bitcoinrichlist.com/top100> accessed 13 March 2015
[265] BTC Blockchain <https://blockchain.info/> accessed 14 March 2015

Extra addresses against an extra payment

Currently it does not cost anything for a wallet user to utilise a new and separate address, which can be created with the click of a button. In fact, it is an officially encouraged practice to utilise a new address when sending or receiving a payment in BTC, in order to increase the difficulty of tracing a transaction back to the original senders or recipients[267]. While such a practice should not be made illegal per se, it would be commendable to charge the creation of a new BTC address, for two primary reasons. First of all, for the sake of AML, it is better that a user has a single BTC address rather than multiple ones. Secondly, added costs would result in higher rewards for the miner, incentivising more and more miners to join the BTC network and hence secure it further, especially when all BTCs are mined and the only rewards would be the transaction fees.

Remove the possibility of publicly viewing amounts in wallets

Currently, anyone with access to the Internet can input any BTC wallet address on the *blockchain*[268] website, on which the public ledger can be accessed, and view the balance of BTC in that particular wallet. In order to protect the privacy of BTC users worldwide, it would be better if developers were to render the possibility of viewing wallet balances solely possible for supervisory authorities, rather than for the public in general. Ideally, this public-viewing feature should only be made available for wallets utilised by PEPs in their public functions, for the sake of political transparency.

Designating a set of administrative entities

In order for most of the abovementioned changes to be implemented, a majority consensus of the BTC network is required; it is extremely difficult to gather the consensus of such a large number of persons over the Internet. Currently, the most prominent entity in the BTC network is the BTC Foundation, a non-profit organisation aiming to push and promote BTC awareness[269]. However, ideally there should be a BTC 'Embassy' in each and every State, which Embassies consist of members chosen by the BTC community of that particular

[266] Ibid.

[267] 'Protect your privacy' (*Bitcoin.org*) <https://bitcoin.org/en/protect-your-privacy> accessed 14 March 2015

[268] <https://blockchain.info>

[269] The Bitcoin Foundation website <http://bitcoinfoundation.org/> accessed 14 March 2015

country. In turn, these BTC Embassies would work hand in hand at overseeing and administering the BTC network by implementing such changes which would not alter the core of the BTC infrastructure but simply ameliorate it. In this way, necessary changes can be implemented more efficiently, without negatively impacting the decentralised nature of BTC as it would still not be controlled or issued by any centralised authority.

4.3 - CHANGES IN THE AML FRAMEWORK

Changes are not only necessary in the BTC infrastructure itself but also in the AML framework, with some changes being required not only to accommodate BTC and other VCs, but also to improve the said AML framework holistically. Apart from local efforts to revise and improve the framework periodically, MONEYVAL conducted several Assessment Visits in the past, with the last one taking place in 2012.

In its last Assessment Visit[270], MONEYVAL commented positively on the Maltese AML regime[271], however highlighting a few deficiencies which merited attention. Apart from the proposed changes by the author, the following are changes which require due attention as well, especially when taking into consideration BTC and other VCs.

The first and foremost issue highlighted in the Assessment was the lack of information on freezing and confiscation orders, which "raise[s] doubts as to the effectiveness of the freezing and attachment regime, and indeed the confiscation regime overall"[272]. The law only provides generically for such orders, with the finer details not listed in the local legislation, especially when de-listing and unfreezing property. Along with the need for clearer and more detailed regulations in this regard, such needed amendments should also take into consideration the freezing and confiscation of digital assets, which will require a slightly different approach than that for physical assets, as shall be discussed in Chapter 4.3.2.

[270] *MONEYVAL*, Report on Fourth Assessment Visit – Executive Summary

[271] Ibid., pg. 5

[272] Ibid., pg. 5

The Assessment also brought out the fact that the FIAU has limited direct access to law enforcement and administrative information databases[273], with such information having to be requested by the FIAU to the relevant authorities. Such indirect access to information hampers the efficiency of the FIAU, especially if the contacted authorities take days to relay the information to the FIAU. While direct access to such databases would be a welcome change from a compliance point of view, care has to be taken to protect sensitive data. MONEYVAL also suggested the implementation of analytical software in FIAU activity in addition and supplementary to the manual analysis carried out by the FIAU staff[274]. A lack of specialised investigators in the Police Anti-Money Laundering Unit was also highlighted[275], a problem which is long overdue for a solution.

Other deficiencies have since been addressed, such as the need for a National Risk Assessment (NRA) which is underway, as well as Memorandums of Understanding (MOUs) with authorities such as the MFSA in order for the latter to carry out some of the functions of the FIAU, such as on-site visits.

As previously mentioned, such changes are not the ones solely required in the author's opinion, in order to have a more efficient framework which can also work alongside VCs. The author has conducted several surveys in order to gain a better understanding of some of the strengths and shortcomings of the current AML framework.

4.3.1 – Surveys on the current AML Regime

The common questions asked to each of the mentioned persons shall be listed in a table below, with each of their respective tendered answers; the author's opinion and analysis shall follow such table, tackling each of the questions in turn. Two of the interviewees were also asked particular questions pertaining to their professions; each set of answers shall also be commented upon respectively.

[273] Ibid., pg. 8

[274] Ibid., pg. 13

[275] Ibid., pg. 18

The interviewees were the following:

- A lawyer practising in the criminal law area, whose identity shall not be disclosed, hereinafter referred to as 'Lawyer A'[276].

- A representative of the MFSA, Dr. Anton Bartolo, who is the Director of the Enforcement Unit within the MFSA, and has also been elected Chairman of MONEYVAL[277].

- A representative of the FIAU, Mr. Antonio Ghirlando, who is the Legal and Compliance Manager within the FIAU[278] [279].

Common questions asked to each of the interviewees

1. Is the current Anti-Money Laundering (AML) framework adequate? If not, why? (In particular mention whether the current framework adequately covers small companies/traders such as car dealers)
2. Is the enforcement of the AML framework taking place as per the intentions of the legislators?
3. In your opinion, what is/are the best means for money laundering, i.e. which type of businesses are most susceptible to usage by criminals as a façade for money laundering?
4. Please comment on the following statement: "Cash is the most anonymous payment method in money laundering"
5. In your opinion, which are the best supervisory authorities and reporting entities for AML?

[276] Interview conducted on 4 December 2014
[277] Interview conducted on 20 March 2015
[278] Interview conducted on 24 March 2015
[279] Disclaimer: The views and answers tendered by Dr. Bartolo and Mr. Ghirlando in the interviews are not representative of the views or positions adopted by the MFSA and the FIAU respectively, and should simply be construed as personal opinions.

Table 1:

	Lawyer A	**Dr. Bartolo**	**Mr. Ghirlando**
1.	*The current framework is technically and theoretically adequate, in that subject persons are required to identify their clients/customers and the range of subject persons is always on the increase. Also, black-listing countries or persons is a good disincentive since blacklisting would heavily damage that person's reputation and handicap his or her trade. In practice, the AML framework might be more difficult to implement, especially when it comes to persons such as car dealers, and that is precisely where the problem lies as it is very difficult to monitor such smaller players on a regular basis; surprise visits are not enough.*	*The current AML framework is more than adequate; however, it is not perfect. Following the FATF revision of the Recommendations in 2012, as well as the P4ML, our framework needs to be perfected.* *Regarding small companies and traders: the generic threshold of €15,000 for a single large transaction covers and binds them as well. Before, the law used to talk about auctioneers and gold dealers, now it deals with a much wider spectrum of persons. In theory, whenever, for example, furniture dealers, car dealers and so on receive payment in cash, they are supposed to carry out CDD.*	*The FATF recommendations are an adequate framework that should ideally be implemented internationally – in fact, the EU AML directives emerge from the FATF recommendations. The framework itself is not faulty, but the implementation of such a framework may be. In regulated areas and institutions such as financial institutions, the implementation of the framework is relatively hassle-free as they are already regulated by the MFSA for instance. Secondly, they have also been set up and regulated for a far longer period of time and therefore already have the necessary know-how.*
2.	*Yes, as the financial industry, including credit institutions, is operating positively and applying the framework as intended by the legislators. An interesting concept adopted by one of our local banks is the inclusion of a "whitelist" of practitioners, rather than simply having a blacklist. This requires more KYC on their part, but it saves having to conduct extensive KYC on more*	*Mostly it is. The problem however lies in enforcing the AML framework with respect to each and every subject person out there. In order to partly remedy this, it is being contemplated that there may be a situation where payments in cash over a certain threshold can be made illegal.*	*As already said, credit and financial institutions present few problems when enforcing the framework in their regard. However, when it comes to unregulated professions such as real estate agents and car dealers, the situation becomes trickier. For one thing, it is difficult to identify each and every one of such persons or traders. Secondly, even though technically speaking they would*

	transactions. However, some clients, especially foreign ones, have complained that the requirements are too stringent and might stifle economic growth. Surprisingly enough, the weakest link in the AML framework is the FIAU. Since they are understaffed, they are often behind the loop in certain procedures such as extensive KYC on foreign customers, and more often than not, only close in on the procedure when it's either too late or their input is not required any more.		*be caught under the Act were they to transact in cash in amounts exceeding €15,000, in practice it is very difficult to ensure whether such persons are adhering to their obligations under the Act.*
3.	*From my own personal experience as a practitioner, money laundering takes place at food and catering establishments such as supermarkets, bars, restaurants, butcher shops, etc., for the simple reason that in such establishments one can launder money in big volumes using cash. The price of food is not set and huge profit margins leave a lot of space for laundered money to be included. Auctioneers, brokerage firms, estate agents, and commission-based profit firms are used as well since the commission percentage can be freely changed to suit one's own purpose.*	*Cash based businesses lend themselves to money laundering very well – it is easy to hide illegitimate cash in legitimate cash. However, money laundering is not reserved solely to cash – one can even launder funds by transfers through banking channels. If you originally receive money, even by wire transfer, which was paid to you in consideration for something illegitimate, once there is the bank's rubber stamp, it makes it an even more formidable means than cash in certain instances, as long as it is masked as a legitimate transaction. Every business wherein you can transact in large amounts, whether cash or not, can be abused for money laundering purposes; that being said, money laundering is primarily cash-based.*	*Large cash-based companies and businesses are mostly susceptible to money laundering, as in Malta the use of cash is abnormally high. However, there is also an increasing use of shell companies for such purposes, which are solely created for use in money laundering.*

4.	*Without a doubt, cash is the most anonymous means.*	*Yes, I agree that cash is most the most anonymous means, as it is untraceable.*	*Yes, I agree that it is the most anonymous means. Along with pure cash, there are also cash-type instruments such as negotiable instruments and bearer instruments which deserve mention. These include alternative remittance systems such as Hawala and Hundi.*
5.	*The banks are the best reporting authorities for AML, as most transactions have to go through the banks at some point or another. The FIAU needs to step up its game in order to become a better supervisory authority.*	*The category of subject persons which tenders the most reports are banks, according to the annual report of the FIAU. This is due for several reasons: they deal with the most persons, handle the most money, and out of all subject persons, they are the most aware and well-prepared to do their duties according to the AML rules.*	*With more pressure in compliance, the STRs overall have increased. Circa half the STRs are from banks, because they are the main gatekeepers. Financial institutions and investment services companies should ideally increase their submissions of STRs. Moreover, I firmly believe that iGaming companies will become a major player, i.e. a prolific subject person when it comes to STRs, as there is a heavy use of prepaid cards in their transactions, to which simplified CDD applies.* *The FIAU is the body responsible for compliance; however, the law also makes provision for the FIAU to use agents. There is an MOU with the MFSA regarding this for instance, as well as agreements with other supervising*

			authorities.

The author's analysis and opinion

Questions 1 and 2: All of the three interviewees agreed that the current AML framework is adequate, at least in theory. Dr. Bartolo mentioned that the proposed changes in the P4MLD still need to be implemented in order for the framework to be up to date. However, all three interviewees mentioned the fact that the enforcement of the AML framework per se presents problems, particularly with regards to small-time traders or companies. Mr. Ghirlando stated that while credit and financial institutions are aware of their obligations and are normally well-equipped to implement the AML regulations, other persons are not so equipped; all three interviewees agreed that it is very difficult, in practice, to supervise and check upon each and every subject person.

Dr. Bartolo also presented a possible solution by suggesting that rather than requiring subject persons to perform the required checks on cash transactions of over €15,000, such transactions are outright prohibited. However, again, the problem lies in enforcing such a measure. The public ledger system utilised by BTC would help the supervision of such subject persons.

Lawyer A lauded the blacklisting system, and also commended the whitelisting system adopted by one of the local banks. The author agrees with Lawyer A's statements, in that the whitelisting system would help alleviate perfunctory checks on subject persons which present no real threat of money laundering. Such a system would work well were the colour-coding suggestion to be implemented, and it would be more efficient to have a 'multi-colour' system rather than simply having a blacklist and a whitelist.

Interestingly, Lawyer A mentioned that the "weakest link" in the AML framework is the FIAU, due to its being understaffed and under-resourced. Mr. Ghirlando also stated that the FIAU does not have enough resources. Such problem is partly alleviated by the use of the risk-based approach; however, a better allocation of resources to the FIAU should be considered by the Maltese government, especially with the advent of BTC and other VCs.

Question 3: All three interviewees agreed that cash-based businesses are the most susceptible to use for money laundering purposes; Lawyer A specifically mentioned food and catering establishments, such as supermarkets, due to the large volume of trading and the equivocal pricing of items. Such businesses are difficult to monitor as they mostly engage in micro-transactions; since BTC is ideal for use in micro-transactions, it would be a better means than cash in order to at least reduce abuse in this regard.

Mr. Ghirlando mentioned shell companies, a problem which can only be solved by more thorough requirements for the establishment of a company. Dr. Bartolo made a very interesting point concerning the use of banking systems for money laundering; such a problem would also be present in BTC systems as any transaction can be masked as a legitimate one. Thorough checks on the provenance of funds are possible, but such checks cannot be applied for each and every subject person, for practical reasons.

Question 4: All three interviewees agreed that cash is the most anonymous form of payment; Mr. Ghirlando agreed on this, being fully aware of what BTC is. He also mentioned cash-type instruments which are used in countries such as India, Middle-Eastern and North-African countries. It is important to point out, *in obiter,* that this is precisely the reason why a completely homogenous AML framework will not work, as each and every country has its own economic ecosystem, traditions and different requirements.

With cash being in wide use, even with the increasing use of payment methods such as credit cards and wire transfers, BTC would certainly not present a greater threat than cash, and if utilised correctly, would serve as a more transparent payment method than either of the aforementioned.

Question 5: Banks were generally agreed upon as being the best reporting entities; it stands to reason that in order to ensure the most efficient oversight of BTC transactions, banks should accept customer accounts in BTC. Mr. Ghirlando also mentioned that iGaming companies will also become important subject persons; with such companies having IT influences, it is entirely possible that BTC would be considered by them as one of the accepted payment methods, and therefore it would be prudent to include such companies as subject persons, and moreover, regulate BTC appropriately.

MOUs between the FIAU and supervisory authorities such as the MFSA also help in alleviating some of the workload on the FIAU, and delegating some of the functions of the FIAU, such as on-site checks, would help ensure a more widespread compliance on part of the subject persons. Additionally, in the author's opinion, it would also be prudent to work with private businesses in this regard, both to collect more information from them apart from the annual compliance reports, as well as perhaps delegate more functions to trusted and established subject persons, which again would help spread compliance and awareness in the AML area. However, as Lawyer A correctly stated, it is the FIAU which should be first and foremost improved and emancipated, both by a bigger allocation of resources as well as the allocation of more powers, as will be mentioned in Chapter 4.3.2.

Questions particular to Dr. Bartolo and Mr. Ghirlando

Dr. Bartolo

Table 2:

Questions	**Answers**
1. The generic threshold for a large volume transaction currently stands at 15,000 euro, which will be reduced to 7,500 euro with the adoption of the Fourth AML Directive. Should the limit be further lowered below 7,500 euro or is it adequate?	*The €7,500 euro threshold for a SLT is adequate.* *[When asked whether a €5,000 threshold is acceptable] €5,000 is also viable, but definitely not thresholds of €1,000/€1,500. If you lower the limit you are lowering the targeted quality of money laundering happening; one needs to control money laundering on a large scale, the metaphorical "big fish", rather than small ones.*
2. Which problems are encountered when liaising with foreign supervisory authorities, both EU and non-EU based?	*As the MFSA is a supervisory authority, liaising is mainly done with foreign supervisory authorities, not other FIUs, such as the Financial Conduct Authority in the UK and BaFin in Germany. The relationships with such supervisory authorities are normally regulated by multilateral MOUs (memorandums of understanding), which are of an*

	international nature, obliging the concerned supervisory authorities to assist each other and exchange information. The biggest problem is the tardiness of answers, which may be due to either legal reasons or practical ones. Sometimes, the law of a country does not permit the supervisory authority to provide information, notwithstanding the MOU and the law of the country with whom you are dealing. If cooperation cannot happen due to legal reasons, it can be amended by the law – but practical reasons have to persist unless practical solutions are found.

Author’s comments

Dr. Bartolo correctly commented on the fact that if one were to lower the transaction limit too much, it would do more harm than good, due to the type of money laundering targeted at those levels. Moreover, it would heavily increase the workload both on the reporting entities as well as the supervisory authorities. The author believes that the limit should be lowered to €5,000, and an even lower limit should be imposed on BTC transactions whose source cannot be verified, as shall be explained in Chapter 4.3.3.

Furthermore, Dr. Bartolo hinted at the problems, which are of a bureaucratic nature, that the FIAU faces when liaising with foreign supervisory authorities, namely the turnaround time for communications. Such a problem should have prominence on the agenda of national and regional law-makers, as in order to be well-prepared for BTC/VCs, there should at the very least be implemented a more rigid regional framework concerning communication and liaising between supervisory authorities on a transnational scale, due to the global nature of BTC/VC transactions. Ideally, such framework should be international rather than regional.

Mr. Ghirlando

Table 3:

Questions	**Answers**
1. Which is the most salient problem faced by the FIU when combating money laundering?	*The biggest problem is the lack of resources. In order to counter this, risk-based supervision is being implemented, which entails the filing of annual compliance reports by the subject entities and subsequently identify which entities are most prone to risk for money laundering. More pressure on agents is being placed by the FIAU in order to check that compliance is being adhered to by subject entities on behalf of the FIAU. There is also an increasing emphasis on training, after a close look was taken in the national risk assessment at the operations of subject persons. Such training is important as it is further passed down the pipeline and hence mitigates some of the problems with which the FIAU is faced when ensuring compliance.*
2. Would the advent of Bitcoin hinder/disrupt the FIU in its operation or would it aid them since the public ledger shows all of the transactions taking place?	*Solely having access to the public ledger is not going to be of great assistance if you have anonymous accounts. Currently, one of the biggest selling points of BTC is that it is unregulated. One needs to see how it's going to develop before changing any laws specific to VCs (Virtual Currencies), as their development may be hindered. If anything, one should regulate the exchangers for now; the idea is to protect the FCs and monitor the gateways to VCs from FCs and vice-versa, leaving the VCs in themselves unregulated for now.* *[Asked if KYC together with the public ledger would work well together] An exchanger can help force a person to divulge personal information, but it would still ultimately be up to the customer himself to*

	justify the source of funds and other relative findings. The current BTC system cannot work, as there has to be some kind of traceability, and certain features such as being able to publicly access the balance in a particular wallet is not desirable. Moreover, one should be careful not to overregulate as it would lead to inefficiency and even perhaps kill off VCs. I believe that the technology behind BTC is great and may be used in the future.
3. Have there been any local incidents regarding the use of Bitcoin for money laundering?	*There have been no local incidents.*
4. If Bitcoin service providers such as exchanges were to follow KYC and CDD procedures, would Bitcoin be in line with the AML framework or would ulterior changes in the AML Framework be required?	*It would be a step forward but even so, eventually the framework would have to be changed nonetheless. Before deciding on how the framework has to change and adapt, it would be prudent to wait and see what is going to happen to BTC.*

Author's comments

Mr. Ghirlando also referred to the problem of lack of resources afflicting the FIAU. He also made reference to the National Risk Assessment, wherein the FIAU is currently undergoing a self-critical exercise in order to address several issues.

When asked about BTC, Mr. Ghirlando positively lauded the technology underlying BTC, and firmly believes that such technology will be useful. However, he does not believe that BTC in its current state can work well with the existing legislation and systems. The author does not fully understand Mr. Ghirlando's scepticism on the viability of KYC coupled with BTC's public ledger, which scepticism was evident when Mr. Ghirlando said that ultimately it would be up to the customer to justify the source of his/her funds. This is an issue which also afflicts FCs and therefore, in the author's opinion, such an argument does not hold water. Rather, the public ledger would help instil the element of transparency which is still largely missing when dealing in FCs, especially when the functions of PEPs are put into the equation. The author agrees with Mr. Ghirlando that the fact that a wallet's funds are publicly available for viewing is a feature which should be done away with for data protection purposes; such feature should solely be made available to the supervisory authorities.

It is interesting that there have been no local incidents regarding BTC to date; this may be due to two main reasons. Firstly, BTC is still relatively unknown in Malta, and secondly, the author firmly believes that local authorities are not yet well equipped to deal with possible money laundering instances wherein BTC is used. Finally, the author fully agrees with Mr. Ghirlando in that it would be prudent to wait and see how BTC is going to develop before enacting a brand new bespoke legal framework.

4.3.2 - Possible Amendments to the Prevention of Money Laundering Act

The main Maltese legislative act on AML is the PMLA, as aforementioned in Chapter 2. The PMLA has been amended regularly over the years, particularly after the issuance of a new set of Recommendations or a new EU directive. However, the PMLA still does not mention anything about BTC and other VCs, restricting itself to mentioning electronic money only, which, as already explained, is merely a digital representation of FCs and therefore completely separate from VCs. In this section, the PMLA shall be dissected and analysed, with the shortcomings which require a change being highlighted, as well as suggestions for new sections where and if necessary.

The exclusive reference to banks

As evidenced by the results of the surveys, banks are considered to be the best reporting authorities in AML. However, this does not render them the sole reporting authorities, especially with the advent of BTC, since exchanges can likewise play an important role in monitoring and reporting suspicious transactions. The issue here is not whether exchanges and other BTC service providers should be subject persons, as that will be replied in the affirmative shortly – rather, the issue is that the powers afforded to banks by the PMLA should be extended to other entities in order to increase the efficiency needed to improve the AML framework.

There are two options available –

1. Include another term instead of "banks", which term has to be more generic and allows for more institutions to be embraced within the term. The terms "credit institutions" and "financial institutions" may be used, with the latter hence including exchanges.

2. Include other institutions in articles where the word "bank" is included in the PMLA, naturally if and where necessary so as not to mar the meaning of that particular provision.

In the author's opinion, the best option would be the second one, albeit being more cumbersome than the other option; it allows for more flexibility and the pinpointing of specific institutions for that particular provision of the PMLA. It would require more frequent amendments but it should provide the highest degree of accuracy.

An adequate example of such implementation would be in monitoring orders, whereby the AG may apply to the Criminal Court so as to have it order a bank "to monitor for a specified period the transactions or banking operations being carried out through one or more accounts in the name of the suspect"[280]. In order to extend the efficiency of the monitoring order, banks should not be the only institutions which may be availed of. Users may store large amounts of BTC on exchanges as evidenced by the Mt. Gox exchange incident[281], as well as with wallet service providers, and therefore banks, were they to accept storing accounts in BTC, would not be the sole venue for such transactions. Therefore, monitoring orders should be extended to other entities such as exchanges, wallet service providers and other service providers which tend to store an appreciable amount of BTC belonging to their customers.

[280] Chapter 373 of the Laws of Malta, Article 4B(1)

[281] Robert McMillan, 'The Inside Story Of Mt. Gox, Bitcoin's $460 Million Disaster'(*Wired*, 3 March 2014) <http://www.wired.com/2014/03/bitcoin-exchange/> accessed 28 March 2015

Forfeiture of assets

One of the biggest headaches when enforcing a judgement is the forfeiture of the convicted person's assets which may include the proceeds of the offence committed. It is the Court Registrar's duty "to conduct inquiries to trace and ascertain the whereabouts of any moneys or other property, due or pertaining to or under the control of the person charged or accused or convicted, as the case may be"[282]. If the property of the person convicted consists of BTC as well, then the matter becomes even more complicated as it is a virtual asset and not a physical one.

Article 3(5) of the PMLA, which talks about the forfeiture of the proceeds of an offence, makes reference to the main articles of the Criminal Code regarding such forfeiture[283]. The modes of forfeiture heavily depend on the type of property involved, as, for example, a house cannot be forfeited in the same way that a car can. With regards to BTC, it is important firstly to draw a distinction between wallets stored on an exchange, online wallet service or any other type of third-party hosted accounts, and a personal wallet. Forfeiture in the case of BTCs stored in the former type of accounts may tend to be easier than the latter, as the third party account host would be able to retrieve the BTCs and transfer them to a wallet/s held by the Maltese Government; the situation may still be a bit prickly if such third party account hosts are situated in a foreign jurisdiction, especially if such foreign jurisdiction has a lax judicial system.

The true problem however lies in the case of personal wallets owned by the convicted person. Before elaborating further on the matter, it is worth explaining how data in a BTC wallet is saved and stored onto a PC or other computing device. The data contained in the wallet, namely the private keys to access your BTC, is stored in a DATA file which is named "*wallet.dat*" by default[284]. When a backup of a wallet is made, it is solely this file which is saved and stored; therefore, if one needs to store a copy of his BTC wallet on, say, a USB flash drive, then all one needs to do is copy the *wallet.dat* file onto the USB flash drive. This means that a plethora of backups can be made relatively quickly and easily, and the mentioned file can even be stored online in cloud-based storage. All a person needs to

[282] Ibid., Article 11A(1)

[283] Criminal Code, Chapter 9 of the Laws of Malta, Articles 23-23D

[284] Personal knowledge of the author after having conducted several transactions and transferred several wallets from one PC to another.

access one's BTC is the *wallet.dat* file and the password, if any, which protects the wallet data. The password is different than the set of private keys used to access the owned BTCs, as the latter is simply a sort of code used to claim ownership to the BTCs which are found in the virtual domain; the password is set by the user to encrypt the access to the wallet. If this *wallet.dat* file is permanently lost, it does not mean that the BTC are destroyed, but it simply means that the access to those BTC is permanently lost and cannot be reclaimed by anyone.

In order for forfeiture of BTC to take place, firstly one needs the *wallet.dat* file. This can either be obtained by forcing the convicted person to transfer such file to the forfeiting authorities, or by physically seizing the medium on which such file is stored and access it directly. It is important to note that access to a single *wallet.dat* file is enough, even if there are multiple copies of it, as anything changed in one file will be relayed throughout the BTC network and will hence also be changed in any other copy of the same file. Once the *wallet.dat* file is obtained, one needs to see whether it is protected by a password. If it is, the password either has to be cracked or obtained from the convicted person; the more complex the password is, the more difficult it is to crack using 'brute-force' mechanisms. Once the BTCs are accessed, all that remains to be done is to transfer the forfeited amount in favour of the Maltese government. All this is akin to a situation where the convicted person owns an amount of cash money which needs to be forfeited and whose location is unknown. The private keys stored in the *wallet.dat* file are akin to a map showing the precise location where the cash money is stored; the password is akin to a lock combination on a safe which can be cracked if it is not too complex.

Subordinately, if the convict refuses to transfer the *wallet.dat* file or to divulge the password protecting such file, then he/she must transfer the amount affected by such forfeiture order to the forfeiting authorities. As long as the BTCs in question are stored in a wallet which is in the convict's control, even if the *wallet.dat* file is transferred to third parties, then the forfeiture can still take place as long as the authorities have access to a single copy of the *wallet.dat* file. The elephant in the room is what happens when the convict transfers his/her BTC to a third party-owned wallet – the situation becomes thornier especially if such third party cannot be identified, which may be the case if tumblers are used. If the third party is identifiable, then such third party may in turn be proceeded against if in bad faith, without prejudicing the rights of those third parties who are in good faith[285].

If the BTC cannot be retrieved or the whole amount owned is not disclosed by the convicted person, then a very important provision of the PMLA[286] comes into play. The mentioned provision stipulates that should the proceeds of the offence prove to have been dissipated or otherwise impossible to recover, as would be the case in an untraceable *wallet.dat* file or unknown password, then the Court may impose the payment of a fine (multa) on the convicted person, which fine would be equal to the amount of the proceeds of the offence, and such fine would be recoverable as a civil debt constituting an executive title *ipso jure*[287]*.* Such fine should be payable in either BTC or FC.

Finally, in order for the Court Registrar to trace and ascertain the whereabouts of any stored BTC which are the proceeds of an offence, the same Registrar has to be versed in IT and may require ulterior training in order to deal with such a novel facet to the aspect of asset forfeiture.

Presumptions of bad faith/illicit intent

In order to facilitate the prosecution's task in proving such a complex offence as money laundering, especially with the advent of BTC, two further presumptions may be introduced. The first one is linked to what has been aforementioned regarding the forfeiture of assets, specifically the mentioned situation where the attached *wallet.dat* file is transferred to third parties. A *juris tantum* presumption of bad faith may be assumed if, rather than receiving the BTCs themselves, the third party receives the *wallet.dat* file from the accused person, especially if that is the sole copy of such a file. While a third party who receives BTC may or may not be in good faith, such issue becomes unequivocal were the third party to receive the *wallet.dat* file itself; a transfer of the file itself is never required when transferring BTC, so sending the file which contains the private key of the wallet may be assumed to amount to an attempt to conceal the file itself away from the eyes of the confiscating authorities.

[285] European Parliament and Council Directive 2014/42/EU, Article 6(2)
[286] Chapter 373 of the Laws of Malta, Article 3(5)(b)
[287] Ibid.

A similar presumption may be invoked vis-à-vis the accused person in the case where there is the proven utilisation of a tumbler. As shall be explained shortly, the use of BTC tumblers denotes the intent to 'anonymise' the transaction, which in turn makes it extremely difficult to trace even with the use of the public ledger. Such a presumption would be linear to the line of thought present in the EU Directive concerning the retrieval of the proceeds of crime, wherein it is stated that "when determining whether a criminal offence is liable to give rise to economic benefit, Member States may take into account the modus operandi"[288] of the person concerned in the proceedings. Therefore, this presumption should be introduced in the PMLA as well.

Naturally, both such presumptions can be rebutted by the third party/accused respectively, as "the affected person shall have an effective possibility to challenge the circumstances of the case, including specific facts and available evidence on the basis of which the property concerned is considered to be property that is derived from criminal conduct"[289].

Ban the use of tumblers

BTC Tumblers, as explained previously, are programs or service providers which "randomly crisscross your BTC with other users' BTC so that you get a clean address that the blockchain cannot connect with any of the addresses from which the coins were stolen"[290]. It is a tool specifically purposed to make BTC transactions anonymous, or at the very least, very difficult to trace back to the original transacting persons. Therefore, it is clear that the use of such Tumblers should be included in the PMLA as an illegal practice, in order to ensure that the public ledger shows as much as possible licit transactions and the proper addresses used for such listed transactions.

Freezing orders

Article 5 of the PMLA stipulates that the prosecution can request the Court to order that the property of the accused is 'frozen', whereby the accused, or third parties as the case may be, are prohibited from "transferring, pledging, hypothecating or otherwise disposing of any

[288] European Parliament and Council Directive 2014/42/EU, Preamble 20
[289] Ibid., Article 8(8)
[290] Adrianne Jeffries, 'How to steal Bitcoin in three easy steps' (*The Verge*, 19 December 2013) <http://www.theverge.com/2013/12/19/5183356/how-to-steal-bitcoin-in-three-easy-steps> accessed 1 April 2015

movable or immovable property"[291]. Such a procedure is generally termed, and the property involved includes both immovable and movable property such as BTC. While it would be relatively easy for BTC service providers such as exchanges to freeze the requested amount in BTC, the situation may be a bit more complex for private wallets. It is therefore advisable that the suggestion of 'colour-coding addresses' referred to previously is coupled with the notion of freezing orders, whereby BTC addresses affected by such order are 'colour-coded' in order to differentiate them from other assets which may be free of such freezing orders. Hence, an amendment under Article 5 of the PMLA may be introduced whereby any persons who receive BTCs suppressed by a freezing order would immediately be alerted and, apart from safeguarding their rights, inform the relevant authorities about the matter. Failure to do so should bear adverse consequences.

Investigation order – the addition of a cloud-based warrant

Article 4 of the PMLA gives the AG the power to request the Criminal Court to issue an investigation order, which order grants the AG and/or other persons indicated in the order access to material or to persons indicated in the said order, in connection with an ongoing investigation on a person suspected to have committed an offence. The person/s indicated in the order also have the power to enter any building, house or other enclosure for the purpose of searching for the indicated material[292]. Sub-article 4 of the same Article then speaks about information contained on a computer, where such an investigation order "shall have effect as an order to produce the material or give access to such material in a form in which it can be taken away and in which it is visible and legible"[293].

In an era where data and information is increasingly being stored online rather than on one's own PC or other device, the latter provision of the law may be said to be rather outdated. It would be too cumbersome for the investigating authorities to physically locate the computer or server hardware[294] on which such information is stored, and then ask the person with access to such computer or server to produce the material in a physical form, in a world where digital prevails over analogue. Indeed, a lot of data nowadays is stored on the so-called virtual "cloud", which is made up of a "shared pool of configurable computing

[291] Chapter 373 of the Laws of Malta, Article 5(1)
[292] Ibid., Article 4(1)
[293] Ibid., Article 4(4)
[294] A web server is run on computer hardware

resources"[295], with the term "cloud" mostly being used as a "a generic term that refers to a network where the physical location and inner workings are abstracted away and unimportant to the usage"[296].

Instead of physically accessing the location in which the required data for the investigation order is stored, the investigative authorities would be better off issuing a cloud-based warrant. Such warrant has already been mentioned in Chapter 3.5.2, while discussing the Liberty Reserve case, where the investigative authorities in that case executed one of the first ever cloud-based warrants. Such a cloud-based warrant would entail requesting the administrators of the web server on which the required data is stored to produce and forward the said requested data to the investigative authorities, without the necessity to pinpoint the location of the physical machines on which the data is stored, as the term 'cloud' would refer to the virtual storage of the data, not the physical storage of such data. Therefore, if one were to ask for data stored on a fictitious webpage called *www.thesistestwebpage.com* using a cloud-based warrant, the warrant need not include the physical location of the hardware on which such data is stored, but it would be up to the person named in the investigation order, such as the server administrator or trained investigation officer, to retrieve such data irrelevantly of its true physical location. Regardless of whether the data's true physical location is Malta, France, Russia, Australia or anywhere else, the warrant would be concerned with the web domain itself, the virtual world rather than the real world.

Such a suggestion presents a myriad of obstacles, one of them being the shift from a physical legal jurisdiction to a virtual one. Whereas traditionally the collection of electronic evidence relied on the jurisdiction in which it was situated, "the cloud offers location independence so that data are available from anywhere, even though location may determine jurisdiction"[297], and such a shift would require an international forum, perhaps even a treaty, in order to have it crystallised and homogenised globally to allow an authoritative person to sift through the

[295] Peter Mell & Timothy Grance, 'The NIST definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology', National Institute of Standards and Technology Special Publication 800-145, 2011 <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf> accessed 30 March 2015

[296] Josiah Dykstra, *Seizing Electronic Evidence from Cloud Computing Environments*, (University of Maryland, Baltimore 2013) <http://www.csee.umbc.edu/~dykstra/Seizing-Electronic-Evidence-from-Cloud-Computing-Environments.pdf> accessed 30 March 2015, pg. 158

[297] Ibid., pg. 157

data of a website. Secondly, it would also require highly trained experts to locate and individualise the required data for the investigation from the vast amount of data which is at hand, particularly when investigating data-heavy websites such as PayPal, especially as there exist several types of programs and software 'languages' in which websites are coded, with each of them requiring a separate specialist. Other issues such as the ownership of the data found in the 'cloud' arise as well – such intricacies however do not form part of the subject of the thesis.

Apart from this, it is also advisable that the powers of the police are increased vis-à-vis the cyber sphere in order to enable them to identify and track criminals who use VCs in a covert manner, most likely with the aid of tumblers and other anonymity tools. Europol highlighted this issue and expressly stated that "police forces do not have sufficient powers to operate online and identify groups using the so-called dark net to carry out illicit transactions using digital currencies"[298].

Although this suggestion may be more of a *'sui generis'* one rather than specific to the PMLA, it would be an added asset for those combating money laundering.

Increase the powers of the FIAU

The FIAU can be described as the overseer in AML regulation compliance, and hence it requires the proper tools in order to combat money laundering. The FIAU has already had its powers widened by Act III of 2015 and L.N. 464 of 2014, with added functions such as the ability to terminate a business relationship which has a risk of money laundering[299], requesting information about transactions from a non-reputable jurisdiction[300], and other added powers. However, with the advent of VCs, the FIAU may need additional powers and resources.

[298] Jane McCallion, 'Europol calls for greater Bitcoin policing powers'(*IT Pro*, 25 March 2014) <http://www.itpro.co.uk/public-sector/21903/europol-calls-for-greater-bitcoin-policing-powers> accessed 30 March 2015

[299] Regulation 18 of L.N. 464 of 2014

[300] Ibid., Regulation 12(c)

One such paramount need is the introduction of a specialised IT department, separating it from the current "Administration and IT section"[301]. Such a department should employ persons who are well-versed in VCs and have a high-level IT background. Their purpose would not specifically be to track down and investigate cyber money launderers per se, as that would be a task mostly pertinent to the Cyber Crime Unit of the Malta Police Force, but it would be worth having in-house expertise both so as to increase the efficiency in the liaising with the Police as well as to be in a position to monitor and track suspicious VC transactions if need be. At a time where online transactions are gaining more and more importance, the IT aspect should definitely not be neglected.

The FIAU should also have direct access to the log of IP addresses of large volume transactions, which log has been suggested in Chapter 4.2. Along with such access, the FIAU should also have direct access to databases held by subject persons, with such access being strictly limited to what is necessary for the FIAU to carry out its functions, and with the data accessed being protected in accordance with data protection regulations. Potentially, such access could be limited to special circumstances which would require the FIAU to override access to the relevant database in order to identify a high-risk money laundering threat.

Delayed execution of suspicious transaction

Article 28 of the PMLA stipulates the imposition of an obligation on the subject person to delay a transaction which is known or suspected to be linked to money laundering or funding of terrorism, or constitutes the proceeds of a crime. Before executing the transaction, the subject person has to forward all information concerning the transaction to the FIAU, and if the FIAU is of the opinion that the transaction is indeed linked to money laundering or funding of terrorism or constitutes the proceeds of a crime, it may oppose the execution thereof.

If the subject person acts as a receiver for a transaction request and has to process the transaction itself, then such a provision would work. However, if the subject person allows a direct transaction to the BTC network from its users, then the situation changes and Article 28 cannot be used, as BTC transactions cannot be delayed and are executed immediately,

[301] 'Organisational Chart' (*FIAU* website) <http://www.fiumalta.org/about/organisational-chart> accessed 1 April 2015

becoming ‘stamped’ with the next mined block as explained previously. Ideally there should be a provision entailing the prohibition of subject persons from allowing direct transactions to the BTC network, meaning that transactions would be screened and blocked, if need be, by the subject person. Therefore, if a customer or account holder of the subject person wishes to initiate a transaction, such transaction would not take place the moment the customer/account holder makes the transaction, but it would have to be processed by the subject person, hence slightly adding to the total transaction time.

Another suggestion, which may be seen as draconian, would be to automatically reject any transactions originating from addresses which have been ‘colour-coded’ or tagged as linked to money laundering/funding of terrorism, or are suspected to be so. However, this may act as a double-edged sword, as such automatic blocking may interfere with an ongoing investigation by the enforcing authorities, or, in cases where the transacting persons are later proven not to be linked to money laundering, cause unnecessary vexation and interference with the said persons’ activities.

Prohibit the tenure of unauthorised BTC addresses by subject persons

In order to adequately supervise subject persons and the transactions received and carried out in their capacity as subject persons (that is, not in their private capacity), such subject persons should be required to register the BTC addresses used with the FIAU, hence greatly simplifying the oversight process and ensuring that each and every transaction is monitored, enabling the FIAU to act immediately on suspicious transactions. Moreover, subject persons should not be allowed to retain BTC addresses which are undeclared to the FIAU. Naturally, the same cannot apply to private persons, both for privacy reasons as well as the near-impossibility of ensuring that each and every person registers his or her BTC addresses with the authorities.

4.3.3 – Possible Amendments to the Prevention of Money Laundering and Funding of Terrorism Regulations

As with the PMLA, certain changes would be required in the FTR in the eventuality that BTC, or other VCs, become mainstream and therefore would need to be integrated in the AML framework, especially since without proper regulation, the pseudonymity offered by BTC can pose a serious threat for law enforcers and an opportunity for criminals.

Include VC-fiat exchanging and other financial activities in the First Schedule of the Financial Institutions Act

Out of the several service providers which operate in BTC, VC exchanges are perhaps the highest risk-rated ones targetable by money launderers, and therefore require the most stringent regulations in place. The FTR does not, as yet, cater for VC exchanges; however, ideally it should not be the FTR which caters directly for such entities, but such activity should be included in the list of activities of financial institutions present in the Financial Institutions Act[302]. A plausible example of how to list VC exchanges in the mentioned list of activities would be the following:

> *Trading or exchanging* fiat *currencies to Bitcoin or other virtual currencies, or vice-versa.*

Such a definition would cover persons which offer services exchanging FCs to BTC/VCs and vice-versa, or buy/sell BTC or other VCs for FCs; however, it would not apply to those exchanges which solely operate in VCs and offer exchange services from one VC to another. It is highly unlikely that any other VC will gain as much prominence as BTC in the near future, and even if it were so, in the near future the bridge between VCs and FCs will still remain of much greater importance in the AML framework due to the small amount of usage of BTC and other VCs when compared to that of FCs. Moreover, over-regulation would risk stifling the development of VCs, some of which may prove to be better suited to real-world use than BTC, among other potential benefits.

[302] Financial Institutions Act, Chapter 376 of the Laws of Malta, First Schedule

VC exchanges would have to be licensed in terms of the Financial Institutions Act, and it would need to have as its main business activity the exchange, to-and-fro, of FCs and BTC/VCs, or the trading thereof as previously described, and therefore the FTR would not apply to those persons who occasionally offer such a service, or whose primary business is not the exchange of such currencies, therefore being ancillary to their primary business. Such **an inclusion in the First Schedule would thus automatically make VC exchanges within the scope of the FTR**, namely inclusion in the list of "relevant financial business", as well as subject to scrutiny by the MFSA due to the licensing requirements.

Assess the possibility of including other BTC/VC service providers and other entities in the list of relevant financial business

Apart from VC exchanges, other entities such as wallet service providers and payment processors should also be considered for inclusion in the list of relevant financial business at a future stage where BTC and other VCs may have grown and stabilised themselves. Payment processors such as Coin.co[303] can become potential targets for money laundering especially if the volume of transactions increases in the next few years, and the same goes for wallet service providers, especially those which provide hosted online wallets which can be accessed by any device connected to the Internet. Roping in such businesses into the AML regime would be beneficial; however, the author is strictly of the opinion that such a measure should first solely be adopted vis-à-vis VC exchanges, both in order to analyse the effect of such a measure and also because it would not be advisable to legislate upon each and every business tied with BTC/VCs, due to the fact that they are still at a very early stage.

CDD and KYC procedures made applicable to BTC service providers

If VC exchanges and other BTC service providers are brought within the ambit of the FTR, they would be obliged to execute KYC and CDD procedures. If the persons transacting are known to the supervising authorities, this greatly reduces the problem of pseudonymity which is associated with BTC. Moreover, the identities of the users would only be known to the exchange on which they are registered, protected by Data Protection legislation with the exchanges only being bound to disclose information about its users to the supervisory

[303] *Coin.co* website <https://coin.co/> accessed 1 April 2015

authorities and, exceptionally, to the State investigative authorities in case of any criminal investigation tied to one or more of its users.

Expressly list other entities as subject persons

Currently, the only entities obliged to report suspicious transactions are the persons subject to the FTR, ergo "any legal or natural person carrying out either relevant financial business or relevant activity"[304], with both the lists of relevant activities and relevant financial business being exhaustive and not inclusive lists. Out of all the businesses mentioned in the surveys conducted, car dealing is the most worrisome category of business in the author's opinion, which business should be expressly included as a subject person in the FTR. While theoretically covered by the generic threshold of a "single large transaction", in practice car dealers are not adequately covered by the FTR and can be potential targets for money launderers, especially if cash is used as a means of payment. The same will hold if the payment method used is BTC via private wallets. This is due to the fact that normally cars are sold for an appreciable amount of money, and verifying the identity of the customer is only a small added hurdle to the paperwork which has to be conducted when transferring ownership of cars.

Decentralising reporting

With reference to the decentralised flagging system suggestion in Chapter 4.2, any interested person should ideally be able to report a suspicious transaction. This would be possible thanks to the public ledger which lists all the BTC transactions. It is important to note that persons without access to the data concerning the identities of the persons transacting would only be able to report the transaction ID itself, and then it would be up to the FIAU/supervisory authorities to track down the identities of the transacting persons. Colour-coding the transactions on the public ledger would also further help identifying suspicious transactions. Ideally, this should work along an automated system which automatically submits suspicious transactions, acting as double oversight.

[304] S.L. 373.01, Regulation 2(1)

PEPs have supervised and transparent wallets

Politically Exposed Persons (PEPs) are "natural persons who are or have been entrusted with prominent public functions and shall include their immediate family members or persons known to be close associates of such persons"[305] and therefore may also have access to or be in control of public funds. PEPs should therefore be scrutinised and supervised closely; indeed, the FTR obliges subject persons to apply enhanced CDD to PEPs, and also require an ongoing enhanced monitoring of such business relationships with PEPs[306].

In addition to having supervised BTC wallets along with a specially assigned colour code to their BTC addresses, it is also worth considering listing PEPs' transactions on a separate public ledger so as to be completely transparent to the public, as well as making the funds in such wallets available for public viewing. Such a measure should best be applied solely to the "natural persons who are or have been entrusted with prominent public functions"[307] and not to their close family members/associates as well, for the sake of limiting the intrusion into their private family lives. Although it can be described as a somewhat controversial measure, it would greatly increase the transparency of public spending and ensure that every person with access to the Internet can verify how the public money is being spent.

Lastly, the IP addresses and/or identity of both the sender and recipient addresses when BTCs are sent by PEPs should be immediately tagged and made available to the supervisory authorities, so as to truly ensure an effective supervision of PEPs.

Lower the threshold of the single large transaction

Currently, a transaction is considered to be a "single large transaction" (SLT), as defined in the FTR[308], when the amount is that of €15,000 or more, or where several transactions which are linked to each other amount to €15,000 or more. In the P4MLD[309], such a threshold has been lowered to €7,500, as the previous limit was deemed to be too high; this change has not yet been implemented in the FTR.

[305] Ibid.

[306] Ibid., Regulation 11(6)

[307] Ibid., Regulation 11 (7)(a)

[308] Ibid., Regulation 2(1), "Case 3"

[309] 2013/0025 COD, Article 2(1)(3(e))

Since one of BTC's advantages is its use in microtransactions due to the negligible transactions fees, the author opines that even the €7,500 limit to be introduced would still be too high and would present a risk whereby potentially some transactions linked to money laundering/funding of terrorism would pass under the radar. Therefore, in the author's opinion, the limit should be lowered further to €5,000, which, after all, still represents a sizeable chunk of a person's annual salary if such person is on the minimum wage[310] and hence such transactions also merit a detailed check.

Apply Enhanced CDD for private wallets

Regulation 11 of the FTR stipulates the instances in which Enhanced CDD (ECDD) is to be applied, which is a more stringent form of CDD than Simplified CDD (SCDD). With regards to BTC, it is important to once again draw a distinction between BTC accounts held by a company online which already has to apply rigorous ECDD when first creating the said account, and BTC stored in a privately owned wallet. With regard to the former, it is enough if SCDD is regularly conducted, with ECDD only being used in cases where a transaction is either over the stipulated limit for an SLT, or when there is a risk that the transaction may be linked to money laundering/funding of terrorism.

However, if a transaction is being processed via a privately owned BTC wallet, then no prior ECDD would have been conducted on the owner of the wallet and therefore there would be a high risk for money laundering. Two possible suggestions are hereby being proposed: either apply ECDD if the transaction surpasses a certain amount, or outright prohibit BTC/VC transactions exceeding an established amount when payment is made from a private wallet. In the former suggestion, the transaction threshold should be a low one, with a €1,000 limit being deemed a good balance between day-to-day usability and adequate protection against any possible abuse[311]. Such ECDD should be rigorously applied in online transactions, where the customer is not physically present; in face-to-face transactions, certain exceptions may be allowed using the risk-sensitive approach, although the normal SLT limit would still be applicable in such instances.

[310] Eurostat, 'Monthly minimum wages - bi-annual data' (*Eurostat* website) <http://ec.europa.eu/eurostat/en/web/products-datasets/-/EARN_MW_CUR> accessed 2 April 2015

[311] Author's opinion

The same €1,000 threshold may also be applied in the latter suggestion. Although this approach is safer and presents a lower risk of possible abuse, it may potentially hamper BTC trade, and should ideally be considered at a later stage once the BTC network has strengthened so as to allow a freer initial development.

Limit the amount of BTC/VCs which can be held in a single account

Another alternative approach to what has been suggested, which also merits consideration, would be to limit the amount of BTC which can be held by a single account if such account is opened with a bank, exchange, wallet service provider or other similar business. This would operate much like the limit imposed on a VISA card by a bank. The limit imposed should not be as low as to discourage customers or account holders from utilising BTC or other VCs, and such limit can be changed according to established checks on the clients pertinent to their professions and lifestyle.

Recordkeeping requirements

Apart from the mandatory information about clients/customers required to be kept by subject persons, such as the name, surname, physical address, identity card number, and so on, subject persons should moreover record other information when dealing in BTC/VCs. Such information should include the public addresses of the wallets used, the corresponding public keys of the wallets, a complete log of the transactions carried out, including the amount transferred and the wallet address of the other party/parties to the transaction, with other relevant information such as a log of the IP addresses if need be. The records should be kept for an adequate period of time, with five years being a reasonable period in the author's opinion. Moreover, the records should be made available for direct access to the FIAU.

Requirements for the MLRO

A subject person is duty-bound to appoint a Money Laundering Reporting Officer (MLRO), whose function is to receive reports or information on any transaction which has or may be linked to money laundering or funding of terrorism, or any person so linked[312], and if need be, forward such report or information to the FIAU for further investigation. The MLRO

[312] Ibid., Regulation 15(4)

needs to be well-versed in the AML legislation, but with the advent of BTC, the MLRO should also be trained in IT, especially in the way in which BTC transactions work and should have an overall understanding of the BTC network[313].

The subject person, normally through the MLRO, is obliged to report suspicious transactions or persons to the FIAU "as soon as is reasonably practicable, but not later than five working days"[314]. In the author's opinion, the five-day limit is too long a period especially if one considers the near-instantaneous transaction speeds of BTC. The limit should be brought down to two working days, and reports of suspicious BTC transactions should have precedence over other transactions made via other traditional banking systems due to the transaction speed.

Bottom line

One needs to be very careful when treading the fine line between lack of regulation and overregulation, especially with such a novel product as BTC which is still in its infancy. The abovementioned changes would tighten the fence around BTC so as to ensure, as much as possible, that incidents such as Silk Road would be avoided in the future, but it would still allow room for BTC to develop freely. Moreover, the abovementioned changes need not be introduced all at once, or even adopted wholly; they are simply a set of suggestions which may act as guidelines as to what is needed to set the ball rolling on legislation vis-à-vis BTC/VCs in the AML sphere. As stipulated in the FTR, AML measures should not be restrictive "in allowing the provision of financial and other services to the public in general"[315]. BTC users would also be free to an extent to choose whether to keep in line with AML requirements and register an account with an AML-compliant company, forsaking anonymity but still retaining most of the benefits pertaining to BTC. Otherwise, they can choose to continue utilising personal BTC wallets, and even use Tumblers, at the risk of either breaking the law or face greater scrutiny by payment receivers, even perhaps having his/her transactions rejected if they cannot be sufficiently verified.

[313] Author's opinion
[314] Ibid., Regulation 15(6)
[315] Ibid., Regulation 7(9)

What is also important is that, as already discussed, **BTC is not anonymous** and with the mentioned measures, neither would it be classified as pseudonymous, and would therefore satisfy the requirements of S.L. 373.01[316].

[316] Namely, Regulation 7(4) which states that "Subject persons shall not keep anonymous accounts or accounts in fictitious names."

CONCLUSION

The thesis sought to answer the hypothesis laid out in the title itself, but it is important to bear in mind that it is still too early to ascertain the tangible effects of BTC on the economy, and that what has been discussed throughout the thesis is based solely on the information available until the cut-off date stipulated in the introduction[317]. It is entirely possible that BTC and other VCs may die out as some other trends have, rendering the thesis obsolete. However, the author firmly believes that the technology underlying BTC will survive and develop, and that it may also be used as a currency; as stated at the outset, what is applicable to BTC is by and large applicable to other VCs as well, and therefore the thesis would still remain relevant were another VC to supersede BTC. Further research on other themes apart from money laundering, such as whether BTC truly classifies as a currency per se, whether BTC theft classifies as normal theft, the tax implications of BTC, the principle of ownership vis-à-vis BTC and a myriad of other topics can all form the subjects of future theses.

Bitcoin, quo vadis?

Focusing once again solely on BTC, it must be noted that to date, few countries have banned BTC on the premise that it can be used for AML purposes; the idea was simply bandied around at the initial stages of worldwide discussions, but it was duly recognised as an important technological development, and that outright prohibition would drive it underground, out of the regulators' oversight, to be used primarily for illicit intents. It is also worth noting that it is practically impossible to close down BTC; even if one were to somehow ensure that no more miners exist and that no one has access to any of the BTC in existence, it would only stave off the birth of another VC, as the technology underlying BTC cannot be destroyed. Therefore, the only prudent approach is to monitor any developments and legislate cautiously upon it.

For BTC to integrate fully within the existing AML framework, it must forsake some of its features, such as pseudonymity which borders onto anonymity when other tools are utilised. Some of the suggestions in Chapter 4.2 might not be welcome to BTC enthusiasts as they

[317] 1 May 2015

wholly believe in the “liberty” which BTC transactions provide, but if BTC is to survive, then it must gain traction in mainstream use, lest it become a momentary trend and nothing more. Lack of knowledge regarding BTC is still rampant, and if BTC remains the same with no leeway towards integrating with other systems, then inevitably and understandably States shall legislate against it, and in turn the common man on the street will remain ignorant about it. It is also important to remember that with the suggested changes, most of the important features of BTC remain intact, and that pseudonymity from the public point of view is untouched; it is solely the service providers and the supervisory authorities which will be able to access the identities behind the persons transacting, so as to ensure that the law is observed and that no financing of crime or laundering of money is taking place. Those persons who transact legitimately and in good faith do not have reason to be irked with the decreased pseudonymity of BTC, as other features such as fast transactions and global reach far outweigh such an issue. Having said that, it is also important that data protection remains paramount, and that in no way should the people’s privacy be breached and abused.

Moreover, there is no reason to negatively apprehend BTC, as the research conducted shows that most of BTC’s pitfalls are shared with cash, with the latter being a much better-suited tool for money laundering due to a very elevated level of anonymity; if countries consider banning BTC, then they should also consider banning cash. Moreover, BTC are different than the Austrian *sparbuchs,* where the anonymous bank accounts were being utilised for the primary purpose to afford their users anonymity, and were also controlled by a central authority, namely the Austrian central bank, and therefore not subject to public scrutiny and/or control[318]; additionally, BTC certainly cannot be classified as anonymous and would hence not fall foul of Article 6 of the 3MLD[319]. The most prudent approach is to legislate so as to protect the gateways from FCs to VCs and vice-versa, with the most obvious gateway being VC exchanges, and ensure that KYC and CDD procedures are carried out by such exchanges and other prominent BTC/VC service providers.

[318] Refer to Chapter 2.2
[319] Council Directive 2005/60/EC Article 6

Working hand-in-hand on a global scale

Apart from prudent legislation by each individual State at this point in time, the author feels impelled to point out that global AML coordination needs to be stepped up tremendously. It is not acceptable to implement a homogenous AML framework in each and every country, as countries have different economies and different needs. It has been noted in Chapter 2.1 that several countries do not have a developed economy, let alone a comprehensive framework with which to combat money laundering. The advent of BTC should, if anything, serve as a wake-up call for legislators to revamp the current framework and cater for each and every country's needs so as to ensure proper coordination on an international scale. The EU already provides for a regional mutual recognition of judgements and judicial cooperation infrastructure, stipulating that the enactment of such rules "shall take into account the differences between the legal traditions and systems of the Member States"[320]. Moreover, the EU also stresses the importance of international cooperation in areas such as asset recovery and mutual legal assistance, especially in view of the fact that organised criminal groups operate without borders and acquire assets in States other than those in which they are based[321]. These are precisely the kind of approaches which need to be adopted on an international scale.

Apart from the judicial sphere, cooperation has to extend to legislators as well as consulting with BTC/VC businesses in the private sector so that the regulatory bodies gain a better and deeper understanding of the way in which such technologies work, without expending their own resources in order to gain such information and moreover collecting such information over a shorter period of time. Such cooperation in the law-making sphere should ideally concern, *inter alia*, a uniform definition of predicate offences, more efficient extradition procedures, and extended investigative powers of the police when cross-border crimes are involved. Transactions in BTC or other VCs often touch upon infrastructures and entities located in different countries across the world, ergo different jurisdictions with different legal parameters. International cooperation becomes even more important when

[320] Consolidated Version of the Treaty on the Functioning of the European Union [2007] OJ C326/47, Article 82(2)

[321] European Parliament and Council Directive 2014/42/EU, Preamble 2

considering other upcoming novelties such as cloud-based warrants as discussed in Chapter 4.3.2.

The last word

Therefore, in conclusion, it is safe to state that BTC presents no higher risk of money laundering abuse when compared to cash, with proper legislation and technical changes potentially leading to **a system which is even more robust at combating money laundering than the current systems based on FCs**. It is prudent to let BTC distribution and increased awareness take their course, with appropriate and well-timed legislation serving so as to push BTC into the mainstream sphere. Broader distribution is extremely important, as one of the current problems which hamper efforts to bring BTC in line with AML Legislation is the existence of a small number of large 'bagholders'[322] who could in effect autonomously operate as hotspots for money laundering without the need to use an exchange and hence bypass any imposed KYC and CDD safety checks. Such 'bagholders' would effectively be able to act as exchanges in their own right and sell their BTC in exchange for dirty money.

Such a problem can be greatly minimised if, through an increased awareness on BTC and a higher rate of distribution as the technology enters the mainstream sphere, the current global amount of BTC is dissipated and spread across a larger amount of users, with the aforementioned bagholders becoming more incentivised to sell their BTC if their value increases and a wider range of products and services can be purchased with BTC. It will not eliminate the problem altogether, but such a problem is also present in *fiat* currencies[323]. Therefore, prudent and researched legislation would favour both AML efforts as well as BTC itself, ushering in a new era of payment mechanisms and other myriad uses of the technology underlying BTC; what is unknown should not be banished, but it must be embraced and understood, as its uses and benefits may sometimes far outweigh its drawbacks, as is firmly the case with BTC.

[322] A common term used in economics to signify persons or entities which possess a large quantity of the object in question.

[323] Larry Elliott & Ed Pilkington, 'New Oxfam report says half of the global wealth held by the 1%'(*The Guardian,* 19 January 2015) <http://www.theguardian.com/business/2015/jan/19/global-wealth-oxfam-inequality-davos-economic-summit-switzerland> accessed 10 April 2015

BIBLIOGRAPHY

Legislation and Treaties

Malta

Act III of 2015 - Various Laws (Prevention of Money Laundering and Funding of Terrorism) (Amendment) Act, 2015 [Government Gazette of Malta No. 19,385 – 20.02.2015]

Central Bank of Malta Act, Chapter 204 of the Laws of Malta, Article 44

Criminal Code, Chapter 9 of the Laws of Malta

Dangerous Drugs Ordinance, Chapter 101 of the Laws of Malta

Financial Institutions Act, Chapter 376 of the Laws of Malta

L.N. 464 of 2014 - Prevention of Money Laundering and Funding of Terrorism (Amendment) Regulations, 2014 [Government Gazette of Malta No. 19,358 – 16 December 2014]

Prevention of Money Laundering Act, Chapter 373 of the Laws of Malta

Prevention of Money Laundering and Funding of Terrorism Regulations, S.L. 373.01

European Union

Consolidated Version of the Treaty on the Functioning of the European Union [2007] OJ C326/47

Council Directive (EC) 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering [1991] OJ L166/77

Council Directive (EC) 2001/97 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering [2001] OJ L344/76

Council Directive (EC) 2005/60 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing [2005] OJ L309/15

Electronic Money Directive (2009/110/EC) on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC [2009] OJ L267/7

European Parliament and Council Regulation 1781/2006 on information on the payer accompanying transfers of funds [2006] OJ L345/1

European Parliament and Council Directive 2014/42/EU on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union [2014] OJ L127/39

Other Foreign Legislation

Germany: Banking Act of the Federal Republic of Germany (Kreditwesengesetz, KWG)

Germany: Criminal Code in the version promulgated on 13 November 1998, Federal Law Gazette [Bundesgesetzblatt] I p. 3322, last amended by Article 3 of the Law of 2 October 2009, Federal Law Gazette I p. 3214

Isle of Man: Proceeds Of Crime (Business In The Regulated Sector) Order 2015, Article 1(mm)

Japan: The Act on Punishment of Organized Crimes and Control of Crime Proceeds (Act no. 136 of 1999)

Japan: The Act on Prevention of Transfer of Criminal Proceeds (Act no. 22 of 2007)

United States: Assembly Bill 129, California Assembly, 23 June 2014

United States: Bank Secrecy Act, 26 October 1970

United States: Securities Exchange Act, 6 June 1934

United States: U.S. Code, Title 31, Chapter 53

United States: U.S. Code of Crimes and Criminal Procedure, Title 18

Treaties and Conventions

United Nations Vienna Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (adopted 20 December 1988, entered into force 11 November 1990)

Articles

-- AFP, ‘Bangladesh warns of jail for Bitcoin traders’ (*AsiaOne Business*, 15 September 2014) <http://business.asiaone.com/news/bangladesh-warns-jail-bitcoin-traders> accessed 7 February 2015

-- Bloomberg, ‘China Bans Financial Companies From Bitcoin Transactions’ (*Bloomberg News*, 5 December 2013) <http://www.bloomberg.com/news/2013-12-05/china-s-pboc-bans-financial-companies-from-bitcoin-transactions.html> accessed 7 February 2015

-- Circa Media Organisation, ‘Prosecutors attempt to link Ross Ulbricht email address to Silk Road’ (*Circa Media Organisation*, 30 January 2015) <http://cir.ca/news/silk-road-seized> accessed 25 February 2015

--Spiegel, ‘’Private Money': Bitcoins Gain Ground in Germany’ (*Spiegel Online International*, 20 August 2013) <http://www.spiegel.de/international/business/germany-declares-bitcoins-to-be-a-unit-of-account-a-917525.html> accessed 4 February 2015

-- CoinDesk, 'State of Bitcoin 2015: Ecosystem Grows Despite Price Decline' (*CoinDesk,* 7 January 2015) <http://www.coindesk.com/state-bitcoin-2015-ecosystem-grows-despite-price-decline/> accessed 13 January 2015

-- Times of Malta 'Malta lags behind on Bitcoin opportunities' (*Times of Malta*, 14 August 2014) <http://www.timesofmalta.com/articles/view/20140814/business-news/Malta-lags-behind-on-Bitcoin-opportunities.531822> accessed 4 February 2015

Cawrey D., 'Could Bitcoin Become a Policy Issue for US Congress?', (*CoinDesk*, 25 October 2014) <http://www.coindesk.com/bitcoin-become-policy-issue-us-congress/> accessed 9 February 2015

Cawrey D., 'Is Double Spending Unconfirmed Transactions a Concern for Bitcoin?' (*CoinDesk*, 23 April 2014) <http://www.coindesk.com/double-spending-unconfirmed-transactions-concern-bitcoin/> accessed 29 October 2014

Clinch M., 'Bitcoin recognized by Germany as 'private money'' (*CNBC*, 19 August 2013) <http://www.cnbc.com/id/100971898> accessed 22 September 2014

Cohen D., 'Farewell, Facebook Credits' (*Adweek*, 13 September 2013) <http://www.adweek.com/socialtimes/farewell-facebook-credits/428240> accessed 29 October 2014

Davis R. P., 'Isle of Man Welcomes Digital Currency Exchanges "No License Required"' (*Coindesk*, 28 March 2014) <http://www.coindesk.com/isle-man-welcomes-digital-currency-exchanges-license-required/> accessed 4 February 2015

Elliott L. & Pilkington E., 'New Oxfam report says half of the global wealth held by the 1%' (*The Guardian,* 19 January 2015) <http://www.theguardian.com/business/2015/jan/19/global-wealth-oxfam-inequality-davos-economic-summit-switzerland> accessed 10 April 2015

Falconer R., 'World powers react to the Bitcoin boom' (*Al Jazeera*, 7 December 2013) <http://www.aljazeera.com/indepth/features/2013/12/world-powers-react-bitcoin-boom-2013127115950323990.html> accessed 22 September 2014

Ferenstein G., 'Congressman Calls To Ban U.S. Dollar In Response To Plea For Bitcoin Ban' (*TechCrunch*, 5 March 2014) <http://techcrunch.com/2014/03/05/congressman-calls-to-ban-u-s-dollar-in-response-to-bitcoin-ban/?utm_campaign=fb&ncid=fb> accessed 9 February 2015

Fung B., 'Sen. Joe Manchin calls for a Bitcoin ban as regulators seek 'accelerated push'' (*Washington Post*, 26 February 2014) <http://www.washingtonpost.com/blogs/the-switch/wp/2014/02/26/sen-joe-manchin-calls-for-a-bitcoin-ban-as-regulators-seek-accelerated-push/> accessed 9 February 2015

Gibbs S., 'Nine Bitcoin alternatives for future currency investments' (*The Guardian,* 28 November 2013) <http://www.theguardian.com/technology/2013/nov/28/bitcoin-alternatives-future-currency-investments> accessed 20 September 2014

Gilbert M., 'And 2014's Worst Currency Was...Bitcoin' (*Bloomberg*, 23 December 2014) <http://www.bloombergview.com/articles/2014-12-23/and-2014s-worst-currency-wasbitcoin> accessed 13 January 2015

Gilson D., ‘German government relieves capital gains tax on Bitcoin positions’ (*CoinDesk*, 27 June 2013) <http://www.coindesk.com/german-government-relieves-capital-gains-tax-on-bitcoin-positions/> accessed 4 February 2015

Gorale A., ‘Are Bitcoin Zero Confirmation Transactions Safe?’(*CryptoCoinsNews*, 2 January 2015) <https://www.cryptocoinsnews.com/zero-confirmation-transactions-safe/> accessed 4 April 2015

Greenberg A., ‘Prosecutors Trace $13.4M in Bitcoins From the Silk Road to Ulbricht’s Laptop’ (*Wired*, 29 January 2015) <http://www.wired.com/2015/01/prosecutors-trace-13-4-million-bitcoins-silk-road-ulbrichts-laptop/> accessed 25 February 2015

Hern A., ‘A history of Bitcoin hacks’ (*The Guardian*, 18 March 2014) <http://www.theguardian.com/technology/2014/mar/18/history-of-bitcoin-hacks-alternative-currency> accessed 13 January 2015

Higgins S., ‘New York Reveals BitLicense Framework for Bitcoin Businesses’ (*CoinDesk*, 17 July 2014) <http://www.coindesk.com/new-york-reveals-bitlicense-framework-bitcoin-businesses/> accessed 12 February 2015

Jankelewitz E., ‘Bitcoin regulation in the UK’ (*CoinDesk*, 16 February 2014) <http://www.coindesk.com/bitcoin-regulation-uk/> accessed 6 February 2015

Jeffries A., ‘How to steal Bitcoin in three easy steps’ (*The Verge*, 19 December 2013) <http://www.theverge.com/2013/12/19/5183356/how-to-steal-bitcoin-in-three-easy-steps> accessed 1 April 2015

Lyons R., ‘The Primary Legal and Regulatory Hurdles to Widespread Digital Currency Usage’ (*Digital Currency Council,* 16 September 2014) <http://www.digitalcurrencycouncil.com/legal/the-primary-legal-and-regulatory-hurdles-to-widespread-digital-currency-usage/> accessed 13 January 2015

McCallion J., ‘Europol calls for greater Bitcoin policing powers’ (*IT Pro*, 25 March 2014) <http://www.itpro.co.uk/public-sector/21903/europol-calls-for-greater-bitcoin-policing-powers> accessed 30 March 2015

McKinnon J.D. & Tracy R., ‘IRS Says Bitcoin Is Property, Not Currency’ (*Wall Street Journal*, 25 March 2014) <http://www.wsj.com/articles/SB10001424052702303949704579461502538024502> accessed 2 March 2015

McMillan R., ‘The Inside Story Of Mt. Gox, Bitcoin’s $460 Million Disaster’ (*Wired*, 3 March 2014) <http://www.wired.com/2014/03/bitcoin-exchange/> accessed 28 March 2015

McMillan R., 'Bitcoin Values Plummet $500M, Then Recover, After Silk Road Bust' (*Wired*, 2 October 2013) <http://www.wired.com/2013/10/bitcoin-market-drops-600-million-on-silk-road-bust/> accessed 22 September 2014

Paul I., ‘How to use the Tor Browser to surf the web anonymously’ (PC World, 23 September 2014) <http://www.pcworld.com/article/2686467/how-to-use-the-tor-browser-to-surf-the-web-anonymously.html> accessed 29 October 2014

Rizzo P., ‘Bitcoin Advocates Back Petition for BitLicense Safe Harbor Provision’ (*CoinDesk*, 1 April 2015) <http://www.coindesk.com/bitcoin-petition-bitlicense-safe-harbor/> accessed 6 April 2015

Rooney B., 'Bitcoin worth almost as much as gold' (*CNN Money,* 2013) <http://money.cnn.com/2013/11/29/investing/bitcoin-gold/> accessed 20 September 2014

Simonite T., 'Mapping the Bitcoin Economy Could Reveal Users’ Identities' (*Technology Review*, 5 September 2013) <http://www.technologyreview.com/news/518816/mapping-the-bitcoin-economy-could-reveal-users-identities> accessed 29 October 2014

Southurst J., ‘Bitcoin Trader Gets Four-Year Jail Term Over Silk Road Connection’ (*CoinDesk,* 21 January 2015) <http://www.coindesk.com/charlie-shrem-co-accused-sentenced-4-years-prison/> accessed 28 February 2015

Southurst J., ‘Chinese Official: Bitcoin Can 'Co-exist' with fiat currencies’ (*CoinDesk*, 15 December 2014) <http://www.coindesk.com/chinese-official-bitcoin-can-co-exist-fiat-currencies/> accessed 7 February 2015

Spaven E., ‘HMRC: UK bitcoin exchanges don’t have to register under money laundering regulations’ (*CoinDesk*, 8 July 2013) <http://www.coindesk.com/hmrc-uk-bitcoin-exchanges-dont-have-to-register-under-money-laundering-regulations/> accessed 6 February 2015

Stacke J., ‘Analysis of Silk Road’s Historical Impact on Bitcoin’ (*The Genesis Block*, 3 October 2013 <http://thegenesisblock.com/analysis-silk-roads-historical-impact-bitcoin/> accessed 25 February 2015

Weise K., ‘Why Half the World Doesn't Have Bank Accounts’ (*Business Week*, 25 April 2012) <http://www.businessweek.com/articles/2012-04-25/why-half-the-world-doesnt-have-bank-accounts> accessed 4 November 2014

Wolf B., ‘U.S. Treasury cautions Bitcoin businesses on legal duties’ (*Reuters*, 17 December 2013) <http://www.reuters.com/article/2013/12/17/us-bitcoin-letters-idUSBRE9BG1DC20131217> accessed 9 February 2015

Yeoman K., ‘M-Pesa helps world's poorest go to the bank using mobile phones’ (*The Christian Science Monitor,* 6 January 2014) <http://www.csmonitor.com/World/Making-a-difference/Change-Agent/2014/0106/M-Pesa-helps-world-s-poorest-go-to-the-bank-using-mobile-phones> accessed 4 November 2014

Zetter K., ‘Bullion and Bandits: The Improbable Rise and Fall of E-Gold’ (*Wired*, 6 September 2009) <http://www.wired.com/2009/06/e-gold/all/> accessed 2 March 2015

Books

A.M. Antonopoulos, *Mastering Bitcoin* (1st, O'Reilly Media, California, U.S.A. December 2014)

Alexander R.C.H., *Insider Dealing and Money Laundering in the EU: Law and Regulation* (1st edition, Ashgate Publishing Limited, Surrey 2007)

Lenz K.F., *Japanese Bitcoin Law* (1st edition, CreateSpace Independent Publishing Platform, Charleston 2014)

Sharman J.C., *The Money Laundry: Regulating Criminal Finance in the Global Economy* (1st, Cornell University Press, New York 2011)

Truman E.M. & Reuter P.*, Chasing Dirty Money* (1st ed., Peterson Institute, Washington 2004)

European Union documents and papers

Proposal for a Council Directive (EC) 2013/0025 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing [2013]

Guidelines

'Chargeback Management Guidelines for Visa Merchants' (*Visa*, 2014) <http://usa.visa.com/download/merchants/chargeback-management-guidelines-for-visa-merchants.pdf> accessed 11 January 2015

'Legal Tender Guidelines' (*British Royal Mint* website) <http://www.royalmint.com/aboutus/policies-and-guidelines/legal-tender-guidelines> accessed 21 February 2015

Journals

Subramanian D.K., 'Digital Currency' [2013] FF 2, 6

Miscellaneous

'Revision of the FATF recommendations, 2012', FATF <http://www.fatf-gafi.org/media/fatf/documents/Press%20handout%20FATF%20Recommendations%202012.pdf> accessed 20 January 2015

FATF, *IX Special Recommendations* (October 2001) <http://www.fatf-gafi.org/topics/fatfrecommendations/documents/ixspecialrecommendations.html> accessed 20 January 2015

Financial Action Task Force, *The Forty Recommendations* (20 June 2003) < http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202003.pdf> accessed 20 January 2015

New York State Department of Financial Services, Proposed Amendments to Title 23, Chapter 1 (2015)

Sealed Complaint 13 MAG 2328, *United States of America vs. Ross William Ulbricht, aka "Dread Pirate Roberts", aka "DPR", aka "Silk Road"*, Southern District of New York Court, filed on 27 September 2013

Sealed Indictment, *United States of America v. E-Gold Ltd, Gold & Silver Reserve, Inc., Douglas L. Jackson, Barry K. Downey, and Reid A. Jackson*, United States District Court for the District of Columbia, filed in open court on 24 April 2007

Sealed Indictment, *United States of America v. Liberty Reserve S.A., Arthur Budovsky a/k/a "Arthur Belanchuk" a/k/a "Eric Paltz", Vladimir Kats a/k/a "Ragnar, Ahmed Yassine Abdelghani a/k/a Alex, Allan Esteban Hidalgo Jimenez a/k/a Allan Garcia, Azzeddine El Amine, Mark Marmilev a/k/a "Marko", and Maxim Chukharev*, United States District Court for the Southern District of New York, Indictment filed in open court on 28 May 2013

Sealed Complaint, *United States of America v. Robert M. Faiella, a/k/a "BTCKing", and Charlie Shrem*, United States District Court for the Southern District of New York, Sealed Complaint filed on 24 January 2013

Press releases

U.S. Department of Justice, 'Manhattan U.S. Attorney Announces Charges Against Liberty Reserve, One Of World's Largest Digital Currency Companies, And Seven Of Its Principals And Employees For Allegedly Running A $6 Billion Money Laundering Scheme' (*Press Release by the U.S. Department of Justice*, 28 May 2013) <http://www.justice.gov/usao/nys/pressreleases/May13/LibertyReservePR.php?print=1> accessed 2 March 2015

Reports

Consultative Group Assisting the Poor, *Financial Access Report 2009 – Measuring Access to Financial Services Around the World* (2009) MONEYVAL, *Report on Fourth Assessment Visit – Executive Summary* (2012)

Demirguc-Kunt A. & Klapper L., 'Measuring financial inclusion: the Global Findex Database, Volume 1' (*The World Bank*, 19 April 2012) <http://www-wds.worldbank.org/external/default/WDSContentServer/IW3P/IB/2012/04/19/000158349_20120419083611/Rendered/PDF/WPS6025.pdf> accessed 4 November 2014

MONEYVAL, *Report on Fourth Assessment Visit – Executive Summary* (2012) <http://www.coe.int/t/dghl/monitoring/moneyval/Evaluations/round4/MLT4_MER_MONEYVAL%282012%293_en.pdf> accessed 2 February 2015

United Nations Office on Drugs and Crime, *Illicit money: how much is out there?* (2011) <http://www.unodc.org/unodc/en/frontpage/2011/October/illicit-money_-how-much-is-out-there.html> accessed 28 February 2015

Research papers, Documents, Theses, Committees and Opinions

Basel Committee, *Prevention of Criminal Use of the Banking System for the Purpose of Money-Laundering* (1988) <http://www.bis.org/publ/bcbsc137.pdf> accessed 14 January 2015

Dykstra J., *Seizing Electronic Evidence from Cloud Computing Environments*, (University of Maryland, Baltimore 2013) <http://www.csee.umbc.edu/~dykstra/Seizing-Electronic-Evidence-from-Cloud-Computing-Environments.pdf> accessed 30 March 2015, pg. 158

EBA Opinion EBA/op/2014/08 On Virtual Currencies [2014] <https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf> accessed 20 February 2015

European Central Bank, *Virtual Currency Schemes – a further analysis* (February 2015) <http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> accessed 21 February 2015

European Central Bank, *Virtual Currency Schemes* (October 2012) <http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> accessed 21 February 2015

FATF, *Virtual Currencies: Key definitions and Potential AML/CFT risks* (June 2014) <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 15 February 2015

FinCen, *Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform*, Letter nr. FIN-2014-R011 (27 October 2014) <http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R011.pdf> accessed 9 February 2015

HM Revenue and Customs, *Revenue and Customs Brief 9 (2014): Bitcoin and other cryptocurrencies*, 3 March 2014 <https://www.gov.uk/government/publications/revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies/revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies> accessed 6 February 2015

HM Treasury, *Digital currencies: response to the call for information* (2015) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf> accessed 31 March 2015

Mell P. & Grance T., 'The NIST definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology', National Institute of Standards and Technology Special Publication 800-145, 2011 <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf> accessed 30 March 2015

Senate Committee on Homeland Security and Governmental Affairs, *Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies* (2013)

User Agreements

PayPal User Agreement <https://www.paypal.com/mt/webapps/mpp/ua/useragreement-full#8> accessed 11 January 2015

Websites and blogs

'Data on the internet is permanent after 20 minutes' (*InfoSecurity*, 21 April 2011) <http://www.infosecurity-magazine.com/news/data-on-the-internet-is-permanent-after-20-minutes/> accessed 25 February 2015

'Definition of fiat money' (*Investopedia*) <http://www.investopedia.com/terms/f/fiatmoney.asp>

'Glossary' (*NXT Wiki*) <http://wiki.nxtcrypto.org/wiki/Glossary#Asset> accessed 13 March 2015

'How Feedback works' (*eBay*) <http://pages.ebay.com/help/feedback/howitworks.html> accessed 13 March 2015

'Organisational Chart' (*FIAU* website) <http://www.fiumalta.org/about/organisational-chart> accessed 1 April 2015

'Protect your privacy' (*Bitcoin.org*) <https://bitcoin.org/en/protect-your-privacy> accessed 14 March 2015

'Shop with Points' (*Amazon* website) < http://www.amazon.com/b?node=2634438011> accessed 29 October 2014

'Will Bitcoin Tumbling Be Outlawed By The State?' (*BTCfeed*) <http://www.btcfeed.net/news/bitcoin-fog-tumbling-accepted-bitcoin-community/> accessed 1 April 2015

"Spook-1690" [PayPal account moniker], 'How long does it take for payment to clear?' (*PayPal,* 7 November 2011) <https://www.paypal-community.com/t5/Selling-on-eBay/how-long-does-it-take-for-payment-to-clear/td-p/372826?profile.language=en-gb> accessed 11 January 2015

"What does a Verified account status mean?" (*PayPal*) <https://www.paypal.com/us/webapps/helpcenter/helphub/article/?solutionId=FAQ1014&topicID=ACCOUNT_TYPES_US&m=TCI> accessed 2 March 2015

About Us (*PayPal)* <https://www.paypal.com/mt/webapps/mpp/about> accessed 2 March 2015

About Us, FATF website <http://www.fatf-gafi.org/pages/aboutus/> accessed 20 January 2015

Bitcoin Foundation website <http://bitcoinfoundation.org/> accessed 14 March 2015

Bitcoin Rich List <http://bitcoinrichlist.com/top100> accessed 13 March 2015

BTC Blockchain <https://blockchain.info/> accessed 14 March 2015

Buterin V., 'Ethereum: A Next-Generation Generalized Smart Contract and Decentralized Application Platform' (*VButerin,* 2014) <http://vbuterin.com/ethereum.html> accessed 13 January 2015

Coin.co website <https://coin.co/> accessed 1 April 2015

Coinmarketcap <<http://coinmarketcap.com/#EUR> accessed various times

Eurostat, 'Monthly minimum wages - bi-annual data' (*Eurostat* website) <http://ec.europa.eu/eurostat/en/web/products-datasets/-/EARN_MW_CUR> accessed 2 April 2015

Liu A., 'Why Bitcoins are just like Gold' (*Motherboard,* 21 March 2013) <http://motherboard.vice.com/blog/why-bitcoins-are-just-like-gold> accessed 20 September 2014

Nakamoto S., 'Bitcoin: A Peer-to-Peer Electronic Cash System' (*Bitcoin.org* 2009) <http://bitcoin.org/bitcoin.pdf> accessed 8 August 2013

Nxt website <http://nxt.org/> accessed 13 March 2015

Yunting Y., 'How the Chinese Government Regulates Risk Prevention for Bitcoin Transactions' (DeBund Law Office, 2015) <http://www.debund.com/info/eee3f9062e22495c96dc12881bb0b125> accessed 7 February 2015

COPYRIGHT RELEASE FORM

I, the undersigned, hereby authorise the Faculty Officer of the Faculty of Laws and his or her staff, the Faculty of Laws Librarian and his or her staff and academic members of staff of the Faculty of Laws to make photocopies or electronic copies of my thesis or parts thereof for education and study purposes and to make my thesis available for inspection and lending at the Faculty of Laws Library. I agree that in such cases I would not be entitled to receive any form of remuneration and that the final version of the hardbound and electronic copies of the theses submitted for examination become the property of the University.

Date of submission of final copy: *9th July 2015*

Signed:

Jonathan Galea