# Keeping Bitcoin Clean:
## Anti-Money Laundering Tools for the EU

**Vivian F. Magno**
**(ANR 291948)**

**Master's Thesis**

**Submitted in partial fulfilment**
**of the requirements for the degree of**
**LLM Law and Technology**

**TILBURG UNIVERSITY**
**Tilburg Law School**
**Tilburg Institute for Law, Technology, and Society (TILT)**

# TABLE OF CONTENTS

# CHAPTER 1. Introduction

In January 2014, criminal charges for money laundering were filed against one of the most famous faces in the bitcoin community before the federal court in New York.[1] Charlie Shrem, a young bitcoin promoter, millionaire[2] and owner of BitInstant, a bitcoin exchange company,[3] of which he was also Chief Executive Officer and Compliance Officer, was charged together with Robert Faiella, an "underground Bitcoin exchanger,"[4] for conspiring and knowingly selling more than US$1 million in Bitcoins to users of Silk Road.[5] Each of them was charged with money laundering conspiracy and operating and unlicensed money transmitting business. Shrem was further charged with wilful failure to file a suspicious activity report.[6]

One month following the arrest of Shrem, in February 2014, criminal charges were filed against the creator of Silk Road, Ross Ulbricht, in a Manhattan court[7] for narcotics trafficking conspiracy, operating a continuing criminal enterprise, computer hacking conspiracy and money laundering conspiracy, for operations conducted during the period from January 2011 to October 2013.[8] According to the indictment, the Silk Road website was the most sophisticated and prolific criminal marketplace online where thousands of drug dealers and vendors of illegal products and services were offered for sale, creating opportunities to launder the proceeds of illegal activities.[9] Silk Road used bitcoins as the exclusive means of payment.[10]

---

"Manhattan U.S. Attorney Announces Charges Against Bitcoin Exchangers, Including CEO Of Bitcoin Exchange Company, For Scheme To Sell And Launder Over $1 Million In Bitcoins Related To Silk Road Drug Trafficking" (*US DOJ,* 27 January 2014) <http://www.justice.gov/usao/nys/pressreleases/January14/SchremFaiellaChargesPR.php> accessed 29 July 2014

2 Kim Lachance Shandrow, "Bitcoin Millionaire Charlie Shrem Under House Arrest Following Federal Indictment" *Entrepreneur* (California, 15 April 2014) <http://www.entrepreneur.com/article/233107> accessed 29 July 2014

3 Jose Pagliery, "Bitcoin exchange CEO arrested for money laundering" *CNN* (US, 28 January 2014) <http://money.cnn.com/2014/01/27/technology/security/bitcoin-arrest/ > accessed 29 July 2014

4 "Manhattan U.S. Attorney Announces Charges Against Bitcoin Exchangers, Including CEO Of Bitcoin Exchange Company, For Scheme To Sell And Launder Over $1 Million In Bitcoins Related To Silk Road Drug Trafficking" (n1) <http://www.justice.gov/usao/nys/pressreleases/January14/SchremFaiellaChargesPR.php> accessed 29 July 2014

5 US v Faeilla and Shrem (Indictment before the United States Magistrate Judge Southern District of New York) Violations of 18 U.S.C. §§ 1950 and 1956; 31 U.S.C. §§ 5318 (g) and 5322 (a) [page 2] <http://www.justice.gov/usao/nys/pressreleases/January14/SchremFaiellaChargesPR/Faiella,%20Robert%20M.%20and%20Charlie%20Shrem%20Complaint.pdf> accessed 29 July 2014

6 Ibid

7 Andy Greenberg, "Alleged Silk Road Creator Ross Ulbricht Pleads not Guilty on all Charges" *Forbes* (New York, 02 July 2014) <*http://www.forbes.com/sites/andygreenberg/2014/02/07/alleged-silk-road-creator-ross-ulbricht-pleads-not-guilty-on-all-charges/*> accessed 29 July 2014

8 US v Ross Ulbricht (Indictment before the United States District Court Southern District of New York) 14 Crim 068 <http://www.justice.gov/usao/nys/pressreleases/February14/RossUlbrichtIndictmentPR/US%20v.%20Ross%20Ulbricht%20Indictment.pdf> accessed 29 July 2014.
The Silk Road website was shut down by law enforcement authorities in October 2013.

9 Ibid

10 Andy Greenberg, "Alleged Silk Road Creator's Lawyer Denies Bitcoin is Monetary Instrument Moves to Drop all Charges" *Forbes* (New York, 04 January 2014) <http://www.forbes.com/sites/andygreenberg/2014/04/01/alleged-silk-road-creators-lawyer-denies-bitcoin-is-monetary-instrument-moves-to-drop-all-charges/> accessed 29 July 2014

Interestingly, one of the defences of Ulbricht against the money laundering charge is that "[b]itcoins, do not qualify as 'monetary instruments,' and therefore cannot serve as the basis for a money laundering violation,"[11] an argument that was roundly rejected by the court.[12]

In Florida, police arrested Pascal Reid and Michell Espinoza in February 2014 during an entrapment proceeding where undercover agents posed as credit card thieves who purportedly wanted to buy bitcoins with cash supposedly generated by the hacking of Target Corp. customer information. [13] News reports say that this case marked the first time money laundering charges involving bitcoins are brought by a state. Again, one of the defences raised by defendants' lawyers is that current state legislation on money laundering contemplates only government-issued currency and does not apply to bitcoins. [14]

Notably, all these cases occurred in 2014, within a month of each other. Of these, the indictment and arrest of Shrem, the "newest boy wonder" of the New York technology scene, has focused the attention of the global public on the most popular digital currency at the moment, the bitcoin. These developments also stoke fears in regulators and other stakeholders all over the world that the bitcoin network is being used as a haven for money launderers.[15]

The Financial Action Task Force (FATF), in its report released in June 2014, echoes the sentiment of most regulatory bodies that while bitcoins offer many potential benefits, the intrinsic nature of the bitcoin system allowing a certain degree of anonymity in transactions also brings with it anti-money laundering (AML) risks. [16] A paper submitted to the Organization for Economic Cooperation and Development (OECD) agrees with this view, and states that "the anonymity features of the crypto-currencies [such as bitcoin]...facilitate money laundering."[17]

In the European Union, bitcoin is unregulated, nor has been there any specific legislation to address the status of bitcoin as a currency, although some jurisdictions, like Germany, have

---

11 Ibid

12 Stan Higgins, "Ross Ulbricht Loses Bid to Dismiss Federal Silk Road Suit" (*Coindesk,* 10 July 2014) <http://www.coindesk.com/ross-ulbricht-loses-bid-dismiss-federal-silk-road-suit/> accessed 29 July 2014

13 Curt Anderson, "US Bitcoin Case tests Money Laundering Limits"*3news.co.nz* (New Zealand, 10 April 2014) <http://www.3news.co.nz/US-bitcoin-case-tests-money-laundering-limits/tabid/417/articleID/339614/Default.aspx> accessed 29 July 2014

14 Susannah Nesmith, " Bitcoin Charges Improper under Florida Law Lawyer Says" *Bloomberg* (New York, 28 February 2014) <http://www.bloomberg.com/news/2014-02-27/bitcoin-charges-improper-under-florida-law-lawyer-says.html> accessed 29 July 2014

15 Kim Zetter, "FBI Fears Bitcoin's Popularity with Criminals" *Wired* (05 September 2012, California) <http://www.wired.com/2012/05/fbi-fears-bitcoin/ > accessed 30 July 2014

16 "Virtual Currencies: Key Definitions and Potential AML/CFT Risks" (*FATF)* <http://www.fatf-gafi.org/topics/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html > accessed 12 August 2014

17 A. Blundell-Wignall, (2014), "The Bitcoin Question: Currency versus Trust-less Transfer Technology", *OECD Working Papers on Finance, Insurance and Private Pensions*, No. 37, OECD Publishing <http://www.oecd-ilibrary.org/content/workingpaper/5jz2pwjd9t20-en > accessed 12 August 2014

recognized bitcoins as legally binding financial instruments.[18] The European Banking Authority (EBA) has been keeping a watchful eye on global developments on bitcoin and other virtual currencies, and on 12 December 2013, it issued a public warning alerting consumers on the risks of losing their money when using virtual currencies as a means of payment and the potential for the abuse of bitcoins for criminal purposes.[19]

On 04 July 2014, the EBA issued an Opinion addressed to EU legislators on virtual currencies identifying more than seventy (70) risks associated with the use of virtual currencies. The Opinion identified the causal drivers of these risks, and proposed long-term and short-term regulatory approaches to address these causal drivers. [20] The European Commission is poised to heed the EBA's warnings and signalled "it will try to impose rules on virtual currencies such as Bitcoin." [21]

The bitcoin, wide and constantly changing, is composed of various participants. These participants include, among others, users, miners, bitcoin exchanges, merchants, trade platforms, processing service providers, wallet providers, inventors, and technical service providers.[22] BitInstant, owned by Shrem, is one of such bitcoin exchanges, the business of which is to engage in the exchange of bitcoins for real currency or other virtual currencies.[23] Software developers also play a part in the bitcoin ecosystem.[24] This list of bitcoin participants is far from exhaustive in view of rapidly developing technologies in the bitcoin system. [25]

Most money laundering risks attach to participants that deal with or facilitate an interaction between fiat currency and bitcoin, and in transactions involving an exchange of goods and services for fiat currency or bitcoin. Of the aforementioned participants in the bitcoin ecosystem, money laundering risks are pervasive in transactions made by users and bitcoin exchanges.

---

18 "Regulation of Bitcoin in Selected Jurisdictions" (*US Library of Congress)* <http://www.loc.gov/law/help/bitcoin-survey/#denmark> accessed 07 October 2014

19 "Warning to Consumers on Virtual Currencies 12 December 2013" EBA/WRG/2013/01 (*EBA*) <http://www.eba.europa.eu/documents/10180/598344/EBA+Warning+on+Virtual+Currencies.pdf> accessed 07 October 2014

20 "EBA Opinion on Virtual Currencies 04 July 2014" (EBA/Op/2014/08) (*EBA*) <http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf> accessed 07 October 2014

21 Ben Moshinsky and Jim Brunsden, "Bitcoin faces regulatory backlash as EU tells banks to stay away" *Bloomberg* (New York, 04 July 2014) <http://www.bloomberg.com/news/2014-07-04/bitcoin-faces-regulatory-backlash-as-eu-tells-banks-to-stay-away.html> accessed 07 October 2014

22 "EBA Opinion on Virtual Currencies dated 04 July 2014" (EBA/Op/2014/08) (n20) 13

23 "FATF Report 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 12 August 2014

24 "FATF Report Virtual Currencies Key Definitions and Potential AML/CFT Risks" (June 2014) (n23) 8

25 Ibid

This thesis proposes to answer the following question:

"How effective are the proposed EU money laundering regulations on bitcoins?"

This central research question is divided into the following three (3) sub-questions, each of which will be discussed in separate chapters (Chapters 2 to 4):

1. What are bitcoins? What is the legal status of bitcoins in the EU?
2. What are the principles and rules of anti-money laundering and how are bitcoins used or can be potentially used for money laundering?
3. How effective are the EBA regulatory proposals in preventing money laundering in relation to bitcoin?

## *1.1 Significance of the Research*

That the three (3) cases mentioned above all happened within the span of less than a year illustrates that the bitcoin system is increasingly becoming vulnerable to abuse by criminal elements to launder illegal profits. Countries have responded in different ways to the threat. Some jurisdictions have stepped up their AML rules, while the EU has yet to develop its AML framework despite an observed increase in the use of bitcoin use both as an investment and a means of payment across EU Member States.[26] This process is now jumpstarted by the issuance of the EBA of its Opinion dated 04 July 2014. The bitcoin market has also increased ever since the introduction of bitcoins in 2009. As of 28 October 2014, approximately 13,433,575 bitcoins have been mined, with a market capitalization of around 3,774,834,575 EUR.[27] Given the rising popularity of bitcoins and its susceptibility to abuse, AML regulation has become imperative. This thesis is the first systematic study on the effectiveness of the proposed AML regulations of the EU which will hopefully provide helpful guidance and lessons.

## *1.2 Methodology*

Considering the recent development of bitcoin, most of the literature search for this thesis is available online. Resources included online articles, journals, news articles, books, and blogs. An effort was made to select the most up-to-date materials and to verify the contents of these materials by referring to various other internet sources.

26 "EBA Opinion on Virtual Currencies 04 July 2014" (EBA/Op/2014/08) (n20) 7

27 See <https://blockchain.info/charts/total-bitcoins> accessed 28 October 2014

# CHAPTER 2. A Technical and Legal Background on Bitcoins

> "What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers."[28] (underscoring mine)
>
> - Satoshi Nakamoto, "Bitcoin, a Peer-to-Peer Electronic Cash System"

## *2.1 What are bitcoins?*

It is not exactly known who created the bitcoin system. Some believe it is a real person by the name of Satoshi Nakamoto,[29] while others believe that this is just a pseudonym.[30] Nonetheless, the white paper entitled "Bitcoin, a Peer-to-Peer Electronic Cash System" authored by Satoshi Nakamoto describes how the bitcoin system works.

A bitcoin is a cryptocurrency or a digital currency that is created and held electronically.[31] It is not printed, unlike conventional currency, but "mined" through the use of a "widely distributed computing power."[32] It is not issued by any government but is created using peer-to-peer (P2P) technology without any central authority. This means that transactions are managed and currency is issued, collectively in the bitcoin network.[33]

A bitcoin is not represented by a tangible physical object that can be exchanged for goods or services. Instead, it is a computer file, similar to a music or a text file, and consequently, it can be lost or destroyed just like any computer file. They can be stored either on a personal computer or entrusted for safekeeping to an online service. Each bitcoin may be subdivided into 100 million smaller units called satoshis, defined by eight decimal places.[34]

---

28 Satoshi Nakamoto, "Bitcoin: a Peer-to-Peer Electronic Cash System" 1 <https://bitcoin.org/bitcoin.pdf> accessed 12 August 2014

29 "Bitcoin Frequently Asked Questions" (*Bitcoin.org)* <https://bitcoin.org/en/faq#who-created-bitcoin> accessed 12 August 2014

30 Joshua Brustein, "Is this the man who created bitcoin?" *Businessweek* (United States, 06 March 2014) <http://www.businessweek.com/articles/2014-03-06/is-this-the-man-who-created-bitcoin> accessed 12 August 2014

31 "What is bitcoin?" *Coindesk* (UK) <http://www.coindesk.com/information/what-is-bitcoin/> accessed 30 July 2014

32 Danny Bradbury, "The problem with bitcoin" Volume 2013 Computer Fraud & Security 11 <http://www.sciencedirect.com/science/article/pii/S1361372313701015> accessed 06 August 2014

33 "Bitcoin" (*Bitcoinwiki)* <https://en.bitcoin.it/wiki/Main_Page> accessed 30 July 2014

34 Rhys Bollen, "The Legal Status of Online Currencies: Are bitcoins the future" (Journal of Banking and Finance

The entire bitcoin system is a peer-to-peer software system, similar to the networks that are used for BitTorrent, a file-sharing system, and Skype, an audio, video and chat service.[35] In practical terms, this means that the entire bitcoin system is composed of software versions of the bitcoin client program[36] that users download and run on their computers. There is no central administrator, nor a bitcoin server or a bitcoin company that administers or manages the system. This is the core design of bitcoin as envisioned by its creator/s. Bitcoin operates using a cryptographic proof system, which allows users to deal directly with one another without needing a third party to authorize the transaction.[37]

This decentralization stems from the desire to avoid a trusted third party, "that is, an authority, above reproach, that can inform others of the canonical state of the system." [38] Indeed, bitcoin transactions "occur without the presence of a government, bank, payment network, regulator, or other third party entity." [39] According to the bitcoin creators, the root problem with conventional currency is the requirement of trust needed to make electronic payments work. To make the traditional system work, privacy had to be sacrificed by trusting banks to protect information. Massive overhead costs likewise make micropayments impossible.[40]

Like any other traditional currency, bitcoins fluctuate in value in relation to other currencies, hence, its value is constantly changing. Unlike traditional currencies, however, no centralised bank prints the currency and sets relative values for the currency.[41] Transactions determine the value of bitcoin through supply and demand.[42]

---

Law and Practice [2013]) 4 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2285247&download=yes> accessed 31 July 2014

35 Bollen (n34) 3

36 "Bitcoin" (*P2P Foundation)* <http://p2pfoundation.net/bitcoin> accessed 30 July 2014

37 Nakamoto (n28) 1

38 Shawn Bayern, "Of Bitcoins, Independently Wealthy Software, and the Zero-Member LLC" *(*108 Nw. U. L. Rev. Online 257 (2014) ; FSU College of Law, Public Law Research Paper No. 675 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2366197&download=yes> accessed 30 July 2014

39 Nicholas Plassaras, "Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF" (Chicago Journal of International Law, 14 Chi J Intl L [2013] Forthcoming) 6 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2248419&download=yes> accessed 30 July 2014

40 "Bitcoin" (n36). See also Nakamoto (n28)

41 Raghu Kumar, "Bitcoin explained in layman's terms" *NDTV Profit* (India, 27 December 2013) <http://profit.ndtv.com/news/your-money/article-bitcoin-explained-in-laymans-terms-376029> accessed 12 August 2014

42 "Bitcoin frequently asked questions" (*Bitcoin.org*) <https://bitcoin.org/en/faq#what-determines-bitcoins-price> accessed 12 August 2014

## 2.2 Who uses bitcoins and for what purposes?

At the moment, bitcoins can be spent on goods or services either online or in the real world. They are spent by sending them from one user to another, much like sending an email.[43] Additionally, some organizations accept bitcoins as donations, including political candidates[44] and political or non-profit organizations[45] like Wikileaks that prefer to keep their donations private. For instance, supporters of Wikileaks[46] who are apprehensive about being publicly linked to the organization can offer their support through bitcoins.

Despite the fact that a record of every bitcoin transaction is stored on every user's computer to prevent digital counterfeiting, bitcoin transactions offer a certain degree of anonymity and for this reason is a preferred method of transferring funds. Regulators around the world have recognized that this high degree of anonymity is what attracts criminal elements to use bitcoins[47] to launder criminal proceeds.

## 2.3 What makes bitcoins popular?

Bitcoins have gained popularity among its supporters because it offers the following advantages over conventional currency:

First of all, the use of digital currency like bitcoin creates significant economic benefits as the costs that are associated with the production, transportation, and handling of physical currency are taken away from the equation.[48]

Secondly, the transaction fees associated with bitcoin transactions, if any, are very low.[49] Most

---

43 Plassaras (n39) 6

44 Leilei Huang, "More Political Candidates Accepting Bitcoin Donations" (*Bitcoin Vox,* 5 August 2014) <http://bitcoinvox.com/article/905/more-political-candidates-accepting-bitcoin-donations> 12 August 2014

45 Lalita Clozel, "FEC allows political groups to accept bitcoin donations" *LA Times* (US, 8 May 2014) <http://www.latimes.com/nation/politics/politicsnow/la-pn-fec-political-action-committees-bitcoins-20140508-story.html > accessed 12 August 2014

46 Paul Quintaro, "Why Julian Assange of Wikileaks loves bitcoins" (*Benzinga,* 15 June 2011) <http://www.benzinga.com/general/politics/11/06/1172451/why-julian-assange-of-wikileaks-loves-bitcoin#ixzz38xFgNVnQ> accessed 31 July 2014

47 Jim Bronskill, "Bitcoin's anonymity makes it ripe for crime: finance department memo" *Huffington Post* (US, 28 July 2014) <http://www.huffingtonpost.ca/2014/07/28/bitcoin-anonymity-crime-finance-dept_n_5628126.html> accessed 31 July 2014

48 Plassaras (n39) 9

49 Jerry Brito, Andrea Castillo, Bitcoin: A Primer for Policymakers (2012, Mercatus Center) 10 <http://books.google.nl/books?id=yC-nAwAAQBAJ&pg=PA26&lpg=PA26&dq=liberty+reserve+centralized&source=bl&ots=b3tOD-eOMD&sig=EWa3nyR3PGlB_SQGfETyd8tJeo0&hl=nl&sa=X&ei=9GEAVIPvCObI0QXerIHIBg&ved=0CEYQ6AEwBA#v=onepage&q=liberty%20reserve%20centralized&f=false> accessed 03 September 2014

transactions at the moment are processed without need to pay transaction fees. However, transactions that have a large data size usually are processed after payment of a small transaction fee.[50] These fees are usually used as a protection to prevent users from overloading the network with transactions. According to studies, the fee is not actually related to the amount of bitcoins being sent in one transaction but to the aggregate number of transactions that are being sent to the network. For example, for a 1,000 BTC transfer, the transfer fee may be 0.0005 BTC, and for a 0.02 BTC payment, the transfer fee may be 0.004 BTC. When fee is required, it is usually worth less than 40 US cents.[51] As a rule, the fees for sending a large number of tiny amounts is larger than for sending one or several transactions with higher amounts. Hence, the fee is determined by "attributes such as data in transaction and transaction recurrence." [52]

These fees go to the miners to incentivise them to keep mining, which in turn keeps the bitcoin network secure.[53] Mining is the processing of transactions in the digital currency system, in which the records of current bitcoin transactions, known as a blocks, are added to the record of past transactions, known as the block chain. Mining will be discussed in detail later.[54]

Third, the use of bitcoins also spells less risk for merchants because bitcoin transactions are relatively secure, are irreversible, and do not contain sensitive or personal information of customers. Hence, merchants can easily expand to markets where either credit card use is not available or fraud rates are unacceptably high.[55]

Fourth, bitcoin use affords users some degree of security and control over their transactions and makes it impossible for merchants to force unnoticed charges as can happen with other payment methods such as credit cards. Moreover, the fact that no personal information is required for bitcoin transactions offers strong protection against identity theft.[56]

Moreover, users are attracted to bitcoins because of the relative "anonymity" and the transparency of the bitcoin network. All bitcoin transactions as well as information concerning the bitcoin money supply itself are all published on the block chain for anybody to check and verify and use in real time.[57] It is important to note that in the bitcoin system, the trail of all transactions from all accounts could be seen and traced, but there is nothing that links account

---

50 "Transaction Fees" (*Bitcoin wiki)* <https://en.bitcoin.it/wiki/Transaction_fees > accessed 01 August 2014

51 "Bitcoin transaction fees explained" (*Bitcoinfees.com)* <http://bitcoinfees.com/> accessed 01 August 2014

52 Ibid

53 Ibid

54 "Bitcoin mining" (*Whatis.techtartget.com)* <http://whatis.techtarget.com/definition/Bitcoin-mining > accessed 01 August 2014

55 "Advantages/Disadvantages" (*bitcoinembassy.ca* ) <http://bitcoinembassy.ca/about/what-is-bitcoin/advantages-disadvantages> accessed 01 August 2014

56 Ibid

57 Ibid

to the identities of individual holders.[58] The block chain shows only the **transaction ID and the amount of currency transferred**. There is relative anonymity in the bitcoin system because personal details like name, address, email, phone number are not required.[59] Under the current bitcoin system therefore, without using anonymization software, transactions are relatively anonymous or more aptly, "pseudonymous." On the other hand, payment systems like Paypal require all these personal details. [60]

Finally, the bitcoin system at present, is cryptographically secure inasmuch and there is no individual or organization that can control or manipulate the bitcoin protocol.[61] It was designed in such a way that for an individual or organization to gain control or manipulate data or transactions, he or it must have control over 51% of the hash rate which makes it possible to execute a denial of service or to double spend since the party is controlling more than half of the mining.[62]

## *2.4 How are bitcoins obtained?*

Bitcoins can be obtained in various ways. First, through bitcoin exchanges or other trading platforms, users can purchase bitcoins in exchange for real currency like dollars or euros,[63] other digital currencies.[64] BitInstant, owned by Shrem, was one of such exchange but it has temporarily closed shop based on a news report as of July 2013.[65] Another bitcoin exchange is Mt. Gox, based in Tokyo, one of the biggest during its time, but which fell into bankruptcy after hackers broke into the system and stole 850,000 bitcoins[66] or US$ 460 Million. [67]

---

58 Reuben Grinberg, "Bitcoin: An Innovative Alternative Digital Currency" (4 Hastings Science & Technology Law Journal 162-165 ) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1817857&download=yes> accessed 01 August 2014

59 Ashutosh KS, "10 Things you need to know about bitcoins" (*hongkiat.com)* <http://www.hongkiat.com/blog/bitcoin-questions/ > accessed 07 August 2014

60 Ibid

61 "Advantages/Disadvantages" (n55 )

62 Mick Ayzenberg, Adam Cecchetti, Akshay Aggarwal, "A Security Analysis of the Bitcoin Mining System" <http://static.squarespace.com/static/53168f6ce4b0ee73efea0c2a/t/53c5cc86e4b0cf6b53648339/1405471878208/Bitcoin%20Mining%20Security-%20Deja%20vu%20Security%20-%202014.pdf > accessed 01 August 2014

63 Plassaras (n39) 8

64 "Complete List of Bitcoin Exchanges" *(Planetbtc.com) <http://planetbtc.com/complete-list-of-bitcoin-exchanges/*> accessed 02 August 2014

65 David Gilson, "BitInstant temporarily shuts down service to work on next upgrade" *Coindesk* (UK, 13 July 2013) <http://www.coindesk.com/bitinstant-temporarily-shuts-down-service-to-work-on-next-upgrade/ > accessed 02 August 2014

66 James Lyne, "$116 Million Bitcoins 'Found' At Mt. Gox And How To Protect Your Wallet" *Forbes* (US, 21 March 2014) <http://www.forbes.com/sites/jameslyne/2014/03/21/116-million-bitcoins-found-at-mtgox-and-how-to-protect-your-wallet/ > accessed 12 August 2014

67 Robert Mcmillan, "The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster" *Wired* (California, 03 March 1014) <http://www.wired.com/2014/03/bitcoin-exchange/> accessed 12 August 2014

Second, bitcoins can be exchanged for goods or services.[68] Plenty of online shops accept bitcoins as payment, including overstock.com,[69] as well various brick–and-mortar shops.

Lastly, bitcoins can be obtained through a process called "mining." Mining is a process of generating bitcoins. Bitcoins are mined by users by essentially using their computer's processing power or even that of computer networks to solve complicated computer algorithms, all for the purpose of verifying or settling bitcoins transactions. [70] Approximately every ten minutes, bitcoins are awarded to whichever miner completed a "proof-of-work" or from an accounting perspective, "balanced the books."[71]

The maximum number of bitcoins in circulation is finite. When the algorithm was created, the creator(s) set a definite limit on the number of bitcoins that will ever exist – 21 million. As of January 2014, more than 12 million bitcoins are in circulation, leaving only around less than 9 million bitcoins to be mined.[72] The bitcoin system was set up in a way that mining coins was easy in the beginning, but becomes progressively harder until the 21 millionth bitcoin is reached. It has been predicted that the final bitcoin will be mined in 2140.[73]

Bitcoin mining is a difficult, arduous and time-consuming process. To illustrate the difficulty of mining bitcoins, it has been described that a typical office computer would have to be running nonstop for approximately five to ten years to be able to mine any bitcoin. The value of bitcoins generated would be outweighed by the cost of electricity used in mining the bitcoin. Currently, the reward for solving the mining algorithm is 25 bitcoins.[74]

## *2.5 How are transactions verified in a decentralized bitcoin system?*

Let's say, Juan buys a laptop from Pedro using bitcoins. In order to make sure that Juan's bitcoin is authentic, miners perform complicated processes using their computers to make sure Juan's bitcoin is genuine. This is the process of mining.

68 Plassaras (n39) 8
69 See <http://www.overstock.com/bitcoin > accessed 02 August 2014
70 Plassaras (n39) 8
71 "Proof of work," <https://en.bitcoin.it/wiki/Proof_of_work> accessed 19 December 2014
72 Anthony Volastro, "CNBC Explains: How to mine bitcoins on your own" *CNBC* (US, 23 January 2014) <http://www.cnbc.com/id/101332124#> accessed 02 August 2014
73 "How bitcoin mining works" *Coindesk* (UK) <http://www.coindesk.com/information/how-bitcoin-mining-works/> accessed 02 August 2014
74 Volastro (n72)

### *2.5.1 The problem of double spending*

Since a bitcoin is a computer file or digital data, there is the problem of making copies of the file or digital data and use these files as many times as one would like for separate and different transactions.

In the example above, Juan may have made digital copies of the computer files representing his 10 bitcoins, then transferred these 10 bitcoins to Sancho on day 1 for a travel voucher, and, again transferred a copy of the same files to Pedro on day 2 for a laptop. Hence, for one bitcoin, it is possible that copies are reproduced and used in as many transactions as desired. This is called double-spending.

The problem of double spending was solved by the creators of bitcoin by broadcasting all transactions in a public ledger or list, called the **block chain**. In essence, the validity of a transaction is checked by verifying against the public ledger, or the blockchain, that the bitcoin involved in the transaction was not previously used, through the process of mining. This system prevents the double use or double spending of the bitcoin.[75]

The blockchain is practically a record of every transaction and of information on the ownership of every single bitcoin. [76] All transactions are verified by miners who constantly verify transaction blocks to ensure that all information is correct and update the blockchain each time a transaction is verified. In short miners "confirm transactions,"[77] and for their work, are paid an incentive of 25 bitcoins.

### *2.5.2 Mining*

In order to preserve the integrity and authenticity of the block chain and prevent it from being tampered with, miners perform complicated processes to confirm the transactions using basic software and, for faster and more intensive mining, specialized hardware. This software is open source and is straightforward.[78]

The process of transferring bitcoins takes place by sending bitcoins from one bitcoin address to another. These addresses are long, alphanumeric strings understood by the bitcoin network. [79] The bitcoin network processes these transactions by collecting transactions that occur within a set period into a list, called a **block**.[80] When a miner creates a block, it is broadcasted to the bitcoin network, after which each bitcoin user would confirm the validity of the block and

75 Ashutosh (n59)
76 Kumar (n41)
77 Ibid
78 Volastro (n72)
79 Bradbury (n32)
80 "How bitcoin mining works"(n73)

thereafter add the block to the general ledger called the **block chain**.[81]

The block chain contains all transactions related to any bitcoin and can be used to explore and examine transactions between any bitcoin address, and at any point on the network. New blocks of transactions that are created are added to the block chain. This results in an increasingly long list of practically all the transactions that ever occurred on the bitcoin network. Users of the bitcoin network are constantly given updated copies of the block chain so they are aware of what is happening in the network,[82] although it has been noted that the block chain has been quite lengthy at this point that most modern bitcoin wallets don't contain the entire chain.[83]

Using mining software, miners take the information in the block and apply a mathematical formula or a cryptographic function, in effect, producing a digital signature for that block and creating a seal on it, preventing tampering.[84] The cryptographic function used by the bitcoin network is SHA-256[85] or Secure Hash Algorithm 256-bit which was developed by the United States National Security Agency.[86]

This cryptographic function turns the transaction into a hash, which is a shorter and random sequence of numbers. The hash is composed not only of the data in the transaction but also other pieces of information including the hash of the last block stored in the chain. The hash is stored along with the block, and is attached at the end of the block chain. The interesting thing about hashes is that while it is easy to produce a hash from a bitcoin block, it is impossible to determine what the underlying data of the transactions was just by looking at the hash.[87]

And because a particular block's hash contains the hash of the block before it, tampering with the hash of a block would alter the hash of the block after it, and the one after it, and so on.[88] Thus, it would be very time-consuming and practically impossible to tamper with the block chain because each block then becomes a "digital version of a wax seal."[89] It is a digital

81 Chris Pacia, "Bitcoin Mining explained like you're 5: Part 2 – Mechanics" <http://chrispacia.wordpress.com/2013/09/02/bitcoin-mining-explained-like-youre-five-part-2-mechanics/> accessed 06 August 2014

82 "How bitcoin mining works"(n73)

83 Paul Bischoff, "Pick up your pickaxes and headlamps: here's how Bitcoin mining works" *Techinasia.com* (21 July 2014) <http://www.techinasia.com/how-min-bitcoin-works-guide-tutorial/ > accessed 06 August 2014

84 Bradbury (n32)

85 "SHA-256 and Scrypt Mining Algorithms" (*coinpursuit.com)* <https://www.coinpursuit.com/pages/bitcoin-altcoin-SHA-256-scrypt-mining-algorithms/ > accessed 06 August 2014

86 Pacia (n81)

87 "How bitcoin mining works"(n73)

88 Ibid

89 Ibid

confirmation that the block concerned and the one after it is legitimate, and if a block is tampered with, it would be apparent and detectable.[90]

A valid block is produced after proof that a miner used a certain amount of processing power to create the block. Essentially this means that miners must submit an answer to a complicated mathematical problem that could be solved only by running random numbers through an equation many times over until the right answer is found. This mathematical problem is calibrated or adjusted in such a way that only a miner or a pool of miners could find the solution to the problem only once every ten minutes on average.[91]

## *2.6 What are the steps in a typical bitcoin process?*

In order to understand how money laundering occurs in a bitcoin transaction, it is important to explore the processes in a typical bitcoin transaction from the viewpoint of a typical user.

(1) Obtain a bitcoin wallet[92]

The first step in utilizing bitcoin is to obtain a bitcoin wallet. The bitcoin wallet is a virtual wallet, much like a physical wallet or even a bank account, that the user can use to store, transfer and receive bitcoin.[93] A bitcoin wallet can be established by downloading a software wallet, which is installed on the computer or a mobile device, or use a web wallet or hosted wallet hosted by a third party. A software wallet allows the user to have complete control over the security of the bitcoins, while a web wallet's security is in the hands of a provider which requires a degree of trust in the ability of the provider to provide the required level of security.[94] An example of a software wallet is Electrum, while Coinbase is an example of a web wallet. For more advanced users, Armory and Bitcoin-QT are examples of high-security software wallets.[95] There are other types of wallets like cold wallets, brain wallets and hard wallets.[96]

---

90 Ibid

91 Chris Pacia, "Bitcoin Mining explained like you're 5: Part 1 – Incentives" <http://chrispacia.wordpress.com/2013/09/02/bitcoin-mining-explained-like-youre-five-part-1-incentives/ > accessed on 06 August 2014.

92 "Getting started with bitcoin" (*bitcoin.org)* <https://bitcoin.org/en/getting-started > accessed 20 August 2014

93 To be technically accurate, however, bitcoins are actually stored on the blockchain. According to a news article, "Bitcoin wallets hold the private keys that give users the right to use those coins. Each Bitcoin wallet comes with at least two keys (multisig wallets can have more) one public, and one private. The public key lets any Bitcoin user send a sum of Bitcoins directly to any other Bitcoin user, without a middle man. The private key must be kept as secure as possible, since anyone who gets a hold of it has access to every Bitcoin associated with it." See <http://cointelegraph.com/news/111891/the-many-types-and-functions-of-bitcoin-wallets> accessed 20 August 2014

94 "How to set up a wallet" (*bitcoinsimplified.org*) <http://bitcoinsimplified.org/get-started/how-to-set-up-a-wallet/> accessed 20 August 2014

95 Ibid

96 See <http://cointelegraph.com/news/111891/the-many-types-and-functions-of-bitcoin-wallets> accessed 20

After downloading a wallet, the user will be assigned a bitcoin address which may look something like this -- 1GVA4cyUc7wXCu1nsN6TahVkMXE4vC1nGe. This address is akin to a bank account number which is safe to distribute and is where people send money.[97]

Users are allowed and are even encouraged to have as many bitcoin wallets on the bitcoin network. Multiple wallets provide anonymity to the user,[98] as well as minimize the losses a user may otherwise sustain if he maintained all his bitcoins in a single wallet. There are many documented cases of hacking incidents involving bitcoins.[99] One of these attacks involved Mt. Gox in June 2011 which resulted in the loss of 25,000 bitcoins through theft, with a value at that time of around US$8.75 million resulting in the precipitous drop in the value of the bitcoin from US$32.00 per bitcoin to mere pennies.[100] Much like any decrease in demand for bitcoins for whatever reason, attacks on the bitcoin system cause drops in the value of the bitcoin exchange rate. [101]

(2) Purchase bitcoin [102]

After establishing a wallet, the user is ready to purchase his first bitcoins. He may obtain bitcoins by selling goods or services and accepting bitcoins as payment, or by buying them from another person,[103] or by mining bitcoins.[104] For a new bitcoin user, however, the most common method of obtaining bitcoins is to purchase them directly from a bitcoin exchange. A bitcoin exchange is an intermediary that holds buyer's and seller's funds. A prospective seller places a "sell order" and a buyer places a "buy order" stating the amount and the type of currency and the price per unit each would want to sell/buy. When someone places a matching order, the order will facilitate or complete the transaction. Because a bitcoin exchange holds funds, it may take an inordinate amount of time to receive funds from a cash out transaction if the exchange faces liquidity problems.[105]

---

August 2014

97 Matthew Sparkes, "How to get your virtual hands on some bitcoins" *The Telegraph* (UK, 15 January 2014) <http://www.telegraph.co.uk/technology/news/10559175/How-to-get-your-virtual-hands-on-some-bitcoins.html> accessed 20 August 2014

98 "Anonymity" (*bitcoinsimplified.org*) <http://bitcoinsimplified.org/learn-more/anonymity/> accessed 20 August 2014

99 See <http://www.theguardian.com/technology/2014/mar/18/history-of-bitcoin-hacks-alternative-currency> accessed 20 August 2014

100 Ibid

101 Catherine Martin Christopher, "Whack-a-Mole: Why Prosecuting Digital Currency Exchanges won't Stop Online Money Laundering" (18 Lewis & Clark L. Rev. 1, 2014) 21 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312787&download=yes> accessed 04 September 2014

102 "Getting started with bitcoin" (n92)

103 "Getting started with bitcoin" (n92)

104 Volastro (n72)

105 "How to sell bitcoin" (*Coindesk)* <http://www.coindesk.com/information/sell-bitcoin/> accessed 05 November 2014

Some exchanges put up bitcoin ATMs which allow users to exchange cash and bitcoins without humans to facilitate the exchange.[106] As of September 2014, there are 64 bitcoin ATMs spread out over 20 countries in the EU, with the Netherlands and UK home to almost a third of these ATMs.[107]

Another way to purchase bitcoin involves a direct trade with the prospective seller, through the use of an intermediary which facilitates the connection. The process usually requires users to register and post an offer. The website would send an alert once another user wants to trade. From thereon, the parties solely interact with each other using the website to complete the trade. Localbitcoins.com and bitbargain.com are examples of websites offering direct trade services.[108]

(3) Spend bitcoins[109]

Purchased bitcoins are transferred to the user's bitcoin wallet. As mentioned earlier, the wallet is designated with a particular address and the user should provide the address to the exchange or to whomever it purchases bitcoins from. Once the user has the bitcoins in his bitcoin wallet, he can now conduct various transactions like purchasing goods or services online or in brick-and-mortar stores.

## *2.7 What is the role of public/private keys in the bitcoin system?*

The bitcoin network is a public key cryptographic system. It is this public key cryptographic system which renders the bitcoin network decentralized,[110] relatively secure and pseudonymous.

Going back to the earlier example, Juan buys a laptop from Pedro for 10 bitcoins. This is done by making a transaction that identifies Pedro as the transferee of the bitcoins and 10 bitcoins as the amount to be transferred. Considering the decentralized and trustless nature of the system, it is imperative for Juan to find a way to identify himself and Bob in the transaction. [111]

This is where public key cryptography system comes in. This system uses two crucial pieces of

106 "Bitcoin ATM" <http://en.wikipedia.org/wiki/Bitcoin_ATM> accessed 04 November 2014
107 Tom Sharkey, "Europe's top 5 countries for bitcoin ATMs" (*Coindesk,* 14 September 2014) <https://www.coindesk.com/5-popular-european-countries-bitcoin/> accessed 04 November 2014
108 "How to sell bitcoin" (n79) <http://www.coindesk.com/information/sell-bitcoin/> accessed 05 November 2014
109 "Getting started with bitcoin" (n66) <https://bitcoin.org/en/getting-started > accessed 20 August 2014
110 "Six Things Bitcoin Users Should Know about Private Keys" (*Bitzuma*, 23 April 2014) <http://bitzuma.com/posts/six-things-bitcoin-users-should-know-about-private-keys/> accessed 21 August 2014
111 Ibid

information for identification and verification purposes, called the public key and the private key.[112] The public key and the private key are actually strings of text, are uniquely linked and are crucial in sending and/or receiving bitcoins. The public key identifies a sender or recipient, and can be shared or distributed to others in order to facilitate the transaction. A private key is mathematically linked to the public key and allows the user to spend or to send bitcoins to the recipient. It is important to keep the private key confidential. [113]

An analogy could be made between public and private keys and a bank account and bank account password. A public key is analogous to a bank account which may be distributed to people where they can deposit funds to said account. A private key is analogous to a bank account password that must be kept secure because it allows the user to spend or transfer funds to another user or account.[114]

Bitcoin users may also use a bitcoin address which may serve the same purpose as a public key, that is, it is used to receive bitcoin payments.[115] It differs slightly from a public key in that it is a modified version of the public key.[116] Bitcoin accounts are free to set up and a user can practically obtain as many bitcoin address as possible. Users are often encouraged to have different addresses for each separate transaction to increase anonymity, [117] "hampering or defeating a third party's ability to extract identifying information from a pattern of transactions."[118]

## *2.8 What is the legal status of bitcoins in the EU?*

Because of its ability to send money across distances directly from one person to another with little or no cost and with relative anonymity, the bitcoin system has gained popularity the world over, more particularly in the EU.

The EU has no legislation concerning the status of the bitcoin as a currency.[119] The European Central Bank (ECB), in October 2012, [120] issued a report on virtual currency schemes. It analyzed

112 Ibid
113 Ibid
114 "What are public-private keys?" (*explainbitcoin.com*) <http://explainbitcoin.com/public-private-key/> accessed 21 August 2014
115 "Address" (*en.bitcoin.it*) <https://en.bitcoin.it/wiki/Address> accessed 21 August 2014. According to <https://en.bitcoin.it/wiki/Address> accessed 21 August 2014: "Addresses can be generated at no cost by any user of Bitcoin. For example, using Bitcoin-Qt, one can click "New Address" and be assigned an address. It is also possible to get a Bitcoin address using an account at an exchange or online wallet service."
116"Bitcoin Addresses" (*learncryptography.com*) <http://learncryptography.com/bitcoin-addresses/ > accessed 21 August 2014
117 "Address" (n115) <https://en.bitcoin.it/wiki/Address> accessed 21 August 2014
118 Christopher (n101) 14
119 "Regulation of Bitcoin in Selected Jurisdictions January 2014 " (n18) 8
120 "Virtual Currency Schemes October 2012" 43 *European Central Bank*
<http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf > accessed 07 August 2014

the legal status of the Bitcoin system under existing EU legislation and concluded that the legal framework of bitcoin under EU law is "very unclear." The report mentioned that bitcoins may possibly fall within the definition of either the Electronic Money Directive (2009/110/EC) which amended Directive 2000/46/EC, or the Payment Services Directive (2007/64/EC). Still, using the criteria under either Directive, it is unclear whether bitcoin is covered under either legislation.[121]

Under the Electronic Money Directive, an electronic money –

> "(1) should be stored electronically;
> "(2) issued on receipt of funds of an amount not less in value than the monetary value issued; and
> "(3) accepted as a means of payment by undertaking other than the issuer."[122]

According to the ECB report, bitcoin satisfies the first and third requisites but not the second, inasmuch as the "mining" activity leads to the creation of money without "receipt of funds" under item 2. [123] Moreover, Article 11 of the Directive requires that "Member States shall ensure that, upon request by the electronic money holder, electronic money issuers redeem, at any moment and at par value, the monetary value of the electronic money held." According to the report, redemption cannot be ensured under the bitcoin system.[124]

On the other hand, the Payment Services Directive prescribes rules concerning the execution of payments using electronic money. However, the report concludes that bitcoin does not fall within the scope of the Directive because the Payment Services Directive involves payment transactions where the funds are electronic money as defined under the Electronic Money Directive; hence, since it is questionable whether bitcoins are electronic money under the Electronic Money Directive, it follows that it is doubtful whether the Payment Services Directive covers bitcoins.[125]

On 12 December 2013, the European Banking Authority (EBA), the EU regulatory agency that advises EU institutions on matters concerning banking, e-money regulation, and payments,[126] issued a warning to consumers on virtual currencies on risks associated with transactions, such as buying, holding, or trading virtual currencies, including bitcoins.[127]The EBA warned

121 Ibid
122 Article 2 (2), Directive 2009/110/EC of the European Parliament and of the Council <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0110&from=EN > accessed 07 August 2014
123 "Virtual Currency Schemes October 2012" (n120) 43
124 Ibid
125 Ibid
126 "Regulation of Bitcoin in Selected Jurisdictions" Report for Congress (n119) 8
127 "Warning to consumers on virtual currencies, EBA/WRG/2013/01, 12 December 2013" (n19) 1

consumers that inasmuch as bitcoin is not regulated, "consumers are not protected and are at risk of losing their money and that consumers may still be liable for taxes when using virtual currencies."[128]

In its 04 July 2014 Opinion, the EBA has stated that virtual currencies, including bitcoins, are not considered legal tender. This is because the following characteristics of legal tender are not satisfied: (a) mandatory acceptance, which means that bitcoins may be refused as a means of payment unless the parties to the transactions have agreed on the use of bitcoins as a means of payment; (b) acceptance at full face value, which means that the "the monetary value is equal to the amount indicated;"[129] and (c) the power to discharge the payment obligations of debtors. In the same Opinion, the EBA warned against the ML risks accompanying the use of digital currencies. It argues that money laundering risks are high with virtual currencies like bitcoins because the system allows criminal elements to deposit/transfer virtual currencies anonymously, globally, quickly and irrevocably. [130]

128 Regulation of Bitcoin in Selected Jurisdictions" Report for Congress (n119) 9
129 "EBA Opinion on Virtual Currencies, EBA/Op/2014/08, 4 July 2014" (*EBA*) (n20) 13
130 "EBA Opinion on Virtual Currencies, EBA/Op/2014/08, 4 July 2014" (*EBA*) (n20) 17

# CHAPTER 3. Money Laundering in the Bitcoin System

This Chapter will discuss the concept of money laundering and how bitcoins are used or can be potentially used in laundering money. A background on the essential requirements of anti-money laundering measures --the three-fold anti-money laundering (AML) compliance requirements-- will be helpful in understanding the next Chapter.

The Chapter continues with a discussion on the ways money laundering is committed as well as the reasons that make bitcoins especially attractive to money launderers and how they take advantage of these features to launder money and further their criminal purposes. Money laundering is committed by buying and selling bitcoins or traditional currency with illegal proceeds through bitcoin exchanges and other relevant market participants. It can also be committed by buying and selling goods or services using bitcoins derived from unlawful activities. Finally, exchanges and other relevant market participants may also commit money laundering when they facilitate money laundering activities. Illustrations of real-life cases of money laundering will also be provided.

## *3.1 What is money laundering?*

Criminal elements that hold substantial profits from criminal activities such as illegal arms sales, smuggling, and drug trafficking, must find a way to disguise the origin of the profits without attracting attention to the underlying illegal activity.[131] Money laundering is the "processing of…criminal proceeds to disguise their illegal origin."[132] It is an offense because it is the outgrowth of some underlying crime. [133] In other words, it is a derivative offense because it is preceded by an illegal activity, the so-called predicate offense of money laundering. The offense was first made punishable under the UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances,[134] the UN Convention against Corruption[135] and the UN

131 "Manual on Countering Money Laundering and the Financing of Terrorism" (*Asian Development Bank*, January 2003) 4 <https://www.unodc.org/tldb/pdf/Asian-bank-guide.pdf > accessed 04 September 2014

132 "What is money laundering?" (*FATF*)<http://www.fatf-gafi.org/pages/faq/moneylaundering/ > accessed 04 September 2014

133 Christopher (n101) 6

134 See <https://www.unodc.org/pdf/convention_1988_en.pdf> accessed 04 September 2014

135 Article 23 of the UN Convention against Corruption states:

> Article 23. Laundering of proceeds of crime
>
> *(a)* (i) The conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her action;
>
> (ii) The concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime;

Convention against Transnational Organized Crime.[136]

Money laundering is done by: (1) conversion or transfer of property knowing that such property is the proceeds of crime, (2) concealment or disguise of the nature, source location, etc. of property, (3) acquisition, possession or use of property of proceeds of crime, (4) participation, association with or conspiracy to commit, attempt to commit and aiding, abetting, facilitating and counselling the aforementioned acts .[137] Criminals launder or disguise the source of their illicit funds for either of two reasons: (1) the fund constitutes evidence of the crime, and (2) the fund itself is susceptible to seizure and has to be protected.[138]

Proceeds of criminal activities or "dirty" money undergo three (3) stages before it becomes "clean:" (1) placement; (2) layering; and (3) integration.[139]

Placement occurs when the criminal introduces his illicit funds into the financial system.

---

*(b)* Subject to the basic concepts of its legal system:

(i) The acquisition, possession or use of property, knowing, at the time of receipt, that such property is the proceeds of crime;

(ii) Participation in, association with or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the offences established in accordance with this article.

See <https://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf> accessed 13 August 2014

136 Article 6 of the UN Convention against Transnational Organized Crime states:

Article 6. Criminalization of the laundering of proceeds of crime

1. Each State Party shall adopt, in accordance with fundamental principles of its domestic law, such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally:

(a) (i) The conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her action;

(ii) The concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime;

(b) Subject to the basic concepts of its legal system:

(i) The acquisition, possession or use of property, knowing, at the time of receipt, that such property is the proceeds of crime;

(ii) Participation in, association with or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the offences established in accordance with this article.

See <http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf> accessed 13 August 2014

137 Article 23 of UNCAC and Article 6 of UNCTOC (n135 and n136)

138 "Manual on Countering Money Laundering and the Financing of Terrorism" (n131) 10

139 "The Money Laundering Cycle" (*UNODC*)<https://www.unodc.org/unodc/en/money-laundering/laundrycycle.html> accessed 13 August 2014

Criminals may break up large amounts of funds into less conspicuous smaller sums that are deposited into a bank. It can also be accomplished by purchasing monetary instruments that are subsequently deposited into accounts at a different branch or location. When the funds have entered the financial system, the criminal may engage in acts such as transfers or movements of the funds for the purpose of dissociating the funds from their illegal source. This is the layering stage. The funds may be transferred from one bank account to another in his name or in the name of another person, anywhere in the world.[140] In the integration stage, the funds re-enter the legitimate economy and made available for the use of the launderer. This is accomplished by investing the "cleaned" funds in property, real or personal, or business ventures,[141] or as payment for services. After the "dirty" funds have gone through these three (3) stages, the funds would appear to be "clean," hence, the term "laundering."

In bitcoin transactions, the three (3) stages of money laundering take place in the following manner:

The "placement" stage of money laundering takes place when illicit funds are introduced into the financial system by the exchange of illegal proceeds for bitcoins, or bitcoins that are illegal proceeds for fiat currency. The second step, "layering," is accomplished when bitcoins are used by criminal elements in purchasing goods or services online or offline by transferring bitcoins from one account to another either held by one of more users. However, even without "transacting" the proceeds, money laundering is committed by mere possession of such illicit bitcoins. In the third step, "integration" the illicit funds are returned to the financial system and made available for the use of the launderer.[142]

### 3.1.1 *Three-fold AML compliance obligations*

Essentially, anti-money laundering preventive regulations focus on three (3) key compliance obligations of financial and non-financial institutions ("covered persons").[143] These obligations are:

1. Customer due diligence or Know-your-Customer requirements
2. Record-keeping
3. Reporting of suspicious transactions

These AML obligations were made mandatory or obligatory on signatories of the UN Convention

140 "What is money laundering?" (n132)

141 Ibid

142 Christopher (n101) 20

143 "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation FATF Recommendations February 2012" <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf> accessed 08 October 2014

against Transnational Organized Crime (under Article 7)[144] and the UN Convention against Corruption (under Article 14).[145]

Article 7 of the UN Convention against Transnational Organized Crime provides, *viz*:

> "Article 7. Measures to combat money-laundering
> "1. Each State Party:
> (a) Shall institute a comprehensive domestic regulatory and supervisory regime for banks and non-bank financial institutions and, where appropriate, other bodies particularly susceptible to money-laundering, within its competence, in order to deter and detect all forms of money-laundering, which regime shall emphasize requirements for customer identification, record-keeping and the reporting of suspicious transactions;" (underscoring mine)

Article 14 of the UN Convention against Corruption provides, *viz*:

> "Article 14. Measures to prevent money-laundering
>
> "1. Each State Party shall:
> (a) Institute a comprehensive domestic regulatory and supervisory regime for banks and non-bank financial institutions, including natural or legal persons that provide formal or informal services for the transmission of money or value and, where appropriate, other bodies particularly susceptible to money laundering, within its competence, in order to deter and detect all forms of money-laundering, which regime shall emphasize requirements for customer and, where appropriate, beneficial owner identification, record-keeping and the reporting of suspicious transactions;" (underscoring mine)

Under the FATF Recommendations,[146] Know-your-customer (KYC) regulations (FATF

144 United Nations Convention against Transnational Organized Crime (*UNODC*) <http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf> accessed 03 September 2014

145 United Nations Convention against Corruption (*UNODC*) <http://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf > accessed 03 September 2014

146 FATF Recommendations are internationally recognised and endorsed standards for combating of money laundering and the financing of terrorism that ensure transparency in the financial system and enable countries to prevent any unlawful use of their financial systems. In turn, countries and jurisdictions all over the world comply with these Recommendations by adopting these requirements into their legislative and regulatory frameworks.

Recommendation 10) require a covered person to conduct procedures using a risk-based approach to identify its customer and to verify its customer's identity, [147] including the identification of beneficial ownership (FATF Recommendation 24) and politically exposed persons (FATF Recommendation 12). Record-keeping regulations require covered persons to keep records of transactions for at least five (5) years to enable them to comply with requests for information from government agencies (FATF Recommendation 11).[148] Suspicious transaction reporting regulations require covered persons to report transactions that they deem to be related to an unlawful activity to the financial intelligence unit of their respective jurisdictions (FATF Recommendation 20).[149]

Due to fast changing developments in technology and communication, money, and in particular, illicit funds, have become much more easily and speedily moved anywhere in the world. These developments have made the job of fighting money laundering increasingly urgent. [150] According to the United Nations Office on Drugs and Crime, around 2-5% of global GDP, or approximately US$800 billion to US$ 2 trillion is estimated to be laundered globally in one year.[151]

Money laundering has pernicious effects on the financial system and the economy in general and because of this, it has become imperative to arrest the laundering of dirty money. When illicitly acquired funds are processed through a particular institution – either with the open complicity of its officers or because the institution has no effective AML procedures – the reputation of that financial institution suffers and will negatively affect the perception of regulatory bodies and the public in general.[152] As aptly stated, "The integrity of the banking and financial services marketplace depends heavily on the perception that it functions within a framework of high legal, professional and ethical standards."[153]

On a broader perspective, a particular country or jurisdiction that lacks an effective AML

---

See "Who we are" (*FATF*) <http://www.fatf-gafi.org/pages/aboutus/> accessed 13 August 2014

147 FATF Recommendation 10 <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf> accessed 04 September 2014

148 FATF Recommendation 11 < http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf> accessed 04 September 2014

149 FATF Recommendation 20 <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf> accessed 04 September 2014

150 "Money Laundering and Globalization" (*UNODC*) <https://www.unodc.org/unodc/en/money-laundering/globalization.html > accessed 13 August 2014

151 Ibid

152 "What is money laundering?" (n132) <http://www.fatf-gafi.org/pages/faq/moneylaundering/> accessed 14 August 2014

153 Ibid <http://www.fatf-gafi.org/pages/faq/moneylaundering/ > accessed 14 August 2014

framework may suffer negative macroeconomic consequences such as "inexplicable changes in money demand, prudential risks to bank soundness, contamination effects on legal financial transactions, and increased volatility of international capital flows and exchange rates due to unanticipated cross-border asset transfers."[154] Most importantly, the failure to combat money laundering allows corruption and crime to flourish, assaults the integrity of society and undermines the rule of the law. Unchecked, money laundering allows criminal activity to continue.[155]

### *3.1.2 Money laundering and emerging payment systems*

Money launderers are always on the lookout for new methods to disguise the sources and destinations of their illicitly acquired funds. Moving funds through traditional methods, such as financial institutions, may be considered too risky for criminal elements because of strict AML rules and regulations imposed by these financial institutions. Hence, criminal elements look to new technologies and other ways and means where AML regulations have not yet kept pace with. Emerging payment technologies such as bitcoins are especially attractive to criminal elements who wish to disguise their illicit funds for the reason that financial intelligence units, governments and even business are less likely to fully understand these non-traditional payment systems. [156]

Virtual currencies like bitcoins have gained prominence in the dark underbelly of the internet, informally known as the Dark Web, because of the relative anonymity offered by these virtual currency schemes, making them the currency of choice among organized crime groups and individuals that cater to child pornography, drugs, human trafficking, arms trafficking and the like. [157] Past history reveals that virtual currencies have been used to launder money. The most notable of these involve Liberty Reserve and Silk Road. Liberty Reserve allegedly was "created and structured, and operated, to help users conduct illegal transactions anonymously and launder the proceeds of their crimes"[158] from "credit card fraud, identity theft, investment fraud, computer hacking, narcotics trafficking, and child pornography."[159] As for Silk Road, its

---

154 Ibid <http://www.fatf-gafi.org/pages/faq/moneylaundering/ > accessed 14 August 2014

155 Ibid <http://www.fatf-gafi.org/pages/faq/moneylaundering/ > 14 August 2014

156 Christopher (n101) 10

157 "Technology in the fight against money laundering in the new digital currency age" (*Thomas Reuters*, June 2013) <http://trmcs-documents.s3.amazonaws.com/cfbf4386891bc6cb7ee26f9690294222_20130617083834_AML%20White%20Paper.pdf> accessed 02 September 2014

158 "Co-founder of Liberty Reserve Pleads Guilty to Money Laundering in Manhattan Federal Court" (*US DOJ*, 31 October 2013) <http://www.justice.gov/opa/pr/2013/October/13-crm-1163.html> accessed 02 September 2014

159 "Statement of Jennifer Shasky Calvery, Director Financial Crimes Enforcement Network United States Department of the Treasury Before the United States Senate Committee on Homeland Security and Government Affairs" (US DOJ, 18 November 2013) < http://www.fincen.gov/news_room/testimony/html/20131118.html> accessed 02 September 2014

creator, Ross Ulbricht, is currently facing charges of money laundering. The US DOJ alleged that transactions were required to be paid in bitcoins to avoid detection and to launder hundreds of millions of dollars.[160]

### *3.1.3 Money laundering with bitcoins- Are bitcoins "money?"*

As previously discussed in Chapter 1, in the EU, as in most jurisdictions all over the world,[161] bitcoin is not treated as real money or "real currency." Considering that bitcoins are not "real money", is it possible to commit money laundering using bitcoins?

This was the question raised by Ross Ulbricht. He argued in a motion filed before the court that bitcoins are not monetary instruments and hence, its use could not be the basis for a money laundering charge.[162] In his motion,[163] he argued that even the US Internal Revenue Service has treated bitcoins as property and not as currency.[164] This argument was also raised in the case involving the two Florida men mentioned in Chapter 1 who were also indicted for money laundering.[165]

In the Ulbricht case, the US District court of the Southern District Court of New York rejected the argument of the defendant. Referring to the money laundering statute[166] and case law[167] interpreting the statute,[168] the court ruled that the term "financial transaction" was broadly

---

160 Ibid

161 "Regulation of Bitcoin in Selected Jurisdictions January 2014" (n119) 8

162 US v Ulbricht (09 July 2014) 14-cr-68 (KBF) United States District Court Southern District of New York <http://www.scribd.com/doc/233234104/Forrest-Denial-of-Defense-Motion-in-Silk-Road-Case#download > accessed 18 August 2014 accessed 18 August 2014

163 Andy Greenberg, "Judge Shoots Down 'Bitcoin Isn't Money' Argument in Silk Road Case" *Wired* (California, 09 July 2014) <http://www.wired.com/2014/07/silkroad-bitcoin-isnt-money/ > accessed 18 August 2014

164 US v Ulbricht (n162)

165 Susannah Nesmith, "Bitcoin Charges Against Miami Man May Proceed, Judge Says" *Bloomberg* (US, 07 March 2014) <http://www.bloomberg.com/news/2014-03-07/bitcoin-charges-against-miami-man-may-proceed-judge-says.html> accessed 18 August 2014

166 The statute involved in this case is Title 18, United States Code, Section 1956(a) (1) (A) (I) and 1956 (a) (1) (B) (I).

167 Greenberg (n163) <http://www.wired.com/2014/07/silkroad-bitcoin-isnt-money/ > accessed 18 August 2014

168 See <http://www.law.cornell.edu/uscode/text/18/1956> accessed 18 August 2014

Title 18 US Code §1956 (a)

(1) Whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity—

(A)

(i) with the intent to promote the carrying on of specified unlawful activity; or

(ii) with intent to engage in conduct constituting a violation of section 7201 or 7206 of the Internal Revenue Code of 1986; or

(B) knowing that the transaction is designed in whole or in part—

defined in Title 18 US Code §1956 (c). It held that the term "captures all movements of 'funds' by any means, or monetary instruments." The term "funds" on the other hand, was not defined in the statute and is given its ordinary meaning-- "money, often money for a specific purpose."[169]

The court ruled, viz:

> "Put simply, "funds" can be used to pay for things in the colloquial sense, Bitcoins can be either used directly to pay for certain things or can act as a medium of exchange and be converted into a currency which can pay for things. See Bitcoin, https://bitcoin.orn/en (last visited July 3, 2014); 8 Things You Can Buy With Bitcoins Rights Now CNN Money, http://money.cnn.com/gallery/technology/2013/11/25/bit-with-bitcoin/(last visited July 3, 2014). Indeed the only value for Bitcoin lies in its ability to pay for things – it is digital and has no earthly form; it cannot be put on a shelf and looked at or collected in a nice display case. Its form is digital – bits and bytes that together constitute something of value. And they may be bought and sold using legal tender. See How to Use Bitcoin, https://bitcoin.org/en/getting-started (last visited July 3, 2014). Sellers using Silk Road are not alleged to have given their narcotics and malicious software away for free – they are alleged to have sold them.

---

(i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity; or
(ii) to avoid a transaction reporting requirement under State or Federal law, xxx

Title 18 US Code §1956 (c)
(4) the term "financial transaction" means
(A) a transaction which in any way or degree affects interstate or foreign commerce
(i) involving the movement of funds by wire or other means or
(ii) involving one or more monetary instruments, or
(iii) involving the transfer of title to any real property, vehicle, vessel, or aircraft, or
(B) a transaction involving the use of a financial institution which is engaged in, or the activities of which affect, interstate or foreign commerce in any way or degree;

(5) the term "monetary instruments" means
(i) coin or currency of the United States or of any other country, travelers' checks, personal checks, bank checks, and money orders, or
(ii) investment securities or negotiable instruments, in bearer form or otherwise in such form that title thereto passes upon delivery;
(6) the term "financial institution" includes—
(A) any financial institution, as defined in section 5312 (a)(2) of title 31, United States Code, or the regulations promulgated thereunder; and
(B) any foreign bank, as defined in section 1 of the International Banking Act of 1978 (12 U.S.C. 3101); Greenberg (n163) <http://www.wired.com/2014/07/silkroad-bitcoin-isnt-money/> accessed 18 August 2014

> "The money laundering statute is broad enough to encompass use of Bitcoins in financial transactions. Any other reading would – in light of Bitcoin's sole raison d'etre – be nonsensical. Congress intended to prevent criminals from finding ways to wash the proceeds of criminal activity by transferring proceeds to other similar or different items that store significant value." (underscoring mine)

In the international scene, the FATF has recognized the potential of virtual currencies like bitcoins to be used in laundering proceeds of illicit activities. In June 2014, it released a FATF Report on Virtual Currencies Key Definitions and Potential AML/CFT Risks.[170] The use of virtual currencies like bitcoins renders money laundering activities less detectable and AML efforts more complex because unlike transfers using conventional currency or legal tender, all transactions happen online and there are "no physical materials to observe or intercept for proof of illicit activities."[171]

## *3.2 How are Bitcoins Used for Money Laundering?*

The creator/s of bitcoin envisaged an online payment system that is decentralized and free from intervention from a third-party intermediary. The solution came in the form of a "purely peer-to-peer version of electronic cash [that] would allow online payments to be sent directly from one party to another without going through a financial institution."[172] This section discusses the ways money laundering may be committed by bitcoin users and bitcoin exchanges and other trading platforms by exploiting these characteristics of the bitcoin system.

### *3.2.1 Transactions with bitcoin exchanges and other trading platforms*

Bitcoin users may commit money laundering when they buy or sell bitcoins through bitcoin exchanges and other trading platforms using illegal proceeds.

Criminal elements could launder funds within the bitcoin ecosystem when they use the services of third-party services, notably, exchanges and other bitcoin trading platforms, simply by exchanging funds obtained from illegal activities into bitcoins, or bitcoins obtained from illegal activities into fiat or traditional currency. Exchanges and other trading platforms are one of the gateways of the bitcoin ecosystem in that they provide a service to users to exchange traditional currency into bitcoins that could be used for bitcoin transactions, or cash out of the

170 "FATF Report Virtual Currencies Key Definitions and Potential AML/CFT Risks June 2014" (n23)

171 Danton Bryans, "Bitcoin and Money Laundering: Mining for an Effective Solution" (89 Ind. L.J. 441 2014) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2317990> accessed 18 August 2014

172 Nakamoto (n28) 1

bitcoin system. Where criminal proceeds from drug trafficking or from any other illegal activity are used to purchase bitcoins and vice versa, from an exchange, these users are liable for money laundering; and where an exchange or its officers are aware that the funds or the bitcoins were acquired through criminal means, then the exchange/its officers are also liable for money laundering.

The first stage of money laundering, the "placement" portion of money laundering is accomplished by buying bitcoins through an exchange using illegal proceeds of crime, thereby introducing illegal proceeds into the financial system by the exchange of illegal proceeds with bitcoins. The second step, "layering" usually is accomplished when bitcoins are used by criminal elements in purchasing goods or services online or offline, thereby transferring bitcoins from one account to another either held by one of more users, or *even by simply keeping or possessing these bitcoins*. The use of bitcoins to purchase goods and services, hence, is *not* necessary to commit money laundering as mere "possession" of bitcoins is considered money laundering.[173] In the third step, "integration" the illicit funds are returned to the financial system and made available for the use of the launderer. This occurs when criminals obtain bitcoins in the equivalent value of the illegal proceeds to dispose of, use or possess as they wish.

Notably, transacting with a bitcoin exchange might potentially place such transaction fully transparent and open to inspection by government officials as some jurisdictions require bitcoin exchanges to comply with the three-fold AML compliance obligations.[174] Exchanges may also, upon request or subpoena, provide information such as IP addresses and bank account numbers to law enforcement agencies. [175]

While it is unavoidable to use an exchange for large amounts, it is possible to exchange bitcoins for real currency and vice versa using services provided by services such as localbitcoins.com (by directly matching purchasers and buyers within their vicinity) [176] a study notes that "the current and historical volume on these sites does not seem to be high enough to support cashing out at scale." [177]

Exchanges may also be used to cash out of the bitcoin ecosystem. For example, researchers

---

173 Article 6 of the UNCTOC provides that "possession …..of property, knowing, at the time of receipt, that such property is the proceeds of crime" constitutes money laundering. See n6. Article 23 of the UNCAC provides that "possession ...of property, knowing, at the time of receipt, that such property is the proceeds of crime" constitutes the crime of money laundering. See n5.

174 Christopher (n101)

175 Robert McMillan, "Sure, you can steal bitcoins. But good luck laundering them" *Wired* (California, 27 August 2013) <http://www.wired.com/2013/08/bitocoin_anonymity/ > accessed 02 September 2014

176 Dylan Love, "How to buy bitcoins completely anonymously" Business Insider (NYC, 10 December 2013) <http://www.businessinsider.com/how-to-buy-bitcoins-completely-anonymously-2013-12> accessed 03 September 2014

177 Sarah Meiklejohn, et al., "A fistful of bitcoins: characterizing payments among men with no names" 9 <http://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf > accessed 02 September 2014

showed that they were able to trace that bitcoins that presumably came from a Silk Road public key were transmitted to exchanges. While the study did not confirm that the public keys were indeed owned by Silk Road, the study demonstrated that it is possible to trace money flow throughout the bitcoin system using analytical tools.[178]

Bitcoins can be purchased from bitcoin exchanges using real money in most instances, but also with credit and debit cards, wire transfers, or even other cryptocurrencies.[179] A discussion of how money flows via transactions through bitcoin exchanges is provided below to illustrate the role that traditional financial institutions sometimes play in the bitcoin exchange process. The examples here may be outdated by the time these are read; nonetheless, they are offered here only for purposes of illustrating the process in which legal tender is exchanged for bitcoins and vice versa, and what exact points of the bitcoin process may be subject to AML supervision.

Mt. Gox used to be one of the largest bitcoin exchanges in the world with around 80% of global trading volume at its peak. [180] Bittylicious is another bitcoin exchange registered in England and Wales.[181] To purchase bitcoins from an exchange, typically, as in the case of Mt. Gox, the user must establish an account with the exchange and this account would then be funded by the user. The user can fund his exchange account through the use of a money transmitter. These money transmitters are used by bitcoin users as conduits in order to send funds to bitcoins exchanges for the purpose of sending funds to their exchange accounts. In Bittylicious, there is no need to use a money transmitter. Payment to the exchange is made using online banking services. The user needs to log in first to his Bittylicious account where instructions and information are provided in order to make a bank transfer. Then the user needs to transfer funds using online banking services usually under a heading like *Make a funds transfer* or *Pay a person.* The information provided earlier in the Bittylicious account should be used to make payment instructions using online banking. [182]

In addition, there are various options to an individual wishing to purchase bitcoin who is unwilling or unable to purchase using cash. For instance, some exchanges may allow purchasers to use credit cards or debit cards to purchase bitcoins.[183] Mt. Gox used to accept personal checks drawn on US banks and made out to "Morpheus."[184] In the Netherlands, Ideal could also

178 Ibid

179 "How can I buy bitcoins?" (*Coindesk,* last updated 23 October 2014) <http://www.coindesk.com/information/how-can-i-buy-bitcoins/> accessed 05 November 2014

180 "Mt. Gox bitcoin exchange news" (*Coindesk*) http://www.coindesk.com/companies/exchanges/mtgox/ accessed 20 August 2014

181 Website at <https://bittylicious.com/> accessed 04 September 2014

182 See <https://bittylicious.com/help/index.php/Bitcoin_buying_guide> accessed 20 August 2014

183 BitSource accepts credit cards, debit cards, or bank wire. See <https://bitsource.org/> accessed 24 October 2014, Virwox also accepts credits cards. See <https://www.virwox.com/?stage=1> accessed 24 October 2014. CoinMama accepts credit cards. See <https://www.coinmama.com/> accessed 24 October 2014.

184 Christopher (n101) 20.

be used to purchase bitcoins from Bitonic, HappyCoins and Bittylicious.[185] Moneygram and postal money orders may also be used to pay for bitcoins. [186] Other exchanges allow users to deposit funds in person (over-the-counter, not through an ATM) to their bank account. [187]

Where a purchaser wants to purchase bitcoins from a bitcoin exchange located in a foreign country, the user sends funds through a money transmitter by authorizing the latter to debit funds from the user's bank account and crediting it to his account with the money transmitter. The funds are sent to the foreign bitcoin exchange through a domestic bank and may flow through a foreign-based correspondent bank which services the exchange. When the exchange receives the funds and credits it to the user's exchange account. The user can then use the funds to purchase bitcoins.[188]

For trading platforms offering direct trades like localbitcoins.com, payment may be made using SEPA bank transfer, PayPal, international wire, Ukash and PaySafeCard. [189]

In these cases, the interaction between bitcoin exchanges/other trading platforms and the traditional financial system is apparent, in particular, banks and money transmitters. These transactions using traditional financial systems potentially place these transactions within government radar as these institutions are subject to the three-fold AML compliance requirements of KYC, reporting and record-keeping.[190] This means that when a prospective bitcoin purchaser wishes to purchase bitcoins, he might be required by the exchange to wire money from his bank to the exchange's account in which case, the transactions are subject to the bank's AML procedures.

But criminal elements know that banks keep records of their customers and their transactions and prefer to purchase bitcoins using cash. By doing so, they preserve their anonymity by avoiding any paper trail of their financial flows. Thus, the question of transparency and the need to regulate these transactions from an AML perspective becomes more apparent and pressing.

### *3.2.2 Buying or selling goods or services*

Criminal elements may launder funds within the bitcoin ecosystem when they convert, transfer or use illegal proceeds by purchasing or sell goods or services using funds obtained from unlawful activities. Illegal funds are made to appear “clean” by participating in trade (i.e. buying

185 “Buying Bitcoins (the newbie version). See <https://en.bitcoin.it/wiki/Buying_Bitcoins_%28the_newbie_version%29> accessed 24 October 2014
186 Ibid
187 “How can I buy bitcoins?” (n179)
188 Financial Crimes Enforcement Network Networking Bulletin dated March 2014 on Crypto-currencies (redacted)
189 See <https://localbitcoins.com/> accessed 05 November 2014
190 Christopher (n101) 19

or selling) using bitcoins. The same features that make bitcoin very attractive as a payment system are the same features that attract criminal elements/users that see bitcoin system as a safe haven where they can conceal their illegally obtained funds.

The bitcoin system is decentralized, unsupervised, unregulated and lacks an oversight body. Unlike other popular online payment systems like PayPal, the decentralized nature of the bitcoin system makes it very difficult for law enforcement authorities to obtain information on transactions using bitcoins, detecting suspicious activity and identifying users. There is no centralized authority to supervise, monitor and ensure compliance with the three-fold compliance obligations of KYC, reporting of suspicious transactions, record-keeping and processing legal requests like subpoenas.

The FATF has also identified that absence of a central oversight body as one of the AML risks of digital currencies like bitcoin.[191] According to an FBI Intelligence Assessment (Unclassified, for Official Use only), bitcoin, being the only decentralized, P2P network-based digital currency, is especially useful in, and vulnerable to, illicit money transfers. [192] On the other hand, with traditional payment systems like credit cards, offering banks conduct KYC and keep records on their customers that may be accessed by law enforcement agencies. They are also supervised by a central authority which keeps records on compliance measures taken by the supervised entity, also accessible to law enforcement agencies.

The bitcoin system also provides users with a certain degree of anonymity absent in traditional online payment systems like credit cards and PayPal, closely approximating a true anonymous cash transaction. While all bitcoin transactions are recorded on the block chain, hence, accessible at any time to law enforcement agencies,[193] the information published on the block chain is not tied to any real-life individuals or entities[194] or real world identifying information. The block chain only records the transaction between the two public keys, the time, the amount, and other information.[195] Bitcoin addresses, mere alphanumeric strings,[196] are not linked to real-world identifying information such as names or other customer identification. Neither does the bitcoin system require the disclosure of, or provide identification and verification of the identity of participants nor "generate historical records of transactions that are necessarily associated with real world identity."[197]

---

191 "Virtual Currencies: Key Definitions and Potential AML/CFT Risks" (n16) 9

192 "Federal Bureau of Investigation Intelligence Assessment dated 24 April 2012" states "(u) Bitcoin virtual currency: unique features present distinct challenges for deterring activity" <http://www.scribd.com/doc/92797476/FBI-Bitcoin-Report-April-2012> accessed 29 August 2014

193 Brito (n49) 8

194 Meiklejohn (n177) 1

195 IP addresses are not recorded on the block chain but the bitcoin network does not "actively conceal the IP addresses from which transactions were initiated." There is a way to find out the IP address of a user and to trace his physical location. See <http://cointext.com/bitcoin-and-ip-address-privacy/> accessed 29 August 2014

196 Volastro (n72)

197 "FATF Report Virtual Currencies Key Definitions and Potential AML/CFT Risks"(n23) 9

It is only when a person's identity is independently linked to a public key that one could browse through all the recorded transactions on the block chain and see all transactions associated with that public key and that person.[198] For example, it is possible that a public key or a bitcoin address was discovered on a hard drive belonging to a person or on a piece of paper written in a recognized handwriting or was posted online. One could then make a guess that the public key or bitcoin address belongs to the owner of the hard drive or the person to whom the handwriting pertains. But these linkages to real identities are made independent of or outside the bitcoin system.

It is this pseudo-anonymity[199] which facilitates the concealment of illegally obtained funds. Hence, criminal elements who wish to maintain their relative anonymity under the bitcoin system ensure that they do not share information[200] about their public keys or bitcoin addresses or exchange with or transfer bitcoins with third party services that require identify information.[201]

In addition to the default partial privacy protection offered by the P2P system, criminal elements resort to various ways and means both inside and outside the P2P system to increase their anonymity.[202] According to the FBI Intelligence Assessment,[203] within the bitcoin P2P system, money launderers can increase their anonymity by creating and using new and

198 Yevgeniy Vahlis, "Bitcoin, Identity, and Decentralized Auctions" *Huffington Post* (US, 28 May 2014) <http://www.huffingtonpost.com/yevgeniy-vahlis/bitcoin-identity-and-dece_b_5398577.html> accessed 05 September 2014

199 Joshua Brustein, "Bitcoin May Not Be So Anonymous, After All" *BusinessWeek* (NYC, 27 August 2013) <http://www.businessweek.com/articles/2013-08-27/bitcoin-may-not-be-so-anonymous-after-all > accessed 29 August 2014

200 "Federal Bureau of Investigation Intelligence Assessment" (n192)

201 It is interesting to note a study by Reid and Harrigan analysing anonymity in the bitcoin system which concluded that there are "inherent limits of anonymity when using Bitcoin." Using public information available in the bitcoin system, the study demonstrated that "it is possible to associate many public keys with each other, and with external identifying information." Using passive analysis they concluded that activity of known users can be observed in detail. Using active analysis using "marked" bitcoins an interested party can discover even more information collaborating with other users. They also suggested that law enforcement agencies or other centralized services (such as exchanges) who have access to less public information (such as bank account information or shipping addresses) can connect even more real world identifiers to bitcoin wallets and transaction histories. (Fergal Reid and Martin Harrigan, "An Analysis of Anonymity in the Bitcoin System" <http://arxiv.org/abs/1107.4524> accessed 29 August 2014)

In another study researchers from the University of California, San Diego and George Mason University, showed that it is possible to trace the flow of money through the bitcoin ecosystem by using a method of identifying public keys belonging to certain services such as exchanges, wallets or other services. By transacting with these public keys, the researchers demonstrated that it was possible to trace how bitcoins move through the bitcoin ecosystem. (Meikeljohn, et al. (n79) <http://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf > accessed 02 September 2014)

202 Federal Bureau of Investigation Intelligence Assessment (n192)

203 Ibid

separate bitcoin addresses for each and every transaction. A launderer can also combine the balance of their bitcoins in several bitcoin addresses into a new bitcoin address to make a separate payment. Outside the P2P system, one of the way to increase anonymity is by using exchanges that are located in jurisdictions where the AML laws are lax. Some of these exchanges may not even verify user identification.[204]

Inside the P2P system, third-party services may be utilized to increase anonymity. These services include anonymizers to "erase the origins of xxx bitcoins and de-couple them from previous transactions." [205] While mixing funds or bitcoins helps secure user privacy, it is widely acknowledged that it "can also be used for money laundering - mixing illegally obtained funds."[206]

A 2013 *preliminary* study[207] on the effectiveness of several bitcoin anonymizers was conducted in order to test the possibilities and limitations of imposing AML measures in the bitcoin system. The results showed that Bitcoin Fog and Blockchain.info "successfully anonymize... test transactions."[208] The results led to the researchers concluding that given the findings, it would be difficult to impose KYC measures within the bitcoin system.[209] However, the study recognized several limitations including taking into consideration traffic analysis available to law enforcement.

From the perspective of law enforcement, the bitcoin system presents more difficulties in following the money trail compared with traditional online payment systems like credit cards or PayPal. In addition to the difficulty in linking an identifiable user to a bitcoin address or public key, there is the difficulty in disabling the entire bitcoin network which requires disabling every miner/user on the network in order to stop the processing of transactions. Because of this, the bitcoin P2P system presents a more formidable problem for law enforcement compared to the usual payment systems.[210] For this reason, the bitcoin system has become an attractive venue for laundering funds.

Money could be laundered through the use of fake online auctions, online markets and online sales, online gambling sites and online games, that accept bitcoins as a means of payment or transactions.[211] An example of this is the use of illicit online markets like Silk Road, an

204 FBI Intelligence Assessment (n192)
205 See <https://bitlaunder.com/> accessed 29 August 2014
206 "Mixing service" (*en.bitcoin.it*) <https://en.bitcoin.it/wiki/Mixing_service> accessed 03 September 2014
207 Malte Moser, et al., "An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem" See <https://www.wi.uni-muenster.de/department/groups/security/people/malte-moeser/publications> and <https://maltemoeser.de/paper/money-laundering.pdf> accessed 09 October 2014
208 Moser (n207) 1
209 Moser (n207) 1
210 Bryans (n171) 447
211 Killian Strauss, "How can we effectively combat the use of the internet for money laundering?" 2 <https://www.academia.edu/1369342/Cyber-laundering_-

anonymous website that was especially designed to allow users to anonymously buy and sell illegal good and services like illegal drugs, weapons, stolen identity information, and to launder illicitly acquired funds in hundreds of millions of dollars.[212] The website closed down after its seizure by the US Department of Justice. The use of the bitcoin as the exclusive means of payment and operations under the Tor network were instrumental in maintaining anonymity for transactions on Silk Road, and thus, facilitating the concealment of funds. Bitcoins allowed users to disguise their identity inasmuch as sellers and buyers are identified only by their public keys or bitcoin addresses under the P2P bitcoin system.[213] It was estimated that millions dollars were laundered from illegal transactions done on the Silk Road website[214] and around 9.5 million bitcoins exchanged hands from sales of illegal narcotics.[215]

To emphasize the popularity of anonymous websites similar to Silk Road and the use of bitcoins for nefarious drug deals, after its shutdown, several websites became immensely popular with users of Silk Road. One of these is Silk Road 2.0 reportedly being managed by the former administrators of Silk Road,[216] but was recently seized by law enforcement authorities.[217] Sheep Marketplace is another online marketplace.[218] Like Silk Road, it is an online illicit anonymous narcotics bazaars. [219]

---

How can we combat money laundering over the internet> accessed 03 September 2014

212 Eric R. Barnett, "Virtual Currencies: Safe for Business and Consumers or just for Criminals?" (13th European Security Conference & Exhibition, The Hague, 02 April 2014) 5 <http://photos.state.gov/libraries/useu/231771/PDFs/2014_Erik_Barnett_crypto-currencies_remarks.pdf> accessed 03 September 2014

213 FATF Report Virtual Currencies Key Definitions & Potential AML/CFT Risks (n23) 11

214 Ibid

215 Noel Randewich, "Bitcoin sinks in value after FBI busts Silk Road drug market" Reuters (08 October 2013) <http://www.reuters.com/article/2013/10/08/net-us-crime-silkroad-bitcoin-idUSBRE99113A20131008> accessed 05 September 2014

216 Graham Templeton, "The Silk Road 2.0 is now bigger and better than ever before: What's the FBI to do?" (*Extremetech*, 08 May 2014) <http://www.extremetech.com/extreme/182083-the-silk-road-2-0-is-now-bigger-and-better-than-ever-before-whats-the-fbi-to-do > accessed 04 September 2014. Also see <http://verdict.justia.com/2014/02/25/bitcoin-cant-ban-regulate> accessed 09 September 2014

217 Andy Greenberg, "Feds seize Silk Road 2 in major Dark Web drug bust" *Wired* (US, 06 November 2014) <http://www.wired.com/2014/11/feds-seize-silk-road-2/> accessed 14 November 2014

218 "Did One of the Silk Road's Successors Just Commit the Perfect Bitcoin Scam?" (*Motherboard*, 02 December 2013) <http://motherboard.vice.com/blog/did-one-of-the-silk-roads-successors-just-commit-the-perfect-bitcoin-scam> accessed 04 September 2014

219 Darlene Storm, "Huge bitcoin heist: Black market drug shop Sheep Marketplace poofs with $40 million" (*Computer World,* 02 December 2013) <http://www.computerworld.com/article/2475637/cybercrime-hacking/huge-bitcoin-heist--black-market-drug-shop-sheep-marketplace-poofs-with--40-milli.html> accessed 04 September 2014

### *3.2.3 Money laundering committed by an exchange and other trading platforms*

Money laundering can also be committed by a bitcoin exchange and other trading platforms. Officers, employees or agents, or the exchange or the company operating the trading platform, can commit money laundering in the conduct of business when, having knowledge that bitcoins are to be used to launder money, facilitate or allow the exchange of traditional currency into bitcoins or vice versa. In other words, having knowledge that bitcoins or traditional currencies were acquired through criminal means, these officers, employees or agents of the exchange nevertheless allow or facilitate the exchange. Such acts would be considered aiding, abetting or facilitating the commission of money laundering, and are also considered a money laundering offense.

The most obvious example of money laundering committed by an exchange involves the money laundering case filed against Shrem and Faiella,[220] both owners of different bitcoin exchanges. Shrem, CEO and part owner of BitInstant, a bitcoin exchange, conspired with Faiella, the owner of another bitcoin exchange, by selling bitcoins to the latter knowing fully well that the latter exchange was running its service on Silk Road where illicit drugs were sold. Faiella, operating under the name "BTCKing" ran a Bitcoin exchange on Silk Road, an illegal website which is popular as an online marketplace where users can purchase illegal drugs anonymously. Despite having knowledge that Silk Road was a drug-trafficking website, and that Faiella was conducting a bitcoin exchange business there, Shrem allowed and helped Faiella to conduct his operation by allowing him to fill his orders using the services offered by BitInstant. Besides this, Shrem even personally processed Faiella's transactions, provided him discounts on his high-volume orders, and even wilfully failed to file suspicious activity reports concerning the transactions of Faiella despite knowledge that the purchased bitcoins were to be used to purchase illegal drugs. Shrem also provided Faiella with advice on how to circumvent BitInstant's AML restrictions although it was his responsibility to enforce them.

The other case involving two Florida men, Reid and Espinoza, also illustrates money laundering committed by a bitcoin exchange. The two men were arrested in Miami Beach, Florida, after undercover operatives from the US Secret Service and Miami Beach police posed as buyers of bitcoin supposedly with cash obtained from theft of credit card customer information from the hacking of Target Corporation.[221]

220 US vs. Faiella, Shrem (n5)
221 Nesmith (n165)

# CHAPTER 4. Assessment of the EBA Proposals for the AML Regulation of Bitcoins

This Chapter will discuss how bitcoins are treated under the proposed regulations of the EU, briefly tackle the strengths and limitations of the EU proposed legislation on bitcoins specifically in preventing money laundering in relation to bitcoin, and finally, provide solutions on how the proposed regulations can be improved to deal with the money laundering risks of bitcoin.

## *4.1 What is the background of the EBA proposal for a regulatory framework?*

In accordance with Article 9 (2) of Regulation (EU) No. 1093/2010, one of the tasks of the European Banking Authority (EBA) is to "monitor new and existing financial activities" and to this end, it may issue guidelines and recommendations for the purpose of "promoting the safety and soundness of markets and convergence of regulatory practice."[222]

Around September 2013, pursuant to its power under its founding regulation, the EBA started to monitor digital currencies, including bitcoins, which appeared to be one of the many innovative financial activities requiring monitoring. [223] What prompted the EBA's attention was the increased activity in the use of digital currencies across EU Member States,[224] together with an increase in the number of digital currencies being launched, an increase in the number of merchants accepting digital currencies as a means of payment, and in the number of individual using digital currencies, and bitcoins in particular, as a means of payment and also for investment.[225]

In December 2013, after three months of analysis, the EBA issued a public warning, informing consumers and the public that digital currencies are unregulated and there are various risks associated with the use of digital currencies which continue to be unmitigated as long as the

222 See <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02010R1093-20140819&from=EN> accessed 27 October 2014

223 "EBA Opinion on 'Virtual Currencies'" (n20)

224 According to the EBA Opinion, the size of all digital currency schemes is difficult to measure because of problems with the reliability of data sources. Nevertheless, it was found that the total number of worldwide digital currency transactions, including those involving bitcoins, at its maximum, reached about 100,000 daily, at the time of study conducted by the EBA, compared to 295 million transactions involving traditional payment systems and terminal transactions per day in Europe alone. See "EBA Opinion on 'Virtual Currencies'" dated 04 July 2014, EBA/Op/2014/08. Page 7 <http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf> accessed 27 October 2014

225 "EBA Opinion on 'Virtual Currencies'" (n20)

use remains unregulated.[226] The EBA warned consumers that: they may lose their money on a digital currency exchange, or have their digital currency stolen from their digital wallets, that there is no consumer protection and that digital currencies are highly volatile. The EBA also warned that there is a risk that digital currencies are being used for criminal ends.[227]

At the time of the issuance of this public warning, the issue of whether virtual currencies should be regulated remained unaddressed. Events following the issuance of this warning, however, provided impetus to further explore the issue of regulation. Notably, following the issuance of the EBA warning, some of the risks that had been emphasized in the warning started to materialize, including the closure of Mt. Gox, one of the largest bitcoin exchanges at the time, due to mismanagement and hacking incidents resulting in the theft of a huge amount of bitcoins from Mt. Gox.[228] Furthermore, countries within the EU as well as beyond, took national approaches to bitcoins and digital currencies in general, that differed from one another. The approaches ranged from the imposition of certain requirements on particular market participants, regulation through licensing requirements, while others took the more drastic approach of totally banning financial institutions from dealing with digital currencies. This prompted the EBA to carry out further analysis of this issue. [229]

In 04 July 2014, after careful consideration of this issue, the EBA issued Opinion EBA/Op/2014/08 setting out the results of the assessment. The Opinion provides a background on virtual currencies, potential benefits to the use of virtual currencies, identifies market participants, risks involved in the use of virtual currencies and the causal drivers of these risks, and most importantly, for the first time, proposes a comprehensive regulatory approach for virtual currencies, both in the long term and for the short term.[230] The EBA hopes that this two-pronged approach to regulation would allow digital currency schemes to "innovate and develop outside of the financial services sector, including the development of solutions that would satisfy regulatory demands of the kind"[231] specified in the Opinion. The EBA Opinion was primarily addressed to EU legislators and for national supervisory authorities in the EU Member States. [232]

---

226 "Warning to Consumers on Virtual Currencies" (n19)

227 Ibid

228 "EBA Opinion on 'Virtual Currencies'" (n2) 8 <http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf> accessed 27 October 2014

229 Ibid

230 "EBA Opinion on 'Virtual Currencies' dated 04 July 2014, EBA/Op/2014/08" (n2) <http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf> accessed 27 October 2014

231 "EBA Opinion on 'Virtual Currencies' dated 04 July 2014, EBA/Op/2014/08" (n2) 44 <http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf> accessed 27 October 2014

232 "EBA Opinion on 'Virtual Currencies' dated 04 July 2014, EBA/Op/2014/08" (n2) 5 <http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf> accessed 27 October 2014

The Opinion identifies approximately seventy risks arising from the use of virtual currencies. These risks comprise risks to users, risks to other market participants, risks to financial integrity, risks to payment systems and risks to regulators.[233] Included under "risks to financial integrity" are the following identified money laundering risk descriptions:

(1) Criminals are able to launder proceeds of crime because they can deposit/transfer virtual currencies anonymously. The risk occurs because "senders and recipients can carry out [bitcoin] transactions on a peer-to-peer basis"[234] without requiring personal identification, and "there no intermediary that could notify authorities of suspicious transactions."[235]
(2) Criminals are able to launder proceeds of crime because they can deposit/transfer/ virtual currencies globally, rapidly and irrevocably. This risk occurs because bitcoins are use and accepted across borders, thus, making it harder for law enforcement to intercept transactions.[236]
(3) Criminals use the virtual currency remittance systems and accounts for financing purposes.[237]
(4) Criminals/terrorists disguise the origins of criminal proceeds, undermining the ability of enforcement to obtain evidence and recover criminal assets.[238]
(5) Market participants are controlled by criminals, terrorists or related organizations.[239]

These risks were judged as "**high**" on the probability of their occurrence and the impact of the occurrence.

The Opinion identifies the following causes of these risks ("risk drivers") which the EBA considered helpful in understanding the type of regulatory measures that are required to mitigate the risks:

*(1) Digital currency schemes can be created anonymously by anyone.*[240]
*(2) Payer and payee are anonymous.* Transmitters and recipients of virtual currencies deal on a person-to-person basis but remain basically anonymous;[241]

233 "EBA Opinion on 'Virtual Currencies' dated 04 July 2014, EBA/Op/2014/08" (n2) <http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf> accessed 27 October 2014
234 "EBA Opinion on 'Virtual Currencies'" (n20) 32
235 Ibid
236 Ibid
237 EBA Opinion on 'Virtual Currencies'" (n20) 33
238 Ibid
239 Ibid
240 EBA Opinion on 'Virtual Currencies'" (n20) 38
241 Ibid

(3) *Global reach.* The internet-based feature of digital currency schemes cross jurisdictional boundaries;[242]

(4) *Lack of probity.* Exchanges are "neither audited nor subject to governance and probity standards,"[243] and are "subject to misappropriation, fraud and seizure;"[244]

(5) *No reporting.* There is the "lack of reporting requirements to any authority, e.g. suspicious transactions."[245]

## *4.2 What are the proposed long-term and short-term AML regulatory measures under the EBA Opinion?*

### *4.2.1 Long-term AML regulatory measures*

When new technology, such as bitcoins, make an appearance with such impact as would catch the attention of legislators and regulators, the regulatory response may be one of three: one, apply existing legislation to regulate and control the technology, if warranted; two, deem the technology to be unnecessary to regulate; three, institute new legislation to regulate the technology. In its Opinion, the EBA makes it clear that the appropriate long-term approach to the risks posed by bitcoins and other digital currencies is to issue new comprehensive regulations. In proposing long-term measures, it essentially took a cautious approach against placing digital currencies under the scope of existing legislation such as the EU Electronic Money Directive and the Payment Services Directive. This approach recognizes that there are basic differences between digital currencies and fiat currencies, and rules out against forcing a square peg in a round hole. [246]

In order to address the five (5) risk drivers, the EBA proposed several long-term regulatory measures to address these drivers.[247] These are discussed below. The next sub-section discusses the strengths and weaknesses of these proposals.

**1. The establishment of a scheme governance authority**

The EBA proposes the establishment of a *scheme governance authority*, a non-government

242 Ibid
243 Ibid
244 Ibid
245 Ibid
246 "Why the EBA Report is good news for digital currencies" (*Elliptic*, 08 July 2014) <https://www.elliptic.co/blog/91165773438/why-the-eba-report-is-good-news-for-digital-currencies#.VFDq91eC-Ck> accessed 29 October 2014
247 "EBA Opinion on 'Virtual Currencies'" (n20) 39-40, 42-43

entity the function of which is the maintenance of "the integrity of the central transaction ledger, the protocol, and any other core functional component"[248] of the virtual currency scheme. This authority would be required to "comply with regulatory and supervisory requirements of various kinds to mitigate identified risks."[249] It should be established as a legal person. For purposes of this discussion on the bitcoin system, it shall be referred to as the "bitcoin governance authority."

The proposal states that in a decentralized virtual currency scheme, like bitcoin, the function of a scheme governance authority can remain decentralized and "run, through, for example, a protocol and a transaction ledger"[250] which is what exactly happens under the bitcoin protocol. The proposal states that market participants "may establish themselves as scheme governance authorities."[251] Finally, "if a legal person is not able to exercise authority over market participants and is therefore unaccountable to a regulator for compliance purposes, it would be unreasonable to expect a regulator to guarantee integrity in their place."[252] This last statement means that in the absence of a legal entity that would ensure the integrity of the bitcoin system and be answerable to the regulator, then the regulator could not guarantee the integrity of the bitcoin system.

**2. Customer due diligence requirements**

To address the risk driver concerning the anonymity of payers and payees under the bitcoin system, the EBA proposes that bitcoin exchanges as well as any other "non-user market participants that interact"[253] with fiat currency comply with KYC requirements. These requirements would include the following: (1) collection/verification of basic information on identity; (2) cross-checking names against certain lists of known parties (such as 'politically exposed persons'); (3) determining the customer's risk profile in terms of the probability to commit money laundering; and (4) monitoring transactions of customer against their risk profile, and against that of the customer's peers.

Additionally, payer and payee information details have to be provided to the bitcoin governance authority, with the exception of "person-to-person transactions between wallets."[254] This would enable law enforcement agencies to link transactions to an individual's identity. Finally, the proposal states that "KYC requirements would need to be imposed on exchanges, *scheme governing authorities* and potentially on some other market participants too."[255]

248 "EBA Opinion on 'Virtual Currencies'" (n20) 39
249 Ibid
250 "EBA Opinion on 'Virtual Currencies'" (n20) 40
251 Ibid
252 Ibid
253 "EBA Opinion on 'Virtual Currencies'"(n20) 40
254 Ibid
255 Ibid

**3. Establishment of fitness and probity standards**

To address the risk driver concerning the absence of fitness and probity of individuals that make decisions to the detriment on other market participants, the EBA proposed that "fitness and probity standards" be required for individuals that perform certain tasks in the bitcoin governance body, bitcoin exchange and other relevant market participants in the bitcoin system. Such standards require that individuals that perform these specific functions be "competent and capable, honest, ethical, financially sound and to act with integrity."[256]

**4. A global regulatory approach**

To address the risk driver concerning the global, internet-based nature of the bitcoin system, the proposal requires a regulatory approach to aim for an "international, and ideally global, coordination"[257] in order to accomplish a successful regulatory framework. Without such global approach, the proposal requires that national regulators be required "to issue continued warnings to potential users to make them aware of the risks of VC schemes that do not comply with the regulatory regime."[258]

**5. Submission of reports on transactions**

To address the risk driver concerning the lack of reporting requirements to any authority, the proposal requires that relevant market participants submit "specified documents to regulators, including the results of their transaction monitoring … in addition to an obligation to report suspicious transactions."[259]

### *4.2.2 Short-term AML regulatory measures*

The EBA recognizes that the development and implementation of a comprehensive regulatory framework for virtual currencies would be highly resource-intensive and may take quite a long time to develop. Based on the ratings made by the EBA, risks to financial integrity, particularly, money laundering risks are considered to be of high probability of occurrence. Recognising this, the EBA suggests that EU legislators and national supervisory authorities in the EU Member States consider short-term AML regulatory measures for bitcoins and other virtual currencies. The EBA hopes that these short-term measures, discussed below, would allow virtual currency to further innovate and develop outside of the regulated financial services sector, while finding

256 Ibid
257 "EBA Opinion on 'Virtual Currencies'" (n20) 43
258 Ibid
259 "EBA Opinion on 'Virtual Currencies'" (n20) 44

solutions that would satisfy the long-term regulatory requirements set out above.[260]

First, due to the high risks of money laundering involved in the use of virtual currencies, the EBA recommends that "national supervisory authorities should discourage credit institutions [e.g. banks[261]], payment institutions [e.g. money remittance services, FX services[262]] and e-money institutions from buying, holding or selling" virtual currencies. This response would mitigate the risks associated with interactions between the bitcoin system and the regulated financial services, hence, "shielding" regulated financial services from VCs.

The EBA also proposes that virtual currency exchanges be declared as *obliged entities* that that are required to comply with anti-money laundering requirements set out in the EU Anti-Money Laundering Directive (Directive 2005/60/EC of the European Parliament and of the Council). The Directive required Member States to require their credit institutions and other financial institutions to perform KYC measures on their customers on a risk-sensitive basis,[263] keep appropriate records of transactions of their customers for a period of at least five (5) years for purposes of conducting investigation or analysis of money laundering,[264] and to report any instances of money laundering to the proper authorities, including suspicious transactions.[265] These obligations are akin to the three-fold compliance obligations of financial institutions under the UNCAC, UNCTOC and the FATF Recommendations.

## 4.3 *How can the proposed AML regulations be improved? How can bitcoins be regulated in the EU?*

### *4.3.1 Strengths and limitations*

Most of the proposed long-term and short-term regulatory measures appear to be similar to the AML measures that are already in place for currently AML-regulated financial institutions. These preventive measures target bitcoin exchanges and other non-user market participants that interact with fiat currency. Targeting these AML measures against bitcoin exchanges is a step in the right direction because it is during transactions with exchanges that illegal proceeds

260 Ibid

261 "Credit institutions register" See <https://www.eba.europa.eu/risk-analysis-and-data/credit-institutions-register> accessed 28 October 2014

262 "What is a payment institution?" <http://www.paymentinstitutions.eu/about-epif/the-payment-institutions-sector/about> accessed 28 October 2014

263 Directive 2005/60/EC of the European Parliament and of the Council, Chapter II. <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005L0060&from=EN> accessed 29 October 2014

264 Directive 2005/60/EC of the European Parliament and of the Council, Chapter II, Article 30. <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005L0060&from=EN> accessed 29 October 2014

265 Directive 2005/60/EC of the European Parliament and of the Council, Chapter II, Article 22 (a). <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005L0060&from=EN> accessed 29 October 2014

are converted into bitcoins (or, alternatively, illegal proceeds in the form of bitcoins are converted into cash or other forms of digital currency) thus triggering the first of the three (3) stages of money laundering.

Nonetheless, the main three-fold compliance obligations under the UNCAC, UNCTOC and the FATF Recommendations require jurisdictions to put in place CDD controls, suspicious transaction reporting and record-keeping. The proposals contain two out of these three obligations, but failed to include the obligation to keep records for investigation and law enforcement purposes. This obligation to retain records for at least a period of five (5) years is of fundamental significance because it allows the preservation of documents and information relating to bitcoin users so that law enforcement authorities could access them for purposes of investigating money laundering offenses. These documents are primary evidence of money laundering and their destruction or loss would hamper the efforts of law enforcement.

Furthermore, the proposal that KYC requirements should also be imposed on the bitcoin [scheme] governing authority is misplaced. KYC requirements are due diligence procedures that are performed by businesses before beginning a business relationship with a customer and after its commencement. As framed by the Opinion, a scheme governing authority is a legal person with the function of maintaining the integrity of the central transaction ledger, the protocol, and any other core functional component of the digital currency scheme, in this case, the bitcoin system, and would be accountable to the regulator. Hence, it does not deal with customers or bitcoin users in the way that a bitcoin exchange does and it does not interact with fiat money. The proposals do not even require exchanges and other relevant market participants to submit KYC documents to the scheme governing authority; KYC documents are usually submitted to the financial intelligence unit (FIU). A fair regulatory measure in keeping with the defined function of a scheme governing authority would have been to require it to keep records of the integrity of the system and produce them for the inspection of law enforcement authorities and regulatory authorities.

The proposal to establish a scheme governance authority for digital currency schemes has been met with a lot of opposition by bitcoin followers mainly for reasons of the non-practicality of such measure.[266] One of the criticisms is that the proposal attempts, in the case of bitcoin, "to regulate the [bitcoin] protocol itself, rather than the businesses offering [bitcoin] services"[267] such as bitcoin exchanges. This criticism is valid in view of the proposal to impose KYC obligations on the scheme governance authority as discussed above.

As suggested earlier, the imposition of this KYC requirement is misplaced, and if the KYC

266 "Why the EBA Report is good news for digital currencies" (n246)
See <https://www.elliptic.co/blog/91165773438/why-the-eba-report-is-good-news-for-digital-currencies#.VFEFR1eC-Ck> accessed 29 October 2014

267 Ibid. See <https://www.elliptic.co/blog/91165773438/why-the-eba-report-is-good-news-for-digital-currencies#.VFEFR1eC-Ck> accessed 29 October 2014

requirement on scheme governance authorities is revoked, then the proposal on the creation of a scheme governance authority would be welcome. It would provide a measure of reliability and stability to the system when the regulators know which legal person to hold accountable in case of problems with the integrity of the system. It has to be clarified, however, that the scheme governance authority is only accountable for problems with the integrity of the system, and not AML regulatory concerns because it is not privy to the transactions involving bitcoins and fiat currency.

The short-term measures recommended in the Opinion propose that bitcoin exchanges be declared as "obliged entities" that are required to comply with the three-fold AML requirements under the EU Anti-Money Laundering Directive, while at the same time discourages regulated credit and financial institutions from dealing with bitcoins. The inclusion of bitcoin exchanges within the scope of existing AML regulations provide these businesses the much-needed legitimacy[268] that would allow them to grow and innovate in the interim, without being burdened with the public perception that these businesses are instruments of money laundering. This proposal is also helpful to exchanges that have been refused by banks to open accounts for reasons of lack of AML oversight in the exchanges' businesses.[269] The proposal discourages banks from buying, holding or selling bitcoins but does not prevent them from being indirectly involved with bitcoins such as providing bank accounts to bitcoin exchanges. This measure would allow digital currencies to continue to innovate and develop while within the umbrella of the EU AML Directive, but separated from regulated financial institutions.

### *4.3.2 Proposals for a stronger EU AML framework on bitcoins*

The previous Chapter illustrated the interaction between several bitcoin exchanges and the traditional financial system, in particular, banks and money transmitters, when these institutions are used as conduits to transfer money to bitcoin exchanges. Using regulated financial institutions as conduits may, at first blush, appear to be a desirable measure from an AML perspective because the movement of funds from these institutions to the bitcoin exchange is captured and placed within government radar as these institutions are subject to the three-fold AML compliance requirements.

However, it should be noted that when funds are transferred from the purchaser's bank account to the bitcoin exchange's bank account, there is no sure way for the bank to know that the funds would be used to purchase bitcoins. On record, the bank knows that a transfer was made from

268 Ibid

269 Since banks are subject to AML requirements, a customer such as a bitcoin exchange that potentially may have customers that launder money, may commingle these funds in the exchange's account. The bank could then be potentially holding illegal proceeds without its knowledge. See <https://www.elliptic.co/blog/91165773438/why-the-eba-report-is-good-news-for-digital-currencies#.VFEFR1eC-Ck> accessed 29 October 2014

Juan's bank account to the bank account of X exchange, but the underlying transaction is not known to the bank and the user may provide any number of false reasons to hide the transaction from the bank. In other cases, the bitcoin exchange may use a payment processor (as in the case of BitInstant) and the funds are transferred to the account of the payment processor, and not in the exchange's name. Furthermore, banks do not interact with both parties to the exchange transaction, and hence, it is not in the best position to know the details of the bitcoin exchange. For these reasons, using conduits does not ensure that the necessary and required AML information would be extracted, recorded and reported.

More importantly, money launderers and other criminal elements eschew traditional transparent payment methods like credit cards, debit cards, personal checks and the like, preferring the anonymity of cash when buying bitcoins. Using cash, they deal directly with exchanges for purchases involving large amounts, but for smaller amounts, the services of websites that match them up with potential sellers could be utilized.

In light of these circumstances, the question of transparency and the need to regulate these transactions from an AML perspective becomes more apparent and pressing. The two questions that require resolution when framing regulatory measures are: Who is the subject of the regulation? What are the regulatory measures? These questions and possible answers to these are discussed below.

**Target entities**

1. **Regulate bitcoin exchanges as "obliged entities"**

As previously discussed, money laundering is committed when illegal proceeds are exchanged for bitcoins and when bitcoins that are considered as illegal proceeds are exchanged for other currencies, fiat or digital. There is also money laundering when such bitcoins are used to purchase goods and services from merchants. To be effective, AML preventive regulations should target those market participants that are in the best position to interact with the parties to the transaction. The *possible* "points of contacts" in the aforecited transactions are bitcoin exchanges/other trading platforms as well as merchants accepting bitcoins as means of payment.

Bitcoin exchanges are often considered the gateway to the bitcoin system because they facilitate the exchange between bitcoins and fiat currency or other currencies, thus triggering the first stage of money laundering, i.e. placement. Users that wish to participate in the bitcoin community, including criminals holding illegal proceeds from unlawful activities, would need to exchange their fiat currency for bitcoins. Bitcoin exchanges deal directly with holders of fiat currency, including holders of proceeds of criminal activities. Thus, a bitcoin exchange is in the best position to conduct KYC procedures on its customers, keep records of their transactions, and report any suspicious transactions to the proper authorities. In a way, bitcoin exchanges are

analogous to FX exchanges, an AML-regulated industry, and bitcoins are analogous to a foreign currency, the only difference being that, it is not, unlike a foreign currency, a fiat currency. The facilitation by a bitcoin exchange of the exchange of fiat money to bitcoins and vice versa, like an FX exchange, triggers the first stage of money laundering, putting them in the best position to perform the AML compliance obligations.

On the other hand, it would not be wise from the point of view of AML regulation to impose AML compliance obligations on merchants, the "point of contact" for transactions involving purchases of goods and services. First of all, imposing AML obligations on merchants would be unnecessary and would serve no AML purpose. Bitcoin exchanges, being the gateway to the bitcoin system, already capture the necessary information when they perform KYC, report suspicious transactions and keep records. To oblige merchants would lead to a double reporting to the financial intelligence units which would burden and tax the FIU's systems. Second, it would be outright burdensome and unnecessarily oppressive to businesses to require merchants to require personal identification details, and ascertain whether a transaction is suspicious or not. For these reasons, even in transactions using fiat currency, merchants are not considered obliged entities. There is no reason why transactions using bitcoins should require double reporting.

Finally, the question of whether users and miners may be regulated has been the subject of a study. In that study, it was concluded that there are obstacles to regulating the ordinary bitcoin user or money launderer because of the "pseudonymous dispersed nature" of the identities of users in the bitcoin system. Unless there is contextual or independently available identifying information on the user, the probability of sufficiently identifying users or money launderers is very low. Furthermore, targeting users could lead to increased distrust in the government and increased efforts at anonymization. As to miners, while regulating them may ostensibly seem to fit within the AML scheme considering their role as "payment processors" in all bitcoin transactions, there is no user intervention during the processing of transactions as all mining activity is done by software. Hence, it would be difficult to prove *mens rea.*[270]

### 2. Regulate trading platforms as "obliged entities"

Furthermore, it is possible that suspicious transactions in smaller amounts may fall through the cracks and remain uncaptured or unreported. This is because, at least for smaller amounts (as discussed in Chapter 3), it is possible to exchange bitcoins for real currency and vice versa using services provided by trading platforms such as localbitcoins.com which directly match purchasers and buyers within their vicinity. In localbitcoins, the user types in her location, the amount of the transactions and whether she would like to buy or sell bitcoins. Another website, cointouch.com, locates buyers or sellers of bitcoin within one's extended social network, using

270 Bryans (n171) 470

Facebook or Google accounts.[271] While these two (2) websites provide their services for free, there may be others existing now or in the future that may offer similar services for a fee. If so, then a possible solution to capture transactions of *de minimis* amounts but may potentially be suspicious is to impose the AML obligations on trading platforms offering direct trades, like localbitcoins.com and similar entities.

### 3. Allow banks to deal in the exchange of bitcoins

Another measure is to allow banks to engage in the business of exchanging bitcoins for fiat currency thus making purchases/sales of bitcoins for fiat currency subject to the usual AML measures conducted by banks. This measure could be a desirable alternative to the proposal under the Opinion to include exchanges as AML obliged entities. Presently, many banks are reluctant to accommodate business from bitcoin market participants. The main reason for this is the lack of an AML regulatory framework for bitcoin participants (on their own customers), which effectively forces banks to play the role of regulators, creating an additional work for them as they conduct AML procedures on their own customers.[272] If banks were allowed to trade in bitcoins and fiat currency, such as in buying and selling bitcoins, then banks would be obliged to perform KYC, record-keeping and suspicious transaction reporting on its bitcoin customers, thus capturing bitcoin purchases/sales within the AML framework. This might reasonably be a welcome arrangement for banks as this provides additional business opportunities.

### 4. Regulate bitcoin ATMs

Regulators should also look into exchange transactions using bitcoin ATMs. Money launderers may exploit loopholes in the law by utilizing bitcoins ATMs to cash in or out their bitcoins because ATM transactions can be made without human intervention. The number of ATMs and the number of ATM transactions is slowly increasing. In Europe, as of September 2014, there are 64 bitcoin ATMs spread out over 20 countries in the EU.[273] In Canada, a bitcoin ATM had 81 transactions with a value of CND$10,000 on its first day , and $30,000 on its second day.[274]

Regulators could impose KYC requirements by requiring users of ATMs to submit identifying information such as their name, address, phone number, a government ID, a palm vein scan,

---

271 See <https://www.cointouch.com/> accessed 30 October 2014

272 Kashmir Hill, "Bitcoin companies and entrepreneurs can't get bank accounts" *Forbes* (US, 15 November 2013) <http://www.forbes.com/sites/kashmirhill/2013/11/15/bitcoin-companies-and-entrepreneurs-cant-get-bank-accounts/> and <http://www.coindesk.com/real-reason-banks-dont-like-bitcoin/> accessed 31 October 2014

273 Sharkey (n107)

274 Kashmir Hill, "Why are people so excited about a bitcoin atm?" *Forbes* (US, 31 October 2013) <http://www.forbes.com/sites/kashmirhill/2013/10/31/why-are-people-so-excited-about-a-bitcoin-atm/> accessed 04 November 2014

and allow the ATM to take their photo.[275] This concept was borrowed from a bitcoin ATM developed by Robocoin, an entity based in Las Vegas, USA. The KYC measures were specifically built into the ATM to comply with money laundering regulations.

That the transactions occur without human intervention does not excuse the owners or operators of the ATM machines from complying with suspicious transaction and currency transaction reporting. Because operators have information on customer and transactions details, they could theoretically make a reasonable judgment whether a transaction is suspicious or not. Currency transaction reports are easier to make because the only criterion is the amount of the transaction.

**AML Preventive Measures**

**5. Specify KYC information required for bitcoin transactions**

KYC procedures should apply risk-based procedures to identify and verify customer identity using reliable and independent sources, identifying beneficial owners, or whether such customers are politically exposed persons. Bearing in mind that bitcoins, not fiat currency, are being traded, at the very least the following information should be obtained from customers: identity and physical address of parties involved (i.e. the buyer and seller), the amount of the transaction, the denomination of the currency sold or purchased, the means of payment and the date of the transactions.[276]

**6. Provide specific guidance on "suspicious transactions"**

It would be a wise move to provide bitcoin exchanges and other relevant market participants some guidance on what should be considered or deemed suspicious transactions. An example of this would be to provide a list or enumeration of transactions that are deemed to be suspicious, with a catch-all item providing for "analogous instances." This would not only delimit but also properly capture all transactions which in the mind of legislators are suspicious transactions. A provision of this kind in the regulation would prevent confusion on the part of employees of bitcoin exchanges on the interpretation of what a "suspicious transaction" should be. FATF Recommendation 20 (Reporting of Suspicious Transactions) does nothing to provide enlightenment on this matter as the provision merely states that a financial institution should report suspicious transactions when it "suspects or has reasonable grounds to suspect that

275 Adrienne Jeffries, "The new gold rush: bitcoin ATMs are coming" (*The Verge,* 10 March 2014) <http://www.theverge.com/2014/3/10/5490534/the-new-gold-rush-bitcoin-atms-are-coming> accessed 04 November 2014

276 Section 200.15 (d)(1) of the proposed New York Codes, Rules and Regulations, Title 23. Department of Financial Services Chapter I. Regulations of the Superintendent of Financial Services Part 200. Virtual Currencies. <http://www.dfs.ny.gov/about/press2014/pr1407171-vc.pdf> accessed 03 November 2014

funds are the proceeds of a criminal activity."[277] The FATF Recommendations being merely recommendatory in nature, the use of the phrase in the FATF provision does not mean that jurisdictions are prohibited from providing clearer guidance for their covered institutions/persons on suspicious transactions, as in fact is done in some countries.

It would be helpful to define a "suspicious transaction", for instance, by way of enumeration of any of the circumstances where a suspicious transaction might arise. These would include, for example, transactions where, to the knowledge of the bitcoin exchange, there is no apparent underlying trade, or economic justification; where the amount involved in the transaction is not proportionate to the financial capacity of the customer based on his profile; where there appears to be a structuring of the transactions; in a case where a particular transaction appears to deviate from the profile of the customer; or, where clearly, the bitcoin exchange knows or has reason to suspect that the money involved are illegal proceeds of an unlawful activity.[278]

**7. Incorporate record-keeping obligations**

In addition, the proposed AML regulatory measures should include a provision on the record-keeping obligations of exchanges and other trading platforms. This obligation is one of the three mandatory obligations of covered persons/ institutions under the UN Convention against Corruption and the UN Convention against Transnational Organized Crime. FATF Recommendation 11 requires the retention of records for at least a period of five (5) years. The record-keeping obligation is of fundamental significance because it mandates the preservation of documents and information relating to bitcoin users so that law enforcement authorities could access them for purposes of investigating money laundering offenses. These documents are primary evidence of money laundering and their destruction or loss would hamper the efforts of law enforcement.

**8. Include an obligation to report currency transactions in excess of a certain threshold**

In addition to the three-fold AML compliance obligations, bitcoin exchanges and other trading platforms could also be required to report transactions that are in excess of a certain threshold, say, for instance the equivalent of US$ 10,000. Under United States law, this is the obligation to file the so-called currency transaction report.[279] While these reports do not trigger a money

277 See FATF Recommendation 20.
<http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf> accessed 30 October 2014.
The FATF Recommendations are not binding on covered institutions/persons. They are merely recommendatory in nature and are adopted by jurisdictions as globally endorsed international standards against money laundering. Covered institutions/person become by AML regulations of their country's AML laws.

278 Taken from the Revised Implementing Rules and Regulations of Republic Act No. 9160 (the Philippines' Anti-Money Laundering Law). <http://www.amlc.gov.ph/archive/irr.pdf> accessed 30 October 2014

279 See 31 U.S. Code § 5313 - Reports on domestic coins and currency transactions

laundering investigation because of the absence of a "suspicion" of money laundering, these reports are important to investigators and law enforcement, because they preserve a record of potential money laundering activities that involve large deposits and transactions[280] that investigators could look into when a money laundering investigation has already commenced.

### 9. Require trading platforms to use regulated financial institutions

Market participants that deal in the interaction between bitcoins and fiat currency and other currencies may also be required, *alternatively*, to course their payment through banks (over-the-counter payments), money transmitters and other AML-regulated-financial institutions. This measure specifically targets the customers of market participants that could not be included as obliged persons, in order that transactions from the customers of these market participants could be properly identified by banks and other regulated financial institutions. The market participants contemplated here are those that offer "*de minimis*" services and whose inclusion as obliged entities proves to be too burdensome, unnecessary and not proportionate to the AML objective because of the low volume of transactions, or because the service is free of charge, or because the transaction between the parties does not require the active intervention by the service provider. An example of this would be services offered by a website or social network that merely match up buyers and sellers (localbitcoins and cointouch are examples of these). Particularly, due to lack of active intervention by the service provider in each transaction, the conduct of KYC procedures and the detection of suspicious transactions might be more problematic. Hence, in this case, because KYC procedures would be conducted by the bank or the money transmitter, the AML obligation here is on the bank or the money transmitter.

### 10. Require the use of "transparent" payment methods

An alternative measure that would capture customer and transaction details made through localbitcoins, cointouch and similar "de *minimis*" services, is to prohibit cash payments and instead require payment through wire transfers, online banking, or, where applicable, credit card and debit card, PayPal, postal money orders, personal checks and similar means of payment which automatically capture customer identifying and transaction information. Most of these payment methods are already utilized by most bitcoin exchanges. These payment services leave a paper trail on the customer information and transaction details and provide important information to investigators and law enforcement. While this measure falls short of the full KYC procedure outlined under the EU Money Laundering Directive and the FATF Recommendations, it is proportionate to the so-called "*de minimis*" services offered by these businesses.

---

<http://www.law.cornell.edu/uscode/text/31/5313> accessed 30 October 2014

280 "Currency transaction report" <http://boards.straightdope.com/sdmb/showthread.php?t=362797> accessed 30 October 2014

**Supervision and oversight**

### 11. Create a supervisory authority over bitcoin exchanges and require registration with the supervisory authority

There should be a government agency with the function of regulating, monitoring and supervising the operations of exchanges and other relevant market participants *from an AML perspective*. This function could be performed by a newly-created agency, or an existing agency, such as the central bank. Exchanges and relevant market participants should be registered with the supervisory authority. Registration ensures that its undertaking is recognized as a *bona fide* entity by the supervising authority and is made subject to its supervision and oversight.

To ensure compliance of relevant market participants with AML obligations, the supervisory authority, in this case, the central bank, should be empowered to conduct an examination of the records of the exchanges, as may be necessary in order to determine whether there has been compliance with applicable AML rules and regulations. The concept of an AML examination is derived from the power of the central bank to conduct an "examination to determine compliance with laws and regulations,"[281] including AML regulations issued by the central bank.

The supervisory authority contemplated here should be distinguished from the scheme governance authority proposed by the EBA. The scheme governance authority is "responsible for maintaining the integrity of the … core functional component" of the bitcoin network, and as such is accountable only for problems in the integrity of the bitcoin system, and not AML concerns because it is not privy to transactions using bitcoins. The supervisory authority, on the other hand, would regulate bitcoin exchanges. Because exchanges are in the best position in the bitcoin system to conduct AML measures inasmuch as they deal in transactions using bitcoins and fiat currency and they are in the position to know the customers and the nature of transactions. It follows then, that a regulatory measure placing bitcoin exchanges and other trading platforms under the supervision of supervisory authorities is more effective than the establishment of a scheme governance authority for purposes of AML regulation.

### 12. Require an AML license for bitcoin exchanges and other trading platforms

Exchanges and other trading platforms should be required to obtain an *AML* license *prior* to operation. Without an AML license, these entities should face certain restrictions such as being prohibited from opening bank accounts. This restriction ensures that exchanges are not used for money laundering. The AML licenses could only be issued when the regulatory authority is satisfied that the applicant has the technical and operational expertise and readiness to comply

281 See General Banking Law of the Philippines (R.A. 8791), Section 4.2 <http://www.bsp.gov.ph/downloads/regulations/gba.pdf> accessed 31 October 2014

with its AML obligations by having in place AML policies setting forth the company's AML prevention programs, appropriate technical systems (to flag currency and suspicious transactions, to identify politically exposed persons, to cross check against databases or lists of persons against whom of freeze orders, from the United Nations Security Council and the OFAC, among others), and has sufficiently trained its AML personnel. The idea for an AML "license" is borrowed from the concept of an AML registration required for Canadian exchanges prior to operation.[282]

**Protections and sanctions**

### 13. Include safe harbour provisions

The legal framework should also incorporate safe harbour provisions for employees of bitcoin exchanges and relevant market participants, prohibiting the filing of any criminal, civil or disciplinary proceedings against them for having acted in the performance of their duties in making a suspicious transaction report or a "currency transaction report" as suggested above. This provision is borrowed from the Anti-Money Laundering and Anti-Terrorism Financing Act of Malaysia.[283] This provision would ensure that employees and officers are not hampered by threats of prosecution for disclosing details of customer identity and transaction information to the relevant government authorities.

### 14. Require exchanges to put up bond

A bond may also be required to answer for the liability of exchanges for the protection of their customers. The requirement may be imposed on exchanges as security in case of liquidity problems, to address situations similar to the fate of Mt. Gox, or to answer for civil liability.

### 15. Institute a comprehensive sanctions system to deter money laundering

To ensure that exchanges and other relevant market participants comply with their AML obligations, Members States should establish a legal framework with penal, civil and administrative sanctions for officers and employees who knowingly allow or facilitate the commission of money laundering offenses, and hefty fines for legal persons. A comprehensive AML sanctions system has a huge deterrent effect by sending a strong signal to covered

---

282 Christine Duhaime, "Canada implements world's first national bitcoin law" (Duhaime Law, 22 June 2014) <http://www.duhaimelaw.com/2014/06/22/canada-implements-worlds-first-national-bitcoin-law/> accessed 31 October 2014. According to Duhaime, "[o]n June 19, 2014, the Parliament of Canada approved [Canada's] national law on digital currencies.
Canada's Governor General gave Royal Assent to Bill C-31, *An Act to Implement Certain Provisions of the Budget Tabled in Parliament on February 11, 2014 and Other Measures.*"

283 See Anti-Money Laundering, Anti-Terrorism Financing Act and Proceeds of Unlawful Activities Act 2001 (Act 613), Part IV, 24 <http://www.bnm.gov.my/index.php?ch=en_legislation&pg=en_legislation_act&ac=879>. Part IV, Section 24.

persons/institutions and the officers and employees that there are undesirable consequences to their wilful failure to comply with their AML obligations.

In regard to employees and officers of covered institutions, it might be helpful to criminalize the act of facilitating a transaction, knowing that it constitutes a money laundering offense, or the wilful failure to disclose a suspicious transaction, knowing it to be so. This would measure would help deter the commission of money laundering by bitcoin exchanges and their officers and employees, as illustrated in the prosecution of Charlie Shrem, the owner of BitInstant.

**Other regulatory approaches**

### 16. Clarify the scope of the regulation

The regulatory framework should clarify that the EU AML regulatory framework on bitcoins should apply when bitcoin exchange transactions are made on an online platform when these websites are accessible within a Member State's jurisdiction, provided that there is maximum harmonization of the provisions in Member States. For bitcoin ATMs, the AML framework should also apply where the ATM is located in any Member State.

### 17. Require minimum capitalization requirements

There should be minimum capitalization requirements for exchanges and trading platforms that facilitate the exchange of bitcoins to fiat currency and other digital currencies to encourage responsible business that have enough capital and discourage shadowy entities from engaging in the business of exchanging bitcoins for fiat currency.

### 18. Taxation as a regulatory measure

It might also be helpful for Member States in the EU to consider taxing bitcoin transactions as an additional AML regulatory measure. This tax should be on top of the ordinary taxes already imposed on transactions using fiat currency, thus representing an additional imposition on users. One benefit to taxing bitcoins from a business point of view is that it is "another step towards legitimacy and would lead to greater adoption in the business world." From the government perspective, however, this measure would serve dual purposes: it would raise revenue for important functions of the government, and at the same time, would function to regulate bitcoin.

Regulation through taxation works by "incentivizing (subsidizing) activities [governments] wish to promote and by disincentivizing [penalizing] activities they wish to discourage." [284] Taxing

284 Reuven S. Avi-Yonah, "Taxation as Regulation: Carbon Tax, Health Care Tax, Bank Tax and other Regulatory

bitcoin transactions would provide a huge deterrent effect on the use of bitcoins for money laundering purposes. The imposition of tax on bitcoin transactions could reduce the volume of using bitcoins as means of payment, hence, *theoretically,* reduce over-all incidents of money laundering. More importantly, because of the link between tax evasion and money laundering, criminal elements that wish to launder proceeds of crimes would stay away from bitcoin because they would be required to pay taxes on bitcoin transactions (although this would obviously be the least of their concerns). Furthermore, using bitcoins without paying the necessary taxes would make offenders liable tax not only for tax evasion but also for money laundering, if tax evasion is already one of the predicate offenses for money laundering in their respective jurisdictions. Hence, taxing bitcoins transactions has a potentially huge deterrent effect on the use of bitcoins for money laundering ends.

Understandably, because bitcoin transactions of miners, users and merchants are harder to target using AML regulations, taxation seems to be the most effective means of regulating these market participants. A comprehensive tax treatment of bitcoins that would subject these participants to regulation is suggested below[285]:

Miners may be subject to two different kinds of taxes: (1) income tax – when an individual or an entity mines bitcoins as a source of income, or as a business, the income from that activity should be included in their gross income; (2) capital gains tax – when miners sell the bitcoins they mined, they should pay a tax on any gains due on the profit resulting from difference between the sale price and the fair market value of the bitcoins on the date of acquisition (or mining).

Users may be divided into two (2): investors and consumers. Capital gains tax may be applied in the transactions of both investors and consumers. In the case of investors, the tax may be applied to the profit realized from the gains realized from the difference between the sale price and the fair market value of the bitcoins as of the date of acquisition (or purchase). For consumers, the tax may be applied to any gains realized on the value of the bitcoin at the time of the purchase of a good or service. For example, when the value of a bitcoin increases from the time of its acquisition to the time of its use (for purchasing goods or service), say from 25 EUR (at date of acquisition of bitcoin) to 100 EUR (at date of purchase of a jacket using bitcoins), there is a capital gains of 75 EUR which is subject to capital gains tax. This suggestion would be administratively burdensome because it would require merchants to provide the current value in fiat currency of the bitcoin purchase, and in case of his failure to do so, the consumer would be required to provide this information for each and every bitcoin transaction.

For merchants who are paid in bitcoins, capital gains tax shall be applied to the profit realized

---

Taxes," Public Law and Legal Theory Working Paper Series Working Paper No. 216, August 2010, Empirical Legal Studies Center, Working Paper No. 10-020 University of Michigan Law School. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1664045> accessed 31 October 2014

285 Ibid

from difference between the selling price or exchange price of bitcoin and the fair market value at the time of acquisition (at the time of the sale of goods or services). This means that when a merchant, say Paulo, acquires 1 bitcoin with a value of 25 EUR at the time of the sale of his good, and exchanges that bitcoin for 100 EUR, then there is a profit of 75 EUR to which to which the capital gains tax rate should be applied.

# CONCLUSION

Technology, being a creation of the human mind, can be moulded to take on just about any feature humans value enough to incorporate into it. Bitcoin was born because of distrust in government-issued currencies and central bank policies, and is growing because it answers the desperately sought- after need for privacy in the midst of this age of ubiquitous government surveillance. The bitcoin system was designed to protect privacy by building anonymity features into the bitcoin technology making it difficult to link transactions with real world identities. This anonymity feature is complemented by a decentralized system essentially rendering the bitcoin P2P network free from centralized supervision and regulation making it problematic for the government to pinpoint accountability within the P2P network. Unfortunately, these characteristics have captured the attention, not only of people who wish to protect their anonymity for legitimate reasons, but also of money launderers who find in bitcoins the answer to their need to keep their illegal proceeds away from the government's prying eyes.

The response of governments all over the world has been varied. The EU is yet to develop its own framework but the signs have been promising as the European Commission is poised to heed the proposal of the EBA to regulate virtual currencies.[286] Meantime, the prospect of a "more anonymous" virtual currency is looming in the technological horizon,[287] predictably a boon to money launderers. The urgency of the clarion call of the EBA becomes clearer.

To be effective, AML regulation of bitcoin should occur at that point where the very first stage of money laundering is triggered, i.e. at placement, and should not unnecessarily burden market players, business, and the AML system. In the bitcoin system, the tipping point occurs at the level of bitcoin exchanges and trading platforms. Comprehensive AML preventive regulatory measures also mandate the inclusion of systems to make transactions in bitcoin proportionately more burdensome (such as taxation, capitalization requirements) and protection measures for individuals who perform AML procedures as mandated by law. This comprehensive approach to AML preventive regulation provides a more robust response to the money laundering risks identified by the EBA.

286 Leon Pick, "European Commission to impose rules on bitcoin after EBA bans financial institutions from dealing in it" (*Digital Currency Magnates*, 29 July 2014) <http://dcmagnates.com/european-commission-to-impose-rules-on-bitcoin-after-eba-bans-financial-institutions-from-dealing-in-it/> accessed 06 November 2014

287 Andy Greenberg, "Darkcoin, the shadowy cousin of bitcoin, is booming" *Wired* (California, 21 May 2014) <http://www.wired.com/2014/05/darkcoin-is-booming/> accessed 06 November 2014

# BIBLIOGRAPHY

## Legislation

Anti-Money Laundering, Anti-Terrorism Financing Act and Proceeds of Unlawful Activities Act 2001 (Act 613), at Part IV, 24

Directive 2005/60/EC of the European Parliament and of the Council, at Chapter II

Directive 2009/110/EC of the European Parliament and of the Council at Article 2 (2)

General Banking Law of the Philippines (R.A. 8791), at Section 4.2

Revised Implementing Rules and Regulations of Republic Act No. 9160 (the Philippines' Anti-Money Laundering Law), at Rule 3.g.2

United Nations Convention Against Corruption, at Articles 14 and 23

United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988

United Nations Convention Against Transnational Organized Crime, at Articles 6 and 7

31 U.S. Code, at § 5313

## Cases

US v Faeilla and Shrem [Indictment for Violations of 18 U.S.C. §§ 1950 and 1956; 31 U.S.C. §§ 5318 (g) and 5322 (a)], 14 MAG 0164 <http://www.justice.gov/usao/nys/pressreleases/January14/SchremFaiellaChargesPR/Faiella,%20Robert%20M.%20and%20Charlie%20Shrem%20Complaint.pdf> accessed 29 July 2014

US v Ulbricht 14-cr-68 (KBF) [United States District Court Southern District of New York] <http://www.scribd.com/doc/233234104/Forrest-Denial-of-Defense-Motion-in-Silk-Road-Case#download > accessed 18 August 2014 accessed 18 August 2014

US v Ulbricht [Indictment before the United States District Court Southern District of New York) 14 Crim 068 <http://www.justice.gov/usao/nys/pressreleases/February14/RossUlbrichtIndictmentPR/

US%20v.%20Ross%20Ulbricht%20Indictment.pdf> accessed 29 July 2014

## Secondary Sources

----, “Address” (en.bitcoin.it) <https://en.bitcoin.it/wiki/Address> accessed 21 August 2014. According to <https://en.bitcoin.it/wiki/Address> accessed 21 August 2014

----, “Advantages/Disadvantages” (bitcoinembassy.ca ) <http://bitcoinembassy.ca/about/what-is-bitcoin/advantages-disadvantages > accessed 01 August 2014

----, "Anonymity” (bitcoinsimplified.org) <http://bitcoinsimplified.org/learn-more/anonymity/> accessed 20 August 2014

----, "Bitcoin” (Bitcoinwiki) <https://en.bitcoin.it/wiki/Main_Page> accessed 30 July 2014

----, "Bitcoin” (P2P Foundation) <http://p2pfoundation.net/bitcoin> accessed 30 July 2014

----, “Bitcoin Addresses” (learncryptography.com) <http://learncryptography.com/bitcoin-addresses/ > accessed 21 August 2014

----, “Bitcoin ATM” <http://en.wikipedia.org/wiki/Bitcoin_ATM> accessed 04 November 2014

----, "Bitcoin frequently asked questions” (Bitcoin.org) <https://bitcoin.org/en/faq#what-determines-bitcoins-price> accessed 12 August 2014

----, “Bitcoin Frequently Asked Questions” (Bitcoin.org) <https://bitcoin.org/en/faq#who-created-bitcoin> accessed 12 August 2014

----, "Bitcoin mining” (Whatis.techtartget.com) <http://whatis.techtarget.com/definition/Bitcoin-mining > accessed 01 August 2014

----, "Bitcoin transaction fees explained” (Bitcoinfees.com) <http://bitcoinfees.com/> accessed 01 August 2014

----, “Buying Bitcoins (the newbie version). See <https://en.bitcoin.it/wiki/Buying_Bitcoins_%28the_newbie_version%29> accessed 24 October 2014

----, "Co-founder of Liberty Reserve Pleads Guilty to Money Laundering in Manhattan Federal Court” (US DOJ, 31 October 2013) <http://www.justice.gov/opa/pr/2013/October/13-crm-1163.html> accessed 02 September 2014

----, "Complete List of Bitcoin Exchanges" (Planetbtc.com) <http://planetbtc.com/complete-list-of-bitcoin-exchanges/ > accessed 02 August 2014

----, "Currency transaction report" <http://boards.straightdope.com/sdmb/showthread.php?t=362797> accessed 30 October 2014

----, "Did One of the Silk Road's Successors Just Commit the Perfect Bitcoin Scam?" (Motherboard, 02 December 2013) <http://motherboard.vice.com/blog/did-one-of-the-silk-roads-successors-just-commit-the-perfect-bitcoin-scam> accessed 04 September 2014

----, "EBA Opinion on Virtual Currencies 04 July 2014" (EBA/Op/2014/08) (EBA) <http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf> accessed 07 October 2014

---- FATF Recommendations <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf> accessed 04 September 2014

----, "FATF Report 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 12 August 2014

----, "Federal Bureau of Investigation Intelligence Assessment dated 24 April 2012" states "(u) Bitcoin virtual currency:unique features present distinct challenges for deterring activity" <http://www.scribd.com/doc/92797476/FBI-Bitcoin-Report-April-2012> accessed 29 August 2014

----, "Getting started with bitcoin" (bitcoin.org) <https://bitcoin.org/en/getting-started > accessed 20 August 2014

----, "How bitcoin mining works" Coindesk (UK) <http://www.coindesk.com/information/how-bitcoin-mining-works > accessed 02 August 2014

----, "How can I buy bitcoins?" (Coindesk, last updated 23 October 2014) <http://www.coindesk.com/information/how-can-i-buy-bitcoins/> accessed 05 November 2014

----, "How to sell bitcoin" (Coindesk) <http://www.coindesk.com/information/sell-bitcoin/> accessed 05 November 2014

----, "How to set up a wallet" (bitcoinsimplified.org) <http://bitcoinsimplified.org/get-

started/how-to-set-up-a-wallet/> accessed 20 August 2014

----, “International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation FATF Recommendations February 2012” <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf> accessed 08 October 2014

----, "Manhattan U.S. Attorney Announces Charges Against Bitcoin Exchangers, Including Ceo Of Bitcoin Exchange Company, For Scheme To Sell And Launder Over $1 Million In Bitcoins Related To Silk Road Drug Trafficking” (US DOJ, 27 January 2014) <http://www.justice.gov/usao/nys/pressreleases/January14/SchremFaiellaChargesPR.php > accessed 29 July 2014

----, "Manual on Countering Money Laundering and the Financing of Terrorism” (Asian Development Bank, January 2003) 4 <https://www.unodc.org/tldb/pdf/Asian-bank-guide.pdf > accessed 04 September 2014

----, "Mixing service” (en.bitcoin.it) <https://en.bitcoin.it/wiki/Mixing_service> accessed 03 September 2014

----, "Money Laundering and Globalization” (UNODC) <https://www.unodc.org/unodc/en/money-laundering/globalization.html > accessed 13 August 2014

----, "Mt. Gox bitcoin exchange news” (Coindesk) http://www.coindesk.com/companies/exchanges/mtgox/ accessed 20 August 2014

----, New York State Department of Financial Services Proposed New York Codes, Rules and Regulations Title 23. Department of Financial Services Chapter 1. Regulations of the Superintendent of Financial Services Chapter 1 Part 200. Virtual Currencies <http://www.dfs.ny.gov/about/press2014/pr1407171-vc.pdf> accessed 03 November 2014

----, “Proof of work,” <https://en.bitcoin.it/wiki/Proof_of_work> accessed 19 December 2014

----, “Regulation of Bitcoin in Selected Jurisdictions” (US Library of Congress) <http://www.loc.gov/law/help/bitcoin-survey/#denmark> accessed 07 October 2014

----, "SHA-256 and Scrypt Mining Algorithms” (coinpursuit.com) <https://www.coinpursuit.com/pages/bitcoin-altcoin-SHA-256-scrypt-mining-algorithms/> accessed 06 August 2014.

----, “Six Things Bitcoin Users Should Know about Private Keys” (Bitzuma, 23 April 2014) <http://bitzuma.com/posts/six-things-bitcoin-users-should-know-about-private-keys/> accessed 21 August 2014

----, “Statement of Jennifer Shasky Calvery, Director Financial Crimes Enforcement Network United States Department of the Treasury Before the United States Senate Committee on Homeland Security and Government Affairs” (US DOJ, 18 November 2013) < http://www.fincen.gov/news_room/testimony/html/20131118.html> accessed 02 September 2014

----, “Technology in the fight against money laundering in the new digital currency age” (Thomas Reuters, June 2013) <http://trmcs-documents.s3.amazonaws.com/cfbf4386891bc6cb7ee26f9690294222_20130617083834_AML%20White%20Paper.pdf> accessed 02 September 2014

----, “The Money Laundering Cycle” (UNODC)<https://www.unodc.org/unodc/en/money-laundering/laundrycycle.html> accessed 13 August 2014

----, "Transaction Fees” (Bitcoin wiki) <https://en.bitcoin.it/wiki/Transaction_fees > accessed 01 August 2014

----, "Virtual Currencies: Key Definitions and Potential AML/CFT Risks” (FATF) <http://www.fatf-gafi.org/topics/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html > accessed 12 August 2014

----,"Virtual Currency Schemes October 2012” 43 European Central Bank <http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf > accessed 07 August 2014

----, "Warning to Consumers on Virtual Currencies 12 December 2013” EBA/WRG/2013/01 (EBA) <http://www.eba.europa.eu/documents/10180/598344/EBA+Warning+on+Virtual+Currencies.pdf> accessed 07 October 2014

----, "What are public-private keys?” (explainbitcoin.com) <http://explainbitcoin.com/public-private-key/> accessed 21 August 2014

----, "What is bitcoin?” Coindesk (UK) <http://www.coindesk.com/information/what-is-bitcoin/> accessed 30 July 2014

----, "What is money laundering?” (FATF)<http://www.fatf-gafi.org/pages/faq/moneylaundering/ > accessed 04 September 2014

----, "Who we are" (FATF) <http://www.fatf-gafi.org/pages/aboutus/> accessed 13 August 2014

----, "Why the EBA Report is good news for digital currencies" (Elliptic, 08 July 2014) <https://www.elliptic.co/blog/91165773438/why-the-eba-report-is-good-news-for-digital-currencies#.VFDq91eC-Ck> accessed 29 October 2014

Anderson C, "US Bitcoin Case tests Money Laundering Limits"3news.co.nz (New Zealand, 10 April 2014) <http://www.3news.co.nz/US-bitcoin-case-tests-money-laundering-limits/tabid/417/articleID/339614/Default.aspx> accessed 29 July 2014

Ashutosh KS, "10 Things you need to know about bitcoins" (hongkiat.com) <http://www.hongkiat.com/blog/bitcoin-questions/ > accessed 07 August 2014

Avi-Yonah R S, "Taxation as Regulation: Carbon Tax, Health Care Tax, Bank Tax and other Regulatory Taxes," Public Law and Legal Theory Working Paper Series Working Paper No. 216, August 2010, Empirical Legal Studies Center, Working Paper No. 10-020 University of Michigan Law School. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1664045> accessed 31 October 2014

Ayzenberg M and Cecchetti A and Aggarwal A, "A Security Analysis of the Bitcoin Mining System" <http://static.squarespace.com/static/53168f6ce4b0ee73efea0c2a/t/53c5cc86e4b0cf6b53648339/1405471878208/Bitcoin%20Mining%20Security-%20Deja%20vu%20Security%20-%202014.pdf > accessed 01 August 2014

Barnett E R, "Virtual Currencies: Safe for Business and Consumers or just for Criminals?" (13th European Security Conference & Exhibition, The Hague, 02 April 2014) <http://photos.state.gov/libraries/useu/231771/PDFs/2014_Erik_Barnett_crypto-currencies_remarks.pdf > page 5 accessed 03 September 2014

Bayern S, "Of Bitcoins, Independently Wealthy Software, and the Zero-Member LLC" (108 Nw. U. L. Rev. Online 257 (2014) ; FSU College of Law, Public Law Research Paper No. 675 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2366197&download=yes> accessed 30 July 2014

Bischoff P, "Pick up your pickaxes and headlamps: here's how Bitcoin mining works" Techinasia.com (21 July 2014) <http://www.techinasia.com/how-min-bitcoin-works-guide-tutorial/ > accessed 06 August 2014

Blundell-Wignall A., (2014), "The Bitcoin Question: Currency versus Trust-less Transfer

Technology", OECD Working Papers on Finance, Insurance and Private Pensions, No. 37, OECD Publishing <http://www.oecd-ilibrary.org/content/workingpaper/5jz2pwjd9t20-en > accessed 12 August 2014

Bollen R, "The Legal Status of Online Currencies: Are bitcoins the future" (Journal of Banking and Finance Law and Practice [2013] <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2285247&download=yes> accessed 31 July 2014

Bradbury D, "The problem with bitcoin" Volume 2013 Computer Fraud & Security 11 <http://www.sciencedirect.com/science/article/pii/S1361372313701015> accessed 06 August 2014

Brito J and Castillo A, Bitcoin: A Primer for Policymakers (2012, Mercatus Center) 10 <http://books.google.nl/books?id=yC-nAwAAQBAJ&pg=PA26&lpg=PA26&dq=liberty+reserve+centralized&source=bl&ots=b3tOD-eOMD&sig=EWa3nyR3PGlB_SQGfETyd8tJeo0&hl=nl&sa=X&ei=9GEAVIPvCObI0QXerIHIBg&ved=0CEYQ6AEwBA#v=onepage&q=liberty%20reserve%20centralized&f=false> accessed 03 September 2014

Bronskill J, "Bitcoin's anonymity makes it ripe for crime: finance department memo" Huffington Post (US, 28 July 2014)) <http://www.huffingtonpost.ca/2014/07/28/bitcoin-anonymity-crime-finance-dept_n_5628126.html> accessed 31 July 2014

Brustein J, "Bitcoin May Not Be So Anonymous, After All" BusinessWeek (NYC, 27 August 2013) <http://www.businessweek.com/articles/2013-08-27/bitcoin-may-not-be-so-anonymous-after-all> accessed 29 August 2014

----, "Is this the man who created bitcoin?" Businessweek (United States, 06 March 2014) <http://www.businessweek.com/articles/2014-03-06/is-this-the-man-who-created-bitcoin> accessed 12 August 2014

Bryans D, "Bitcoin and Money Laundering: Mining for an Effective Solution" (89 Ind. L.J. 441 2014) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2317990> accessed 18 August 2014

Christopher CM, "Whack-a-Mole: Why Prosecuting Digital Currency Exchanges won't Stop Online Money Laundering" (18 Lewis & Clark L. Rev. 1, 2014) 21 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312787&download=yes> accessed 04 September 2014

Clozel L, "FEC allows political groups to accept bitcoin donations" LA Times (US, 8 May 2014)

<http://www.latimes.com/nation/politics/politicsnow/la-pn-fec-political-action-committees-bitcoins-20140508-story.html > accessed 12 August 2014

Duhaime C, “Canada implements world's first national bitcoin law” (Duhaime Law, 22 June 2014) <http://www.duhaimelaw.com/2014/06/22/canada-implements-worlds-first-national-bitcoin-law/> accessed 31 October 2014

Gilson D, “BitInstant temporarily shuts down service to work on next upgrade” Coindesk (UK, 13 July 2013) <http://www.coindesk.com/bitinstant-temporarily-shuts-down-service-to-work-on-next-upgrade/ > accessed 02 August 2014

Greenberg A, “Alleged Silk Road Creator's Lawyer Denies Bitcoin is Monetary Instrument Moves to Drop all Charges” Forbes (New York, 04 January 2014) <http://www.forbes.com/sites/andygreenberg/2014/04/01/alleged-silk-road-creators-lawyer-denies-bitcoin-is-monetary-instrument-moves-to-drop-all-charges/> accessed 29 July 2014

----, “Darkcoin, the shadowy cousin of bitcoin, is booming” *Wired* (California, 21 May 2014) <http://www.wired.com/2014/05/darkcoin-is-booming/> accessed 06 November 2014

----, “Alleged Silk Road Creator Ross Ulbricht Pleads not Guilty on all Charges” Forbes (New York, 02 July 2014) <http://www.forbes.com/sites/andygreenberg/2014/02/07/alleged-silk-road-creator-ross-ulbricht-pleads-not-guilty-on-all-charges/> accessed 29 July 2014

----, “Judge Shoots Down ‘Bitcoin Isn’t Money’ Argument in Silk Road Case” Wired (California, 09 July 2014) <http://www.wired.com/2014/07/silkroad-bitcoin-isnt-money/ > accessed 18 August 2014

----, “Feds seize Silk Road 2 in major Dark Web drug bust” Wired (US, 06 November 2014) <http://www.wired.com/2014/11/feds-seize-silk-road-2/> accessed 14 November 2014

Grinberg R, “Bitcoin: An Innovative Alternative Digital Currency” (4 Hastings Science & Technology Law Journal 162-165 ) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1817857&download=yes> accessed 01 August 2014

Kumar R, “Bitcoin explained in layman's terms” NDTV Profit (India, 27 December 2013) <http://profit.ndtv.com/news/your-money/article-bitcoin-explained-in-laymans-terms-376029> accessed 12 August 2014

Higgins S, “Ross Ulbricht Loses Bid to Dismiss Federal Silk Road Suit” (Coindesk, 10 July 2014) <http://www.coindesk.com/ross-ulbricht-loses-bid-dismiss-federal-silk-road-suit/> accessed 29 July 2014

Hill K, “Why are people so excited about a bitcoin atm?” Forbes (US, 31 October 2013) <http://www.forbes.com/sites/kashmirhill/2013/10/31/why-are-people-so-excited-about-a-bitcoin-atm/> accessed 04 November 2014

----, “Bitcoin companies and entrepreneurs can't get bank accounts” Forbes (US, 15 November 2013) <http://www.forbes.com/sites/kashmirhill/2013/11/15/bitcoin-companies-and-entrepreneurs-cant-get-bank-accounts/> accessed 31 October 2014

Huang L, “More Political Candidates Accepting Bitcoin Donations” (Bitcoin Vox, 5 August 2014) <http://bitcoinvox.com/article/905/more-political-candidates-accepting-bitcoin-donations> 12 August 2014

Jeffries A, “The new gold rush: bitcoin ATMs are coming” (The Verge, 10 March 2014) <http://www.theverge.com/2014/3/10/5490534/the-new-gold-rush-bitcoin-atms-are-coming> accessed 04 November 2014

Love D, “How to buy bitcoins completely anonymously” Business Insider (NYC, 10 December 2013) <http://www.businessinsider.com/how-to-buy-bitcoins-completely-anonymously-2013-12> accessed 03 September 2014

Lyne J, “$116 Million Bitcoins 'Found' At MtGox and How To Protect Your Wallet” Forbes (US, 21 March 2014) <http://www.forbes.com/sites/jameslyne/2014/03/21/116-million-bitcoins-found-at-mtgox-and-how-to-protect-your-wallet/ > accessed 12 August 2014

Mcmillan R, “The Inside Story of Mt. Gox, Bitcoin’s $460 Million Disaster” *Wired* (California, 03 March 1014) <http://www.wired.com/2014/03/bitcoin-exchange/> accessed 12 August 2014

----, “Sure, you can steal bitcoins. But good luck laundering them” *Wired* (California, 27 August 2013) <http://www.wired.com/2013/08/bitocoin_anonymity/ > accessed 02 September 2014

Meiklejohn S et al., “A fistful of bitcoins: characterizing payments among men with no names” <http://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf > accessed 02 September 2014

Moser M et al., “An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem” See <https://www.wi.uni-muenster.de/department/groups/security/people/malte-moeser/publications> and <https://maltemoeser.de/paper/money-laundering.pdf> accessed 09 October 2014

Moshinsky B and Brunsden J, “Bitcoin faces regulatory backlash as EU tells banks to stay away” Bloomberg (New York, 04 July 2014) <http://www.bloomberg.com/news/2014-07-

04/bitcoin-faces-regulatory-backlash-as-eu-tells-banks-to-stay-away.html> accessed 07 October 2014

Nakamoto S, “Bitcoin: a Peer-to-Peer Electronic Cash System” 1 <https://bitcoin.org/bitcoin.pdf> accessed 12 August 2014

Nesmith S, “ Bitcoin Charges Improper under Florida Law Lawyer Says” Bloomberg (New York, 28 February 2014) <http://www.bloomberg.com/news/2014-02-27/bitcoin-charges-improper-under-florida-law-lawyer-says.html> accessed 29 July 2014

----, "Bitcoin Charges Against Miami Man May Proceed, Judge Says” Bloomberg (US, 07 March 2014) <http://www.bloomberg.com/news/2014-03-07/bitcoin-charges-against-miami-man-may-proceed-judge-says.html> accessed 18 August 2014

Pacia C, “Bitcoin Mining explained like you're 5: Part 1--Incentives” <http://chrispacia.wordpress.com/2013/09/02/bitcoin-mining-explained-like-youre-five-part-1-incentives/ > accessed on 06 August 2014.

----, “Bitcoin Mining explained like you're 5: Part 2 – Mechanics” <http://chrispacia.wordpress.com/2013/09/02/bitcoin-mining-explained-like-youre-five-part-2-mechanics/> accessed 06 August 2014

Pagliery J, “Bitcoin exchange CEO arrested for money laundering” CNN (US, 28 January 2014) <http://money.cnn.com/2014/01/27/technology/security/bitcoin-arrest/ > accessed 29 July 2014

Pick L, “European Commission to impose rules on bitcoin after EBA bans financial institutions from dealing in it” (*Digital Currency Magnates*, 29 July 2014)<http://dcmagnates.com/european-commission-to-impose-rules-on-bitcoin-after-eba-bans-financial-institutions-from-dealing-in-it/> accessed 06 November 2014

Plassaras N, “Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF” (Chicago Journal of International Law, 14 Chi J Intl L [2013] Forthcoming) 6 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2248419&download=yes> accessed 30 July 2014

Quintaro P, “Why Julian Assange of Wikileaks loves bitcoins” (Benzinga, 15 June 2011) <http://www.benzinga.com/general/politics/11/06/1172451/why-julian-assange-of-wikileaks-loves-bitcoin#ixzz38xFgNVnQ> accessed 31 July 2014

Randewich N, “Bitcoin sinks in value after FBI busts Silk Road drug market” Reuters (08 October 2013) <http://www.reuters.com/article/2013/10/08/net-us-crime-silkroad-bitcoin-

idUSBRE99113A20131008> accessed 05 September 2014

Shandrow K L, “Bitcoin Millionaire Charlie Shrem Under House Arrest Following Federal Indictment” Entrepreneur (California, 15 April 2014) <http://www.entrepreneur.com/article/233107> accessed 29 July 2014

Sharkey T, “Europe's top 5 countries for bitcoin ATMs” (Coindesk, 14 September 2014) <https://www.coindesk.com/5-popular-european-countries-bitcoin/> accessed 04 November 2014

Sparkes M, “How to get your virtual hands on some bitcoins” The Telegraph (UK, 15 January 2014) <http://www.telegraph.co.uk/technology/news/10559175/How-to-get-your-virtual-hands-on-some-bitcoins.html> accessed 20 August 2014

Storm D, “Huge bitcoin heist: Black market drug shop Sheep Marketplace poofs with $40 million” (Computer World, 02 December 2013) <http://www.computerworld.com/article/2475637/cybercrime-hacking/huge-bitcoin-heist--black-market-drug-shop-sheep-marketplace-poofs-with--40-milli.html> accessed 04 September 2014

Strauss K, “How can we effectively combat the use of the internet for money laundering?” <https://www.academia.edu/1369342/Cyber-laundering_-_How_can_we_combat_money_laundering_over_the_internet> accessed 03 September 2014

Templeton G, “The Silk Road 2.0 is now bigger and better than ever before: What’s the FBI to do?” (Extremetech, 08 May 2014) <http://www.extremetech.com/extreme/182083-the-silk-road-2-0-is-now-bigger-and-better-than-ever-before-whats-the-fbi-to-do > accessed 04 September 2014. Also see <http://verdict.justia.com/2014/02/25/bitcoin-cant-ban-regulate> accessed 09 September 2014

Vahlis Y, “Bitcoin, Identity, and Decentralized Auctions” Huffington Post (US, 28 May 2014) <http://www.huffingtonpost.com/yevgeniy-vahlis/bitcoin-identity-and-dece_b_5398577.html> accessed 05 September 2014

Volastro A, “CNBC Explains: How to mine bitcoins on your own” CNBC (US, 23 January 2014) <http://www.cnbc.com/id/101332124#> accessed 02 August 2014

Zetter K, “FBI Fears Bitcoin’s Popularity with Criminals” Wired (05 September 2012, California) <http://www.wired.com/2012/05/fbi-fears-bitcoin/ > accessed 30 July 2014