doi: 10.5102/rdi.v12i2.3557

International criminals and their virtual currencies: the need for an international effort in regulating virtual currencies and combating cyber crime*

Criminosos internacionais e as suas moedas virtuais: a necessidade de um esforço internacional para regular as moedas virtuais e para combater a cibercriminalidade

oy Marie Virga**

Abstract

Technology is constantly evolving and making our lives easier. Since the advent of the Internet, new technologies have developed that make the world smaller and bring people across the continents closer together. However, these new technologies also create a new medium for criminal activity. One example of these new technologies is virtual currencies. While virtual currencies have many benefits, they also create many opportunities for crimes such as money laundering. Virtual currencies are not controlled by any state entity, they allow users to transfer goods anonymously, and they cross borders effortlessly via the Internet. All these characteristics make it difficult for individual states to regulate virtual currencies in isolation. This article will discuss these issues and how international cooperation is necessary in order to effectively counteract cybercriminals who utilize virtual currencies to evade national law enforcement. First, this article will discuss what virtual currencies are and how they work. Next, the article will discuss recent law enforcement actions of various nations to shutdown operations that use virtual currencies to finance criminal activity. This article will then discuss how virtual currencies are moved through various institutions and used to assist criminals in carrying out illicit activity. It will look at how these institutions were taken down through concerted international efforts. Third, I will briefly discuss how various nations regulate virtual currencies domestically. This article will then analyze the need for international regulation of virtual currencies and discuss possible avenues for regulating virtual currencies internationally. The article will discuss how traditional international financial standards and an existing cybercrime treaty may apply to virtual currencies in their present forms. Finally, this article will recommend a method for international cooperation in regulating virtual currencies to reduce the amount of cybercrime.

Keywords: International. International law. International crime. Cybercrime. Virtual currencies. Bitcoin. Silk road. Money laundering. Technology. Crime. Virtual money.

* Recebido em 01/09/2015
Aprovado em 06/10/2015

** J.D. Candidate 2016, American University Washington College of Law; M.B.A. 2013 Stony Brook University. The author thanks Professor Srilal Perera for providing guidance and support throughout the writing process for this article. E-mail: joymarie.virga@gmail.com.

1. Introduction

Virtual currencies have been around since at least 2008, but a federal court only just held that the Securities and Exchange Commission has jurisdiction over virtual currencies on September 18, 2014.[1] In SEC v. Shavers the court held a Texas man liable for the loss he caused investors through a Bitcoin Ponzi scheme.[2] This decision provides protection for investors of virtual currencies within the borders of the United States, but does nothing to protect investors from schemes that originate abroad.[3] This lack of international regulation of virtual currencies opens up investors to fraudulent activities while creating a safe space to finance criminal activities.[4]

International bodies have come out in favor of international regulation of virtual currencies.[5] The Japanese Finance Minister stated that regulation of crypto currencies should involve international cooperation in order to avoid potential loopholes.[6] Additionally, a recent paper by the Organisation for Economic Co-operation and Development cited a need for some form of best practice agreement to provide consumer protection of crypto currencies and prevent money laundering.[7]

This article will argue that there is a strong need for international regulations of virtual currencies in order to deter crime and fraud. It will give background information on why regulation of virtual currencies, specifically international regulation, is important. First, I will briefly describe how virtual currencies work and discuss the types of virtual currencies. Second, I will discuss recent law enforcement actions led by various nations to shutdown operations using virtual currencies to fund criminal activity. This article will discuss how virtual currencies were moved through various institutions and used to assist criminals in carrying out illicit activity. This article will then discuss how these institutions were taking down. Third, I will briefly discuss how various nations regulate virtual currencies within their borders.

This article will then explore and analyze the importance of international regulation of virtual currencies and possible methods for regulating these currencies internationally. I will discuss how traditional international financial standards and an existing cybercrime treaty may apply to virtual currencies in their present forms. Finally, this article will recommend a method for international cooperation in regulating virtual currencies to reduce the instances of cybercrime.

2. The Current status of virtual currencies and legal actions involving virtual currencies

While all virtual currencies are digital currencies, not all digital currencies are virtual currencies.[8] Virtual currencies are a digital representation of value that can be exchanged through the Internet for goods and services.[9] However, virtual currencies have no physical coun-

1 SEC v. Shavers, 13-cv-00416, 2014 US Dist LEXIS 130781 *22 (E.D. Tex. Sept. 18, 2014) (deciding that virtual currencies fall within the definition of a security under the Securities and Exchange Act); see Peter M.J. Gross, A History of Virtual Currencies: Why Bitcoins Shouldn't Surprise You, **CFA Institute**, Jan. 10, 2014, http://annual.cfainstitute.org/2014/01/10/a-history-of-virtual-currency-why-bitcoins-shouldnt-surprise-you/ (outlining the history of virtual currencies).

2 Shavers, 2014 US Dist. LEXIS 130781 at * 20, 22 (finding that virtual currencies fall under the definition of an investment contract of the Securities and Exchange Act).

3 See SEC v. Shavers, at *22, 28-29 (finding reasonable grounds to issue an injunctions because of the likelihood of defendant repeating offensive behavior).

4 See generally Virtual Currencies: Key Definitions and Potential AML/CFT Risks 9 (June 2014) http://www.fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (stating that virtual currencies are particularly vulnerable to money laundering and terrorist financing abuse because they are traded anonymously and on the internet).

5 Eric Naing, International bodies see need for virtual currency regulation, **CG Roll Call Washington Bank Briefing**, (July 22, 2014) (stating that the Organisation for Economic Cooperation and Development, the Financial Action Task Force, and the European Banking Authority have all stated a need for regulation of virtual currencies).

6 Sophie Knight, Japan says any Bitcoin regulation should be international, **Reuters** (Feb. 27, 2014), http://www.reuters.com/article/2014/02/27/us-bitcoin-mtgox-japan-idUSBREA1Q0I520140227 (discussing Japan's reaction to the closing of Mt. Gox, formerly the world's largest Bitcoin exchange).

7 Adrian Blundell-Wignall, The Bitcoin Question: Currenc; versus Trust-less Transfer Technology: OECD Working; Papers on Finance, Insurance and Private Pensions, 17; **OECD Publishing**, http://www.oecd.org/daf/fin/financial-markets/The-Bitcoin-Question-2014.pdf (exploring policy issues related to crypto-currencies).

8 Andrew Wagner, Digital v. Virtual Currencies, **Bitcoin Magazine** Aug. 22, 2014, available at https://bitcoinmagazine.com/15862/digital-vs-virtual-currencies/ (explaining the difference between digital and virtual currencies).

9 Vitual Currencies, supra note 4, at 4 (defining virtual currencies and explaining the difference between virtual currencies and other currencies).

ter part with legal status and are largely unregulated.[10] Fiat currencies, also known as "real money" or "national currencies," are the coin and paper money that a nation assigns as its legal tender.[11] E-money is a digital representation of fiat money used to electronically transfer money that has a legal tender status.[12] Digital money refers to both e-money and virtual money.[13] Since, e-money has a legal standard and is thus already regulated by nations, the focus of this article will be on virtual currencies.[14] In order to understand this issue, it is important to understand the types of virtual currencies and how they function.

2.1. The types of virtual currencies

Virtual currencies can be open or closed and centralized or decentralized.[15] Open virtual currencies have an equivalent value with fiat money and can be exchanged back and forth.[16] Closed virtual currencies are intended for a particular on-line domain and will not be discussed in this article.[17] Centralized virtual currencies have a singular administrative authority that issues the currency, establishes rules, and generally controls the system.[18] The exchange rate for centralized virtual currencies can be floating—determined by supply and demand—or pegged—fixed by the central authority.[19] Decentralized virtual currencies, more commonly known as cryptocurrencies, have no central administrative authority and therefore no oversight.[20] These currencies are math-based, meaning they are distributed among a network of individuals who validate the transaction by running an algorithm.[21] Altcoin refers to all virtual currencies that are both open and convertible, the most popular of which is Bitcoin.[22] These virtual currencies can be swapped for other virtual or fiat currencies through an exchanger.[23] An exchanger is a person or entity that is in the business of exchanging virtual and fiat currencies for a fee and accepts a wide range of payments, including cash, credit cards and wire transfers.[24]

Altcoins are created through a process called mining.[25] Mining requires many computers on a peer-to-peer network working together to solve an algorithm.[26] The purpose of the algorithm is to maintain transparency in the public ledger, which tracks how many altcoins each user owns.[27] In order to encourage users to

10 European Central Bank (ECB), Virtual Currency Schemes,5 (Oct 2012), available at http://www.ecb.int/pub/pdf/other/virtualcurrencyschemes201210en.pdf (visited Apr 10, 2013)(discussing the difference between virtual currencies and electronic money is the lack of a legal status and physical counterpart).

11 Virtual Currencies, supra note 4, at 4 (stating that fiat is customarily used and accepted as a medium of exchange in the issuing country and is also referred to as real currency, real money or national currency).

12 Id.; European Commission, E-money, **Banking and Finance**, http://ec.europa.eu/finance/payments/emoney/index_en.htm (Jan. 21, 2015 10:05PM) (explaining that e-money is the digital equivalent of cash and can be stored electronically on an electric device or a server).

13 Virtual Currencies, supra note 4, at 4; see also Sandeep Dave, et al., Symposium, Getting Ready for Digital Money: A Roadmap, **Imperial College London**, 6 (2014) available at http://icg.citi.com/icg/sa/digital_symposium/docs/DigitalMoneyIndex30012014.pdf (providing examples of digital currencies like the M-Pesa in Kenya, and Paypal).

14 See Virtual Currencies, supra note 4, at 4 (stating that e-money is the digital representation of fiat money).

15 Id. at 4-5 (discussing in depth the differences between the types of virtual currencies).

16 Id. at 4 (providing examples of open currencies such as Bitcoin and WebMoney).

17 Id. at 4-5 (stating that closed virtual currencies are popular on sites like Amazon.com or Massively Multiplayer Online Role-Playing Games and include World of Warcraft Gold. All closed virtual currencies are also centralized); Virtual Currency Schemes, supra note 10, at 13 (explaining that closed virtual currencies have "almost no link to the real economy).

18 Virtual Currencies, supra note 4, at 5 (stating that centralized virtual currencies have a central administrator).

19 Id. (explaining that the exchange rate maybe either pegged or floating).

20 Id.; Virtual Currency Schemes, supra note 10, at 27 (asserting that decentralized virtual currencies exist where there is no central organizer).

21 Virtual Currencies, supra note 4, at 5, 14 (stating that decentralized virtual currencies are also called cryptocurrencies because they use cryptography).

22 Id. at 6; see also Kerry Lynn Macintosh, How to Encourage Global Electronic Commerce: The Case for Private Currencies on the Internet, 11 **Harv. J. L. & Tech.** 733, 750 (1998)(detailing how a private market place of currencies would lead to an optimal number of currencies operating within a global electronic marketplace among niche currencies within their own submarket).

23 Virtual Currencies, supra note 4, at 7 (explaining that individuals usually use exchangers to deposit or withdraw money from virtual currency accounts).

24 Id.(describing an exchanger as "a person or entity engaged as a business in the exchange of virtual currency for real currency, funds, or other forms of virtual currency for a fee.").

25 Castle, Beginner's Guide to Mining Litecoin, Dogecoin, and other Bitcoin Variants, **PC World** May 6, 2014, http://www.pcworld.com/article/2151261/beginners-guide-to-mining-litecoin-dogecoin-and-other-bitcoin-variants.html (asserting that all Altcoins, like Bitcoin, are created through process called mining).

26 Id. (explaining that this process is called cryptography).

27 Id.; Virtual Currency Schemes, supra note 10, at 24 (asserting that the mining process validates transactions by using computer power to find valid solutions to complex math problems and is the

run these algorithms, users are rewarded with altcoins for doing so.[28] Mining of Bitcoins has become so lucrative in recent years that companies have designed chips solely for this purpose.[29] As a result, a normal desktop computer will not be able to compete.[30] However, other altcoins are much less popular and more accessible to the average user.[31]

The benefits of virtual currencies are many.[32] Virtual currencies could create a common medium of exchange, which would simplify international negotiations.[33] A common medium of exchange would reduce or eliminate currency exchange fees, which are present in exchanges of fiat money.[34] Additionally, exchanges of virtual currencies do not incur the same transaction costs that traditional debit and credit card purchases do, which could lead to lower costs for micro transactions like one time music downloads.[35] Furthermore, virtual currencies could facilitate financial inclusion of the un- and under-banked.[36]

Because open currencies, like Bitcoin or Altcoin, can be exchanged for real currencies, they are vulnerable to fraud.[37] Tools called anonymisers are used to further increase anonymity by obscuring the source of an altcoin transaction.[38] For example, Dark Wallet is a web browser extension, currently available on Google Chrome, which enables users to remain anonymous in Bitcoin transactions.[39] This increase in anonymity coupled with the absence of a central oversight body and the global reach of virtual currencies makes them an attractive resource for criminals to reach beyond national borders and escape regulation.[40] Various national governments have already engaged in national and international efforts to identify and shutdown various criminal organizations that utilized virtual currencies to fund their operations.[41] These concerted efforts will be discussed in the following section.

2.2. Legal action taken against organizations that used virtual currencies in national and international criminal activity

To date, there have been a few instances of nations, working alone or in concert, successfully bringing actions against criminals who use virtual currencies to facilitate crime. In this section I will discuss these cases to provide information on how criminals utilize virtual currencies and to demonstrate the international nature of these schemes.

2.2.1. Liberty Reserve

The case of Liberty Reserve is the biggest on-line money laundering case thus far.[42] Liberty Reserve was designed to avoid regulatory scrutiny and assist criminals in distributing, storing and laundering proceeds collected from fraud,

only way to create new coins).

28 Castle, supra note 25; Virtual Currency Schemes, supra note 10, at 24 (discussing how, in the Bitcoin scheme, people who volunteer to partake in this activity are rewarded with 50 newly created Bitcoins each time their computer solves an equation).

29 Castle, supra note 25. See also Virtual Currency Schemes, supra note 10, at 21 (stating that the money supply is determined by a type of mining that depends on the resources, electricity and CPU time, the miner devotes to solve the mathematical problems).

30 "Even the burliest desktop PC with huge gaming GPUs won't be able to generate enough money mining bitcoin to cover the cost of the electricity used in the process." Id.

31 Id. (stating that many Altcoins use an algorithm called script, which can be solved on a personal computer to receive Altcoins. Altcoins can then be used to purchase Bitcoins).

32 See generally, Macintosh, supra note 22, at 756, 762, 783-84(describing how virtual currencies would greatly reduce or eliminate exchange fees, increase privacy and serve as more stable stores of value than national currencies).

33 Id. at 756 (explaining that a user pays a one time exchange fee for the virtual currency, they may buy products freely within the cyber market place without worrying about additional fees that traditional currencies would incur).

34 Id. (detailing the process in which international transactions increase expenses by incurring negotiation costs and bank fees).

35 Virtual Currencies, supra note 4, at 9 (explaining that traditional debit and credit card purchases are associated with higher transactions costs than virtual currency transactions).

36 Id. (stating that virtual currencies can facilitate financial inclusion as new virtual currency services are developed).

37 Id.; see also Adrian Blundell-Wignall, The Bitcoin Question, Currency Versus Trust-Less Transfer Technology, **Organisation for Economic Cooperation and Development**, 8 available at http://www.oecd.org/daf/fin/financial-markets/The-Bitcoin-Question-2014.pdf (stating that the authentication process of Bitcoin opens the way for fraud).

38 Virtual Currencies, supra note 4, at 6 (explaining that anonymisers are tools or services designed to obscure the source of a transaction); Federal Bureau of Intelligence, **Intelligence Assessment**, (U) Bitcoin Virtual Currency: Unique Feature Present Distinct Challenges for Deterring Illicit Activity, (Apr. 14, 2012), 5 (discussing the various ways Bitcoin user can increase anonymity, including the use of an anonmyzer).

39 Virtual Currencies, supra note 4, at 6 (providing examples of anonymisers such as Tor, Dark Wallet and Bitcoin Laundry).

40 Id. at 9-10. See also Blundell-Wignall, supra note 37, at 13 (asserting that a main purpose for Bitcoins is to carry out illicit activities due to the 'anonymity factor').

41 See generally, Virtual Currencies, supra note 4, at 10-12 (detailing the cases of Liberty Reserve, Western Express International, and the Silk Road).

42 Id. at 10 (explaining that Liberty Reserve was taken down by effectively cutting it out of the US Financial System).

identity theft, narcotics trafficking, child pornography and other crimes.[43] It laundered over 6 billion in US Dollars amongst more than a million users.[44]

Liberty Reserve was identified by the United States Department of Treasury as a financial institution primarily concerned with money laundering.[45] Liberty Reserve created virtual currencies called the "Liberty Reserve Dollar" or "Liberty Reserve Euro"[46] which users bought in exchange for national currencies.[47] Once a user had access to Liberty Reserve Funds, the funds can be transferred to any of the accounts within the system.[48] All transactions were anonymous and only the account number was visible, however, with an additional fee, even this could be redacted.[49] Users could then withdraw funds by sending their Liberty Reserve currency to an exchanger, which then sent a bank wire or other transfer method to the user's bank account.[50]

In 2004, Liberty Reserve was being run out of an apartment in Brooklyn, New York but in 2006 was re-registered in Costa Rica,[51] a country sometimes referred to as a money-laundering hub.[52] Costa Rica is often used by foreign institutions primarily to send funds to and from other sovereignties in "bulk cash shipments" or off shore companies.[53] Liberty Reserve's blog explained that the reason for the change in country registration was because Costa Rica does not have a mutual legal assistance treaty with the United States.[54] After Liberty Reserve learned that it was being investigated by United States law enforcement agencies, Liberty Reserve pretended to shut down in Costa Rica but continued to operate through various shell companies and moving millions of dollars through accounts in other countries such as Australia, China, Morocco, Cyprus, Spain among others.[55]

Liberty Reserve took no steps to verify the identities of their users who regularly used unquestionably false names, such as "Hacker Account," with undoubtedly false addresses, like "123 Fake Main Street."[56] Liberty Reserve's exchangers also had little to no verification or monitoring of clients.[57] Liberty Reserve recommended exchangers to its users that were generally unlicensed money transmitting businesses running out of countries with little governmental oversight or regulation of money laundering such as Russia, Malaysia, Vietnam and Nigeria.[58] The use of exchangers enabled Liberty Reserve to avoid collecting information on its users such as banking information, which would create a paper trail.[59]

43 Id. (stating that Liberty Reserve facilitates anonymous and untraceable transactions). See also, FBI, supra note 38, at 6 (referencing a cybercriminal who would only accept Bitcoin, WebMoney or Liberty Reserve as payment).

44 Virtual Currencies, supra note 4, at 10 (explaining that Liberty Reserve handled about 55 million illicit transactions).

45 Department of Treasury, Treasury Identitfies Virtual Currency Provider Libery Reserve as a Finanacial Institution of Primary Money Laundering Concern Under USA Patriot Act Section 331, May 28, 2013, available at http://www.treasury.gov/press-center/press-releases/Pages/jl1956.aspx (using § 311 of the USA Patriot Act to support this finding).

46 Department of Treasury, Notice of Finding that Liberty Reserve SA Is a Financial Institution of Primary Money Laundering Concern, available at http://www.fincen.gov/statutes_regs/files/311--LR-NoticeofFinding-Final.pdf, 3 [herein after, "DOT Notice of Finding"] (finding that Liberty reserve maintained a Dollar for Dollar and Euro for Euro exchange to back their virtual currencies). See also Macintosh, supra note 22, at 759 (suggesting that using a strong national currency to back the Liberty Reserve virtual currency establishes a level of legitimacy).

47 DOT Notice of Finding supra, note 46, at 3 (stating that an exchanger transfers the value to a national currency).

48 Id. See also, Treasury Identifies Virtual Currency, supra note 45 (finding that transfers can be made instantly and anonymously).

49 DOT Notice of Finding supra, note 46, at 3 (asserting that users can pay an addition fee for greater anonymity). See also, Treasury Identifies Virtual Currency, supra note 45 (stating that users can pay an additional "privacy fee").

50 DOT Notice of Finding supra, note 46, at 3 (explaining that exchangers exchange funds through a bank or non bank wire transfer and charge a commission).

51 Id. at 5 (citing registration information from the Liberty Reserve website).

52 See Maguerite Cawley, Authorities Investigate Costa Rica Money Laundering Linked to Venezuela Govt., In Sight Crime, June 28, 2013 http://www.insightcrime.org/news-briefs/authorities-investigate-costa-rica-venezuela-money-laundering-connections (asserting that Costa Rica is the top money laundering nation in Central America); See also Tom Hays, Feds: Costa Rica a hub for money laundering, Salon, May 29, 2013 http://www.salon.com/2013/05/29/feds_costa_rica_a_hub_for_money_laundering_ap/ (claiming that Liberty Reserve is just the latest to take advantage of Costa Rica's lax regulations).

53 DOT Notice of Finding supra, note 46, at 5 (stating that Money Laundering in Costa Rica occurs in formal and informal financial sectors).

54 Id. at 6 (citing the Liberty Reserve blog).

55 irtual Currencies, supra note 4, at 11 (listing the nations in which Liberty Reserve operated).

56 Id. at 10 (presenting the false names and addresses of Liberty Reserve users).

57 DOT Notice of Finding supra, note 46, at 9 (finding that although Liberty Reserve claimed to verify user identity, the only verification practiced was that of a working e-mail).

58 Virtual Currencies, supra note 4, at 10 (asserting that Liberty Reserve used exchangers to evade collecting user information).

59 Id. at 10 (claiming that Liberty Reserve's use of exchangers allowed it to evade collecting bank account information of users).

After a joint investigation by the United States and Costa Rica, the founder and owner of Liberty Reserve, Arthur Budovsky, was arrested in Spain and the site was shut down.[60]

2.2.2. Silk Road

Silk road was a hidden website designed off of the eBay model but functioned as a global black market where users could buy and sell illegal weapons, drugs, stolen identity information and other illicit goods.[61] Unlike Liberty Reserve, Silk Road did not create its own virtual currency but used the crypto currency Bitcoin as the only accepted currency.[62] Silk Road was launched in January 2011 and allegedly generated around 1.2 billion US Dollars in sales and commissioned around 80 million US Dollars through illegal transactions.[63]

By accepting only Bitcoin and operating on the Tor Network Silk Road was able to maintain anonymity.[64] The Tor Network is an underground network of computers on the Internet that obscures IP addresses by routing transactions through numerous computers and wrapping them in encryptions.[65] Users were also able to increase anonymity by using anonymisers, which were built into the Silk Road system and made it nearly impossible to link a user's payment with any Bitcoins leaving the site.[66]

The sites founder and operator, Ross William Ulbricht, was arrested in San Francisco in October 2013 and indicted in New York in February 2014.[67] He faces charges of narcotics trafficking, computer hacking, money laundering and conspiracy.[68] Although Ulbricht argues that the relevant money laundering statute is not broad enough to cover Bitcoin, the judge ruled that the statute did cover Bitcoin because they carry value.[69]

However, shortly after Ulbricht's arrest and the shutting down of Silk Road, Silk Road 2.0 popped up.[70] Fortunately, Silk Road 2.0 was also recently shut down after the November 14, 2014 arrest of Blake Benthall.[71] The government filed a complaint against Benthall, who took over after Ulbricht was arrested, seeking to indict him under the same charges as Ulbright.[72] Silk Road 2.0 had over 13,000 listings for controlled substances.[73] The take down of Silk Road 2.0 was part of a coordinated effort between the United States Justice Department's Criminal Division, the United State Attorney's Office for the Southern District of New York, and Europol's European Cybercrime Centre and Eurojust.[74] But like Ulbricht, Benthall was operating within the United States—San Francisco specifically.[75]

2.2.3. Western Express International

The take down of Western Express International involved an eight-year investigation conducted by the United States Secret Service and the Manhattan District Attorney's Office.[76] Western Express International was

60 Vitalik Buterin, Liberty Reserve Shutdown for Money Laundering, **Bitcoin Magazine**, May 25, 2013 https://bitcoinmagazine.com/4954/liberty-reserve-shut-down-for-money-laundering/ (stating Liberty Reserve has been shut down and its owner arrested in Spain.)

61 *United States v. Ulbricht*, 31 F. Supp. 3d 540, 546-48 (S.D.N.Y 1970) (discussing the facts of the case); Virtual Currencies, supra note 4, at 11 (explaining the facts of the case).

62 *Ulbricht*, 31 F. Supp. 3d 547 (finding that Silk Road was used to launder proceeds through Bitcoin).

63 Virtual Currencies, supra note 4, at 11 (asserting that hundreds of millions of dollars were laundered through these illicit activities).

64 Id. (explaining that this allowed users to maintain anonymity). See also, FBI supra note 38, at 6 (asserting that Silk Road also enabled its users to communicate anonymously).

65 Virtual Currencies, supra note 4, at 6 (discussing how the Tor Network is used to conceal IP addresses).

66 Id. at 11-12 (describing how a transaction went through a "complex, semi-random series of dummy transactions").

67 Id. at 11 (stating that the government seized the website and about 173,991 Bitcoins).

68 *United States v. Ulbricht*, 31 F. Supp. 3d 540, 546 (S.D.N.Y 1970) (citing the Grand Jury indictment).

69 *Id.* at 548 (finding that the purpose of Bitcoin is to carry value and act as a medium of exchange).

70 Dune Lawrence, Silk Road 2.0 Shut Down by FBI, Just Like Its Black Market Predecessor, **Bloomburg Business Week**, Nov. 6, 2014, http://www.businessweek.com/articles/2014-11-06/silk-road-2-dot-0-shut-down-by-fbi-just-like-its-black-market-predecessor (calling Silk Road 2.0 a copy cat of the Silk Road).

71 Julianne Pepitone, FBI Arrests Alleged 'Silk Road 2.0' Operator Blake Banthall, **NBC News**, Nov. 16, 2014, http://www.nbcnews.com/tech/security/fbi-arrests-alleged-silk-road-2-0-operator-blake-benthall-n242751 (asserting that Benthall was arrested for running a "Black Market Bazaar").

72 Lawrence, supra note 70(stating that Benthal will faces of narcotics trafficking; money laundering, and computer hacking).

73 Id. (asserting that the website had more than 13,000 listings for controlled substances).

74 FBI, More Than 400 .Onion Addresses, Including 'Dark Market' Sites, Targeted as Part of Global Enforcement Action on Tor Network, Nov. 7, 2014, available http://www.fbi.gov/news/pressrel/press-releases/more-than-400-.onion-addresses-including-dozens-of-dark-market-sites-targeted-as-part-of-global-enforcement-action-on-tor-network (listing the agencies involved in the takedown).

75 Lawrence, supra note 70 (stating that Benthal is from San Francisco).

76 Virtual Currencies, supra note 4, at 12 (recalling the facts of

a multinational, Internet based cyber crime group.[77] The hub of the operation was a New York corporation that operated as a "virtual currency exchanger and unregistered money transmitter to coordinate and facilitate the Internet payment methods used by the criminal enterprise, and to launder the group's proceeds."[78]

Western Express International was one of the largest currency exchangers in the United States and exchanged 15 million US Dollars and provided knowledge and support via its websites on strategies to move money anonymously and elude reporting requirements.[79] The group was composed of buyers, venders and cybercrime service providers located in a number of countries spanning from the United States to the Ukraine and Eastern Europe.[80] Western Express exchanged WebMoney and e-Gold—centralized open currencies[81]— for US Dollars and charged a commission for the transaction.[82] The buyers would steal identities to buy expensive goods, which they would then sell.[83] Buyers also committed crimes such as larceny and fraud and accumulated proceed from credit card fraud in the amount of about 5 million US Dollars.[84] The venders sold almost 100,000 stolen credit cards and other personal information via the Internet.[85] The international transactions of the buyers' and venders' illicit activities went largely un-scrutinized because e-Gold and WebMoney, as virtual currencies, are unregulated.[86] The cyber crime service providers assisted the buyers and sellers in their criminal activity by providing computer services.[87]

The owner and operator of Western Express International plead guilty to money laundering, fraud and conspiracy offenses in February 2013 in New York State.[88] Additionally, several other defendants plead guilty in 2009 and three others were convicted in June 2013.[89] In all, fifteen defendants were convicted for crimes committed under the auspices of Western Express International.[90] These defendants were a mix of United States and Foreign nationals, although most were operating within the United States.[91] One of them, Egor Shevelev, was one of the premier vendors and a Ukrainian national residing in the Ukraine.[92] Although the United States has no extradition treaty with the Ukraine, he was apprehended while on vacation in Greece.[93]

2.3. Regulations of virtual currencies within the United States and other nations

Although virtual currencies were the main element in all of the above mentioned cybercrime schemes, they remain largely unregulated within the borders of nation states. This part will look at how virtual currencies fit into the legal framework of the United States, the United Kingdom and Japan. The nations were chosen not just because of their role in the world's financial markets, but also because of their approach, or lack thereof, to regulating virtual currencies.

2.3.1. The United States

None of the laws of the United States explicitly outline how virtual currencies fit into United States regu-

the investigation).

77 Id. (calling Western Express a multinational, internet-based, cybercrime group); People v. W. Express Int'l Inc., 19 N.Y. 3d 652, 655 (N.Y. Ct. App. 2012)(reiterating the facts of the case).

78 Virtual Currencies, supra note 4, at 12 (stating the purpose of Western Express).

79 Id. (explaining that money was laundered through WebMoney and e-Gold).

80 Id. (describing the operations of Western Express International).

81 Id. at 4-5 (explaining that money was laundered through WebMoney and e-Gold).

82 People v. W. Express Int'l Inc., 19 N.Y. 3d 652, 655 (N.Y. Ct. App. 2012) (finding that Western Express international charged commission between two to five percent).

83 Virtual Currencies, supra note 4, at 12 (stating that buyers bought expensive goods, which they then fenced).

84 Id. (listing other crimes buyers committed).

85 Id. (describing the activities of vendors in the organization of Western Express).

86 People v. W. Express Int'l Inc., 19 N.Y. 3d 652, 655 (N.Y. 2012) (recalling the facts of the case).

87 Virtual Currencies, supra note 4, at 12 (discussing the role of service providers within Western Express International).

88 Id. (recalling facts of the case)

89 Id. (naming other defendants involved in the case).

90 Manhattan District Attorney, Western Express Cybercriminals Convicted at Trial Sentenced to Significant State Prison Time, Aug. 8, 2013, [herein after, "Manhattan DA, Western Express Cybercriminals Convicted"] available at http://manhattanda.org/press-release/western-express-cybercriminals-convicted-trial-sentenced-significant-state-prison-time (stating that 15 defendants were convicted).

91 See id. (providing the nationalities of the defendants and their locations of operation).

92 Id. (asserting Shevelev as a premier vender operating out of his home in the Ukraine).

93 Manhattan DA, Western Express Cybercriminals Convicted, supra note 90 (stating that Shevelev could not be arrested in the Ukraine but was arrested on vacation in Greece); Jeff Pohlman and Andrea Day, Busted! Inside one massive cybercrime ring, **CNBC** (Sept. 12, 2013, 2:06PM), http://www.cnbc.com/id/101029866 (discussing how Shevelev was outside the reach of United States authorities while inside of the Ukraine but was put on a watch list).

latory framework. However, judges have ruled in recent years that virtual currencies do qualify as money[94] for the purposes of money laundering and that virtual currencies meet the definition of an investment contract.[95] Under the Securities Act of 1934, an investment contract is a security and therefore, virtual currencies fall under the auspices of the Securities and Exchange Commission.[96]

2.3.2. Japan

The Minister of Japan recently stated that currency under Japan's jurisdiction refers to only coins or notes issued by the Bank of Japan and that virtual currencies do not qualify as a legitimate currency in Japan.[97] Officials from Japan's Financial Services Agency and Finance Ministry told reporters that virtual currencies do not fall within their purview and the Bank of Japan is only studying the virtual currency phenomenon.[98] Japan further stated that it does not plan on taking any steps towards regulating virtual currencies.[99] The Vice Finance Minister of Japan stated that any regulation of virtual currencies should "involve international cooperation to avoid loopholes."[100]

2.3.3. The United Kingdom

Currently, there are no regulations of virtual currencies in the United Kingdom.[101] However, in August 2014, the United Kingdom's Chancellor of the Exchequer stated that the United Kingdom will look into how virtual currencies could or should be regulated.[102] As of now, Bitcoins have been classified as a single purchase voucher and are subject to a ten to twenty percent value added tax.[103]

3. The Need for International Regulation of Virtual Currencies and How Regulation May Be Approached

The willingness of certain governments to organize concerted efforts to investigate and prosecute on-line financial institutions that utilize virtual currencies to operate their criminal activities is a great start. However, many risks are associated with virtual currencies. Although representatives of many governmental agencies in the United States and abroad believe that virtual currencies provide many benefits, many of these representatives are still warning banks and investors to stay away from virtual currencies until they can be better regulated.[104] Still, regulation of virtual currencies

94 United States v. Ulbricht, 31 F. Supp. 3d 540, 569 (S.D.N.Y 1970) (comparing Bitcoin to Euros and Dollars).

95 Memorandum Decision Regarding the Courts Subject Matter Jurisdiction at 3, SEC v. Shavers, 13-cv-00416, 2014 US Dist. LEXIS 130781 (E.D. Tex. Sept. 18, 2014) (finding that virtual currencies fall within the definition of a security under the Securities and Exchange Act).

96 15 U.S.C. § 77b; Memorandum Decision Regarding the Courts Subject Matter Jurisdiction at 3, SEC v. Shavers, 13-cv-00416, 2014 US Dist. LEXIS 130781 (E.D. Tex. Sept. 18, 2014) (holding that the Securities and Exchange Commission has jurisdiction over virtual currencies).

97 Knight, supra note 6 (quoting Japanese officials that do not consider Bitcoin to be a currency).

98 Id. (stating that Japanese officials are not taking any action after the fall of Mt. Gox).

99 Japan's ruling party won't regulate Bitcoin for now, **Reuters** (June 19, 2014), http://www.reuters.com/article/2014/06/19/japan-bitcoin-idUSL4N0P01LS20140619 (discussing that Japan has no intention to regulate virtual currencies).

100 Knight, supra note 6 (quoting the Vice Finance Minister of Japan).

101 Jane Wild, UK Taxman, police and spies look at Bitcoin threat, **Financial Times**, Mar. 13, 2013, http://www.ft.com/cms/s/2/42ca6762-bbfc-11e2-82df-00144feab7de.html#axzz2pdQoiDZO (explaining that Bitcoin is currently unregulated by any authority in the United Kingdom).

102 Anna Irrera, U.K. to Examine Virtual Currency Regulation, **Wall St. J.** Aug. 6, 2014, http://blogs.wsj.com/digits/2014/08/06/uk-to-examine-virtual-currency-regulation/ (recognizing the important of virtual currencies, the UK Chancellor of the Exchequer stated he will look into how virtual currencies could of should be regulated).

103 Chris Skinner, The challenge of being a Bitcoin trader, **Financial Services Blog**, Nov. 13, 2013, http://thefinanser.co.uk/fsclub/2013/11/the-challenge-of-being-a-bitcoin-trader.html (stating that if an investor wanted to sell Bitcoin for more than £77,000, the investor would need to register for a value added tax).

104 European Banking Authority, EBA warns consumers on virtual currencies, Dec. 12, 2013, available at https://www.eba.europa.eu/-/eba-warns-consumers-on-virtual-currencies (warning consumers that virtual currencies are not protected); Eric Naing, International bodies see need for virtual currency regulation, **CG Roll Call Washington Bank Briefing**, (July 22, 2014) (naming various international organizations that cite a need for international regulation of virtual currencies); SEC, Investor Alert: Ponzi Schemes Using Virtual Currencies, SEC Pub. No. 153 (7/13). http://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf (advising investors to look out for Ponzi Schemes involving virtual currencies); Government Accountability Office, Virtual Currencies: Emerging Regulatory Law, Law Enforcement and Consumer Protection Challenges, **Report to the Committee on Homeland Security and Government Affaits, U.S. Senate**, 1, 22 May 2014, available at http://www.gao.gov/assets/670/663678.pdf (explaining that virtual cur-

remains a difficult task because of the anonymity factor, which makes them so attractive to criminal elements in the first place.[105]

While authorities hope that the law enforcement actions mentioned above would deter cybercriminals who think they can escape prosecution because they are operating outside of United States' borders, there are nations where cybercriminals could evade prosecution from United States authorities.[106] Additionally, many cases where authorities were successful in prosecuting cybercriminals, a certain level of international cooperation was required.[107] Therefore, as the government of Japan has asserted, regulation of virtual currencies should involve international coordination to ensure that loopholes are minimized.[108] While it is tempting to concentrate on the most popular of the virtual currencies, Bitcoin, most criminal activity has been conducted through other types of virtual currencies.[109]

An additional difficulty is presented when balancing the need to protect users from fraud and to deter crime with the benefit of promoting an emerging technology.[110] This section will analyze possible strategies of regulating virtual currencies internationally in a manner that respects this balance.

3.1. Current methods of international regulation of traditional capital and how they may apply to virtual currencies

Since issues of money laundering and cybercrime have been around for about as long as the Internet, international methods to combat these crimes have emerged.[111] However, since virtual currencies are a relatively new phenomenon, international organizations have not yet incorporated them into any current legal frameworks. This section analyzes how virtual currencies fit into the current policies and provisions of the Financial Action Task Force, the World Bank, and the International Monetary Fund.[112]

3.1.1. The Financial Action Task Force

The need for international cooperation in regulating virtual currencies is not too dissimilar from the need to regulate traditional securities internationally.[113] Strong cooperation between regulators across borders is necessary for proper oversight of international entities and for effective prevention of international securities fraud.[114] This international cooperation in embodied by the Financial Action Task Force, an intergovernmental body formed in 1989 by the governments of its member jurisdictions.[115] It is a policy making body whose purpose is to set standards and promote effective implementation of regulatory measure to prevent terrorist financing and money laundering schemes.[116] Countries ranging from Afghanistan to the Russian Federation to Mexico to the United States are members of either the Financial Action Task Force or one of its regional bodies.[117]

rencies offer lower transaction costs and faster transfers but are also subject to volatile prices and attract illicit activity).

105 Blundell-Wignall, supra note 37, at 13 (stating "[…]a raison d'etre for Bitcoins is to carry out illegal activities due to the 'anonymity factor'").

106 See Manhattan DA, Western Express Cybercriminals Convicted, supra note 90 (quoting the New York District Attorney).

107 Vitalik Buterin, Liberty Reserve Shutdown for Money Laundering, **Bitcoin Magazine**, May 25, 2013 https://bitcoinmagazine.com/4954/liberty-reserve-shut-down-for-money-laundering/ (stating that the takedown of liberty reserve was the product of a join investigation.)

108 Knight supra note 6 (citing the Japanese Vice Finance Minister).

109 FBI, supra note 38, at 6 (indicating that the FBI is less concerned with Bitcoin than other types of virtual currencies). See also People v. W. Express Int'l Inc., 19 N.Y. 3d 652, 655 (N.Y. Ct. App. 2012) (discussing how Western Express utilized WebMoney and eGold as their virtual currency of choice); DOT Notice of Finding, supra note 46 (finding that Liberty reserve maintained a Dollar for Dollar and Euro for Euro exchange to back their virtual currencies)

110 Japan's ruling party won't regulate Bitcoin for now, supra note 99 (stating that Japan has no plans to regulate virtual currencies).

111 See generaly International Convention on Cyber Crime, Available at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm; (lacking any reference to virtual currencies); Financial Action Task Force, The FATF Recommendations infra note 128, at 116 (missing any reference to virtual currencies).

112 These Institutions are chosen as they are the principle international organizations tasked with monitoring money.

113 Ellise B. Walter, Speech by SEC Commissioner: Supervisory Cooperation: The Next Frontier for International Securities Regulation, **US Securities and Exchange Comission**, July 6, 2010 available at http://www.sec.gov/news/speech/2010/spch070610ebw.htm (explaining that national initiatives of financial markets domestically is important, but so are broader, international financial intiatives).

114 Id. (stating that "robust cooperation among regulators is vital to the effective oversight of cross-border entities and to the prevention of international securities fraud").

115 About Us, Financial Action Task Force (Jan. 24, 2015 3:24 PM), http://www.fatf-gafi.org/pages/aboutus/ (explaining the formation of the Financial Action task Force).

116 Id. (explaining the purpose of the Financial Action Task Force).

117 Countries List, Financial Action Task Force (Feb. 21, 2015

The Financial Action Task Force has developed recommendations that are recognized as international standards for combating terrorist financing and money laundering.[118] These recommendations are the product of an international effort to combat these threats within the global financial system.[119] The Financial Action Task Force monitors the progress of its members in implementing measures; reviews techniques of those who launder money or finance terrorism; promotes the implementation and adoption of measure globally; and works to identify national level vulnerabilities.[120] Since the founding of the Financial Action Task Force in 1989, its recommendations have been issued five times: in 1990, 1996, 2001, 2003, and most recently in 2012.[121] Recommendations are issued every few years to ensure that they are up to date and relevant since they are designed to have universal application.[122]

While the recommendations are useful in creating international standards and policies, the Financial Action Task Force has no enforcement mechanism to impose penalties on any non-complying nations.[123] The only tool that the Financial Action Task Force has to enforce its recommendations is to publish a list of high risk and non-cooperative jurisdictions.[124] Before countries are put on this list, they are notified and have the opportunity to respond to the findings.[125] They may meet with an expert from the Financial Action Task Force in order to address any deficiencies or unresolved questions.[126] But a country will only be taken off of the list if the Financial Action Task Force is convinced that the jurisdiction will address any shortfalls by enacting legislation and regulations.[127]

The 2012 recommendations do not address virtual currencies specifically.[128] However, it does include one paragraph on new technologies.[129] Specifically, the recommendations urge countries and financial institutions to actively identify money laundering or terrorist financing risks that may emerge out of new or developing technologies.[130] After identifying such risks, countries and financial institutions should take the appropriate measures to manage and mitigate such risks.[131]

Furthermore, virtual currencies may fit into the definitions the Financial Action Task Force provides for the terms "funds" and "funds or other assets." This is important because the recommendations require countries to ensure funds or other assets are not used in money laundering or terrorist financing schemes.[132] If a country finds that funds or other assets are being used in such schemes, the country must freeze said funds or other assets.[133] The recommendations define funds to include "assets of every kind… and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets" (emphasis added).[134] The recommendations also define "funds or other assets" as,

> any assets, including […] property of every kind, […] and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such funds or other assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends or other income on or value

4:05 PM), http://www.fatf-gafi.org/countries/ (listing member nations of the Financial Action Task Force).

118 About Us, Financial Action Task Force, infra note 111 (naming a few nations which are member of the Financial Action Task Force or one of its regional bodies).

119 Id. (explaining the purpose of the Financial Action Task Force recommendations).

120 Id. (stating the activities of the Financial Action Task Force).

121 Id. (listing the years that the Recommendations have been issued by the Financial Action Task Force).

122 Id. (explaining the purpose of the Financial Action Task Force recommendations).

123 Andrew Ayers, The Financial Action Task Force: The War on Terrorism Will Not Be Fought on the Battlefield, 18 **N.Y.L. Sch. J. Hum. Rts**. 449, 451 (2002) (describing the Financial Action Task Force as primarily a policy making body).

124 Id. at 452-53 (stating that the List of Non-Cooperative Jurisdictions is the only enforcement tool that the Financial Action Task Force holds).

125 Id. at 452-53 (explaining the development process of the List of Non-Cooperative Jurisdictions).

126 Id. at 452-53 (Describing how a nation may seek to remove itself from List of Non-Cooperative Jurisdictions).

127 See id.at 452-53 (explaining when the Financial Action Task Force may remove a nation from List of Non-Cooperative Jurisdictions).

128 See generally Financial Action Task Force, The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, Feb. 2012, available at http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf (missing any mention of virtual currencies).

129 Id. at 17 (addressing new technologies and terrorist financing and money laundering).

130 Id. (suggesting nations be proactive in identifying new technologies that may assist terrorist financing or money laundering).

131 Id. (recommending nations to enact appropriate measures to manage and mitigate risks new techonolgies pose in money laundering and terrorist financing).

132 Id.at 13 (stating that nations should freeze funds or other assets of specified persons).

133 Id. (asserting that nations should freeze funds or other assets of specified persons).

134 Id. at 118 (defining the term "funds or other assets").

> accruing from or generated by such funds or other assets. (emphasis added).[135]
>
> Whether these definitions include virtual currencies depends entirely on how each jurisdiction defines the terms within the definition. For example, in the Unites States, virtual currencies are treated as property for tax purposes.[136] United States courts have also held that virtual currencies are money and securities.[137] Thus, within the borders of the United States, virtual currencies would easily fall under either definition as a kind of property. In the United Kingdom, Bitcoin is a type single purchase voucher subject to a value added tax and therefore may fall under the definition of "funds or other assets" as a legal document or instrument in electronic or digital form.[138] However, virtual currencies other than Bitcoin likely do not fit into this definition since only Bitcoin have the status of single purchase voucher.[139] On the other hand, because Japan manifestly decided to exclude virtual currencies from any regulation, virtual currencies would not likely fall under either of these definitions.[140]

Additionally, many of the virtual currency exchangers, which often assist cybercriminals in maintaining anonymity, may fall under the definition of a "financial institution."[141] A "financial institution is defined as "any natural or legal person who conducts as a business one or more of the following activities or operations for or on behalf of a customer: […] Money or value transfer services".[142] While the legal status of institutions may differ in varying jurisdictions, each individual participating in currency exchanges is a natural person and thus is subject to the requirement that financial institutions participate in anti-money laundering activity.[143]

Despite the fact that the Financial Action Task Force was created with the intent of creating directives aimed at combating money laundering and terrorist financing activities, some of its member nations—including the United States and Canada—have been the least compliant with the recommendations.[144] However, after the attacks on September 11, 2001, many nations have increased their resolve in fighting money-laundering activities.[145]

3.1.2 The World Bank and the International Monetary Fund

The World Bank and International Monetary Fund might have a place for monitoring, regulating or utilizing virtual currencies. However, monitoring crimes facilitated by virtual currencies may be outside the scope of their functions. The World Bank was created for the purposed of financing development.[146] Its first role was to provide loans for reconstruction of Europe after World War II, but since turned its attention to the world's developing nations.[147] Its central purpose is to "promote economic and social progress in developing countries by helping to raise productivity so that their people may live a better and fuller life."[148] There is an argument to be made that The World Bank could utilize virtual currencies to aid its global development efforts,[149] but that argument is outside the scope of this article.

At the same time The World Bank was established, the International Monetary Fund was also developed to address with the financial problems left unresolved after the Great Depression.[150] The IMF's primary purpose is to monitor the international monetary system

135 Id. at 118 (defining "funds or other assets").

136 Internal Revenue Service, Notice 2014-21, available at http://www.irs.gov/pub/irs-drop/n-14-21.pdf (stating that for federal tax purposes, virtual currencies are treated as property).

137 Memorandum Decision Regarding the Courts Subject Matter Jurisdiction, *SEC v. Shavers,* 13-cv-00416, 2014 US Dist. LEXIS 130781 (E.D. Tex. Sept. 18, 2014) (finding that virtual currencies fall under the definition of an investment contract under the Securities and Exchange Act); *Ulbricht*, 31 F. Supp. 3d 548 (finding that the purpose of Bitcoin is to carry value and act as a medium of exchange).

138 Skinner supra note 103 (stating that if an investor wanted to sell Bitcoin for more than £77,000, the investor would need to register for a value added tax).

139 See id. (referencing only Bitcoin).

140 Japan's ruling party won't regulate Bitcoin for now, supra note 99 (citing Japanese officials stating that Japan does not intent to enact any regulations of virtual currencies).

141 Financial Action Task Force, The FATF Recommendations supra note 128, at 116 (defining a "financial institution").

142 Id.

143 See id. (defining financial institution as any natural or legal person who operate money or value transfer services).

144 Ayers, supra note 123, at 458 (explaining the challenged the Financial Action Task Force faces in completing its objectives).

145 Id. at 451 (stating that non-compliant nations saw the attacks on September 11, 2011 as a wake up call on the important of the Financial Action Task Force's work).

146 David Driscol, The IMF and the World Bank, How Do They Differ?, **The International Monetary Fund**, https://www.imf.org/external/pubs/ft/exrp/differ/differ.htm (explaining the differences between the World Bank and the IMF their formation).

147 Id. (explaining the evolution of the World Bank).

148 Id. (stating the purpose of the World Bank).

149 Virtual Currencies, supra note 4, at 9 (asserting that virtual currencies may be able to provide services to the un- and underbanked)

150 Driscol, supra note 146 (explaining the development of the IMF).

of exchanges and payments.[151] While the IMF has the power to; and may want to regulate virtual currencies, especially those like Bitcoin with a large market capitalization,[152] the criminal aspect of virtual currency use is outside the scope of its mandate.[153] The IMF has the power to gather information from member nations to discuss their monetary policy but those discussions focus on the economic, rather than the criminal aspects of money.[154]

3.2. Current methods of international regulation of cybercrime and how they may apply crime facilitated by virtual currencies

Cybercrime is unique compared to other crimes because it has the ability to transcend national borders.[155] The advent of the Internet made it difficult for sovereign states to regulate criminal behavior because it is difficult to impose punishment on criminals outside of a sovereign's jurisdiction.[156] This section explores how crimes facilitated by virtual currencies fit into current international efforts by nations to battle cybercrime.

3.2.1. The International Convention on Cybercrime

The Convention on Cybercrime is an international treaty created with the intent to harmonize the laws of nations on cyber crime and increase investigative cooperation and capabilities.[157] The Convention entered into effect in 2004 and therefore lacks any mention of virtual currencies, digital currencies or even e-currencies.[158] The coordinators of the Convention recognized that the international character of cybercrime conflicted with national sovereignty and that a binding international instrument was necessary to guarantee effectiveness in combating this relatively new type of crime.[159]

The Convention outlines a number of cybercrime offenses that parties are responsible for addressing through legislation or other necessary measures. These offenses include, among others, crimes such as altering computer data without right,[160] possession or distribution of child pornography,[161] and the infringement of copy rights.[162] Although there is no explicit mention of the crimes that are typically committed through the use of virtual currencies—money laundering, buying and selling of illegal goods, and fraud—it is possible, with a broad interpretation of the provisions, that some of these crimes will be covered by the language of the Convention.[163] For example, Article 8 of the Convention concerns computer related fraud. [164] Fraud may be subject to this provision as it is causing of a loss of property to another person through a dishonest intent of

151 International Monetary Fund, The IMF at a Glance (Aug 22, 2012), available at http://www.imf.org/external/np/exr/facts/glance.htm (visited January 24, 2015) (outlining the purpose of the IMF).

152 See Nicholas A. Plassaras, Comment, Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF, 14 **Chi. J. Int'l. L.** 377 (2013) for an argument that IMF needs to regulate the exchange rates of Bitcoin.

153 IMF Mandate, available at http://www.imf.org/external/np/exr/facts/imfwb.htm (explaining the purpose of the IMF).

154 IMF Surveillance, **International Monetary Fund** (Oct. 3, 2014), http://www.imf.org/external/np/exr/facts/surv.htm (clarifying that the IMF's surveillance and consulting activities focus on "exchange rate, monetary, fiscal, and financial policies, as well as macro-critical structural reforms").

155 Amalie M. Weber, The Council of Europe's Convention on Cybercrime, 18 **Berkeley Tech. L.J.** 425, 425 (2003) (explaining the characteristics of cybercrime).

156 Id. (describing the role the internet plays in cybercrime).

157 Id. (detailing the purpose of the Convention). See also Council of Europe, Convention on Cybercrime Signatories, available at, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG (listing signatories of the International Convention on Cyber Crime, including all of the European Union Member States but has also been ratified by Australia, the Dominican Republic, Japan, Mauritius, Panama, and the United States.); Michael A. Vatis, The Council of Europe Convention on Cybercrime 207, 207 available at http://cs.brown.edu/courses/csci1950-p/sources/lec16/Vatis.pdf (explaining that the Convention was drafted by the council of Europe but that other non-European nations participated in negotiations).

158 See Generally International Convention on Cyber Crime, Available at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm; (lacking any reference to virtual currencies).

159 Vatis, supra note 157, at 208 (describing the urgency in addressing the international nature of cybercrime).

160 See Convention on Cybercrime Art. 4 (referring to alteration or suppression of computer data without right).

161 Id. at Art. 9 (addressing offenses related to Child Pornography).

162 Id. at Art. 10 (referring offences related to infringements of copyright and related rights).

163 See Weber, supra note 149, at 435 (listing crimes that could be covered by the International Convention on Cybercrime. None of the crimes); but see generally SEC v. Shavers, 13-cv-00416, 2014 US Dist. LEXIS 130781 *22(E.D. Tex. Sept. 18, 2014) (finding a virtual currency Ponzi scheme as a type of securities fraud).

164 See Convention on Cybercrime, Art 8 (stating the means through which a crime covered by the article must be conducted, "by: a) any input, alteration, deletion or suppression of computer data, [or] b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit.")

procuring an economic benefit.[165] However, the provision narrows itself by providing a means through which the crime may occur. For example, it seems unlikely that the conduct of Shavers in SEC v. Shavers, where a Texas man lied to investors via Internet chat rooms in a Bitcoin Ponzi scheme, would constitute an "input, alteration, deletion or suppression of computer data" or "interference with the functioning of a computer system."[166]

However, a later provision may serve as a catchall for crimes not listed.[167] Therefore, even though crimes usually committed through the use of virtual currencies are not explicitly listed in the Convention, these crimes might fall under the parameters of "other criminal offense committed by means of a computer system" so long as they are recognized by the relevant jurisdiction as criminal. However, this may become problematic if the domestic laws do not consider the action as criminal. For example, if Shavers, operating from within the United States, ran his Bitcoin Ponzi scheme in Japan and took Bitcoins from Japanese investors, would he face punishment since Japan does not seem to recognize virtual currencies?[168] The answer is unclear and requires further analysis.

The Convention includes a provision that grants state's jurisdiction over crimes that occurred within its borders even if the perpetrator committed that offense within the borders of another sovereign.[169] It also requires a state to grant jurisdiction to another state for a crime committed within the first state's borders as long as the act is a criminal offense within that jurisdiction.[170] The Convention also includes mutual assistance provisions, which requires the parties to provide assistance to each other in investigations and proceedings in cases involving cyber crime.[171] Furthermore, the Convention rejects the requirement of dual criminality, which requires that the two nations involved must both outlaw the action in question in order to comply with a request for assistance.[172] Even though the dual criminality requirement has been praised as an innovation that eased the relatively complicated process of drafting extradition treaties,[173] the drafters of the Convention argue that such a requirement would be counter productive in the context of preserving computer data, which could be quickly deleted.[174]

The Mutual Assistance provision and rejection of the dual criminality requirement advance the efforts of individual nations in combating cybercrime.[175] For example, Western Express International member Egor Shevelev was safe in the Ukraine because there was no extradition or other agreement with the Ukraine that would have enabled the United States to assert jurisdiction over him.[176] It was not until he was vacationing in

165 Id. (asserting that "criminal offences […] committed intentionally and […] causing of a loss of property to another person by: a) any input, alteration, deletion or suppression of computer data, [or] b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit."); see also Weber, supra note 155, at 434 (listing fraud as on of the possible crimes covered by the Convention).

166 See generally, SEC v. Shavers, 13-cv-00416, 2014 US Dist. LEXIS 130781 *22(E.D. Tex. Sept. 18, 2014)(outlining the facts of the case. Note the lack of any mention of any manipulation of computer data).

167 See Convention on Cybercrime Art. 14 (outlining the scope of the procedural provisions by stating "Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings […] the criminal offences established in accordance with Articles 2 through 11 of this Convention […] [and] other criminal offences committed by means of a computer system" (emphasis added)).

168 See generally Knight, supra note 6, (stating that Japan will not take any action after more than 744,000 Bitcoins went missing from Mt. Gox, formerly the world's biggest Bitcoin exchange).

169 Explanatory Report to the Convention on Cybercrime, ¶ 233 (stating a "Party would assert territorial jurisdiction if both the person attacking a computer system and the victim system are located within its territory, and where the computer system attacked is within its territory, even if the attacker is not.").

170 Id. ¶ 236 (asserting that "if a national commits an offence abroad, the Party is obliged to have the ability to prosecute it if the conduct is also an offence under the law of the State in which it was committed or the conduct has taken place outside the territorial jurisdiction of any State").

171 Convention on Cyber Crime, Art. 25 (requiring parties to assist each other in "[…] investigations or proceedings concerning criminal offences related to computer systems and data […]").

172 Id. at Art. 29; Explanatory Report to the Convention on Cybercrime, ¶ 285 (arguing that the principle of dual criminality is counterproductive); Weber, supra 155, 434 (stating that the Convention rejects the requirement of dual criminality).

173 Weber, supra note 155, 434 (explaining that dual criminality has been widely lauded in the development of extradition treaties).

174 Explanatory Report to the Convention on Cybercrime, ¶ 285 (asserting that dual criminality is […] counterproductive in the context of preservation.").

175 See DOT Notice of Finding supra, note 46, at 6 (citing the Liberty Reserve blog which stated that the purpose of the change in registration to Costa Rica was because there is no extradition treaty between the United States and Costa Rica); Manhattan DA, Western Express Cybercriminals Convicted, supra note 90 (stating that Shevelev could not be arrested in the Ukraine because there is no extradition treaty between the United States and the Ukraine).

176 Manhattan DA, Western Express Cybercriminals Convicted, supra, note 90 (stating that Shevelv could not be arrested in the

Greece, with which the United States has an extradition agreement, that the United States was able to get Shevelev extradited.[177] Additionally, Liberty Reserve moved its operation from New York to Costa Rica because there was no mutual assistance from Costa Rica and the United States.[178] The inclusion of these two elements in the Convention is important but, unfortunately, the Convention is only signed by a relatively small number of nations.[179]

3.2.2. Other efforts

A common element in the cybercrime cases mentioned in section II of this article is the maintenance of anonymity and lack of oversight. By nature, virtual currencies, especially cryptocurrencies lack a central regulating authority or one that cares to validate identities of users.[180] This fact makes virtual currencies especially useful to criminals but not much can be done to change this characteristic of virtual currencies.[181] However, the regulation of exchangers, the people or institutions that exchange virtual currencies for fiat currencies, is a possibility.[182] New York, one of the most active jurisdictions in fighting cybercrime facilitated by virtual currencies, has proposed a set of regulations, which it hopes will suppress criminal activity without stifling innovation.[183] These regulations include a requirement to obtain a license to act as an exchanger or issue virtual currencies.[184] The rules also require that each licensee must maintain books and records, and comply with all anti- money laundering, anti-fraud and cyber security regulations.[185]

While these rules may not be able to stop every instance of crime facilitated by virtual currencies, they are a good first step because they decrease the level anonymity that virtual currencies offer.

4. Possible Channels for International Regulation of Virtual Currencies

As discussed above, the regulation of virtual currencies might be achieved through the Financial Action Task Force, the International Convention on Cybercrime, and national regulations like those proposed by New York. However, while these three instruments are a decent starting point, the seriousness of the crimes facilitated by virtual currencies warrants action that will act as a deterrent to such crimes, rather than "might" act as a deterrent. Fortunately, the tools for cracking down on cybercrime already exist in each of these institutions and they just need to be altered and updated to reflect how the lack in regulation of virtual currencies facilitate cybercrime.

The International Convention on Cybercrime should develop an addendum to the provisions, or additional provisions that specifically outline the types of crimes that have become problematic in recent years with the growth of virtual currencies and how virtual currencies are used to carry out these crimes. To reiterate, these crimes include, but are not limited to fraud; money laundering; the buying and selling of illegal goods such as drugs, weapons, and stolen credit cards and identifying information; and dissemination of child pornography. Furthermore, it is important that the Convention is signed by additional countries in order to extend its scope.

Ukraine due the lack of an extradition treaty between the United States and the Ukraine).

177 Manhattan DA, Western Express Cybercriminals Convicted, supra, note 90 (explaining that Shevelev was arrested while on vacation in Greece).

178 DOT Notice of Finding, supra note 46, at 6 (citing Liberty Reserve's reason for moving to Costa Rica).

179 See Council of Europe Convention on Cybercrime Signatories, supra note 157 (listing all nations that are signatories to the Convention).

180 People v. W. Express Int'l Inc., 19 N.Y. 3d 652, 655 (N.Y. Ct. App. 2012) (finding that Western Express International did little to verify the identities of its users).

181 W. Express Int'l Inc., 19 N.Y. 3d at 655 (asserting that the nature of virtual currencies "recommends itself for money laundering purposes").

182 See Jacob Davidson, New York Proposes Bitcoin Regulations, **Time Money**, July 18, 2014, http://time.com/money/3004751/new-york-bitcoin-regulations-benjamin-lawsky/ (explaining that the superintendent for New York's Department of Financial Services proposed new rules for regulating virtual currency businesses).

183 Id. (stating that New York proposed regulations of virtual currencies). See also People v. W. Express Int'l Inc., 19 N.Y. 3d 652, 655 (N.Y. Ct. App. 2012) (finding defendants guilty of crime facilitated through virtual currencies in New York Courts).

184 New York State Department of Financial Services, Proposed New York Codes, Rules and Regulations, §§ 200.2(n), 200.3, available at http://www.dfs.ny.gov/about/press2014/pr1407171-vc.pdf (requiring persons who exchange virtual currencies to obtain a license).

185 New York State Department of Financial Services, Proposed New York Codes, Rules and Regulations, §§ 200.7, 200.12 available at http://www.dfs.ny.gov/about/press2014/pr1407171-vc.pdf (explaining that each licensee must maintain their books for ten years and books must maintain information about the transaction and must provide all data to the New York Department of Finance upon request).

Since there are so many nations that are not signatories to this Convention, there are too many places for cybercriminals to hide.

The Financial Action Task Force must also play an active role in encouraging nations to be more active in cooperating with other nations to bring cybercriminals utilizing virtual currencies to justice. The Financial Action Task Force must update its recommendations in a way that recognizes the role that virtual currencies play in financing terrorism and money laundering and how nations can work together to counter cybercrime activity. The Financial Action Task Force should also encourage nations to adopt laws and regulations similar to those that the legislature in New York State seeks to enact into law. It should also expand the definition of "financial institution" to explicitly include exchangers and the definition of "funds" or "funds or other assets" to explicitly include virtual currencies.

Even though any nation would find great difficulty in trying to directly regulate virtual currencies, especially cryptocurrencies, it is much less difficult to try to regulate those that exchange virtual currencies for fiat money. Exchangers should be regulated in the same manner as any other financial institution a nation recognizes as a legal entity. By holding an exchanger responsible for verifying the activities of those they serve, verifying the identities of their customers, and keeping standard book keeping records, the likely hood that virtual currencies will be used for criminal activity decreases significantly. If an exchanger believes that they will be held accountable for not taking to steps necessary to follow the law, they are less like to aid in cybercrime, knowingly or unknowingly. However, it is important that these regulations are enacted along side an increase in application of the Convention on Cybercrime because if, for example, an exchanger is exchanging currencies for customers in the United States in a manner that violates United States law, but is operating in a country that is not a signatory to the Convention, the United States will not have any power to hold this hypothetical person accountable.

Any nation not willing to incorporate such laws or to cooperate in international efforts to investigate and prosecute those who use virtual currencies to commit crime should be listed as a non-complying nation by the Financial Action Task Force.

5. Final considerations

While a few nations have been working against cybercrime facilitated through the use of virtual currencies, other nations have done little if anything to regulate virtual currencies. If international efforts are not continued and strengthened, the appeal of virtual currencies for criminals will only increase, and they will find ways around what little regulation currently exists. While the institutions are currently in place to deal the old realities of money laundering, cybercrime and other related crimes, these institutions need to be updated to reflect a new reality.

Para publicar na Revista de Direito Internacional, acesse o endereço eletrônico www.rdi.uniceub.br ou www.brazilianjournal.org.
Observe as normas de publicação, para facilitar e agilizar o trabalho de edição.