

2013

Beyond the Silk Road: Unregulated Decentralized Virtual Currencies Continue to Endanger US National Security and Welfare

Jared A. Kleiman

American University Washington College of Law

Follow this and additional works at: <http://digitalcommons.wcl.american.edu/nslb>



Part of the [Law Commons](#)

Recommended Citation

Kleiman, Jared A. "Beyond the Silk Road: Unregulated Decentralized Virtual Currencies Continue to Endanger US National Security and Welfare." National Security Law Brief 4, no. 1 (2013): 59-78.

This Article is brought to you for free and open access by the Washington College of Law Journals & Law Reviews at Digital Commons @ American University Washington College of Law. It has been accepted for inclusion in American University National Security Law Brief by an authorized administrator of Digital Commons @ American University Washington College of Law. For more information, please contact fbrown@wcl.american.edu.

BEYOND THE SILK ROAD: UNREGULATED DECENTRALIZED VIRTUAL CURRENCIES CONTINUE TO ENDANGER U.S. NATIONAL SECURITY AND WELFARE

JARED A. KLEIMAN¹

“This isn’t something that’s a flash in the pan. It’s something that’s going to be with us.”
-Senate Homeland Security and Governmental Affairs Committee (HSGAC) Aide²

INTRODUCTION

As pseudonymous Bitcoin³ programmer Satoshi Nakamoto prepares to celebrate his creation’s fifth-anniversary in 2014,⁴ U.S. regulators have made little progress toward developing a comprehensive regulatory framework for virtual currencies. Bitcoin, the first decentralized open-source

1 J.D./M.A. Candidate 2016, American University Washington College of Law/School of International Service; B.A. 2012, Boston University. Former intern, White House Domestic Policy Council; U.S. Department of Commerce, International Trade Administration; U.S. Department of State, U.S. Embassy London, Office of U.S. Ambassador Louis Susman; Office of U.S. Senator John Kerry; Massachusetts Executive Office of Labor and Workforce Development, Department of Labor Standards, Office of the General Counsel; U.K. Parliament, House of Commons, Office of Right Honorable Malcolm Wicks, MP; and Europe/Middle East/Africa debt capital markets public finance analyst at Barclays Investment Bank. Thanks are due to the NSLB Executive Board for helpful discussions during the drafting process, my family for their support throughout my education, and Malcolm Wicks (1947-2012) for welcoming me on my first step towards a public service career. The views expressed in this paper do not represent the views of these individuals or of any organizations with which they are associated.

2 See Zachary Warmbrodt, *Congress Starts Looking Into Bitcoin*, POLITICO (Aug. 13, 2013, 12:08 AM), <http://www.politico.com/story/2013/08/congress-starts-looking-into-bitcoin-95464.html>.

3 This paper uses “Bitcoin” to refer to the open-source cryptographic platform, and “Bitcoins” to describe the substitute for real currency. See *Some Bitcoin Words You Might Hear*, BITCOIN PROJECT 2009–2013, <http://bitcoin.org/en/vocabulary> (last visited Oct. 18, 2013).

4 See Maria Santos, *Sean’s Outpost Invited You to Celebrate Bitcoin’s Fifth Birthday*, BITCOIN EXAMINER (Oct. 12, 2013), <http://bitcoinexaminer.org/seans-outpost-invites-you-to-celebrate-bitcoins-fifth-birthday/>

peer-to-peer cryptocurrency,⁵ is a remittance tool⁶ with a market capitalization of over \$1.7 billion as of October 2013.⁷ Bitcoin represents an emerging platform with unprecedented benefits, from low-cost international transfers to completely private charitable donations and complex investment trusts.⁸ These same qualities allow criminal enterprises to potentially circumvent law enforcement agencies and regulators by using Bitcoins to traffic in illegal goods, launder money, finance terrorism, and evade taxes; establishing clear dangers to U.S. national security and welfare.

The infamous dark website, Silk Road,⁹ exemplifies the regulatory riddle unique to a decentralized virtual currency marketplace made up of administrators, sellers, and buyers contributing to an Amazon.com¹⁰ of illegal goods fuelled by Bitcoin transactions.¹¹ Launched in February 2011¹² and accessible only through the anonymizing internet browser, The Onion Router (Tor),¹³ Silk Road facilitated the trade of an estimated \$1.2 billion worth of illicit goods ranging from heroin and hand-

5 JERRY BRITO & ANDREA CASTILLO, BITCOIN: A PRIMER FOR POLICYMAKERS 1 (2013), available at http://mercatus.org/sites/default/files/Brito_BitcoinPrimer_embargoed.pdf (asserting that Bitcoin is the first decentralized digital currency); see also William J. Luther, *Cryptocurrencies, Network Effects, and Switching Costs* 3 (Mercatus Center at George Mason Univ., Working Paper No. 13-17, 2013), available at http://mercatus.org/sites/default/files/Luther_CryptocurrenciesNetworkEffects_v1.pdf (defining cryptocurrencies as digital alternatives to traditional government-issued paper monies).

6 *What is a Remittance Transfer*, CONSUMER FIN. PROT. BUREAU (Aug. 2, 2013), <http://www.consumerfinance.gov/askcfpb/1161/what-remittance-transfer.html> (explaining that Federal law defines remittance transfers as “certain electronic money transfers from consumers in the United States . . . to recipients abroad, including friends, family members, or businesses,” including “wire transfers” or “remittances”).

7 See Wanfeng Zhou & Nick Olivari, *Bitcoin Buzz Grows Among Venture Investors, Despite Risks*, REUTERS (Oct. 1, 2013, 7:47 PM), <http://www.reuters.com/article/2013/10/01/us-markets-forex-bitcoin-idUSBRE9901HA20131001>.

8 See Andrea Castillo, *Bitcoin: Understated benefits and overstated risks*, THE HILL'S CONGRESS BLOG (Aug. 21, 2013, 11:00 AM), <http://thehill.com/blogs/congress-blog/technology/317875-bitcoin-understated-benefits-and-overstated-risks> (explaining that Bitcoin has many benefits, such as lowering transaction costs); see also Svea Herbst-Bayliss, *Winklevoss Twins Say Bitcoin Could Become a Country's Currency*, REUTERS (Sept. 17, 2013, 1:59 PM), <http://www.reuters.com/article/2013/09/17/us-bitcoin-currency-idUSBRE98G0X320130917> (describing the Winklevoss' plans to launch the Winklevoss Bitcoin Trust, an exchange-traded fund holding Bitcoins as assets and tracking the Bitcoin economy that would allow investors to trade the digital currency like stocks).

9 See Kevin Dolak, *Silk Road Arrest Shines Light on “Dark Web”*, ABC NEWS (Oct. 3, 2013), <http://abcnews.go.com/Technology/silk-road-arrest-shines-light-dark-web/story?id=20460774>; see also Gerald Smith, *FBI Shuts Down the ‘Silk Road’ Black Market, Arrests Infamous Owner ‘Dread Pirate Roberts’*, THE HUFFINGTON POST, (Oct. 2, 2013, 3:54 PM), http://www.huffingtonpost.com/2013/10/02/silk-road-fbi_n_4030750.html (explaining that a dark website is inaccessible through conventional internet browsing methods).

10 *Id.*

11 See Matteo Congregalli, *The Dread Pirate Sailing the Dark New: Silk Road's Shipwreck Explained*, URBANTIMES (Oct. 5, 2013), <http://urbantimes.co/magazine/2013/10/the-dread-pirate-sailing-the-dark-net-silk-roads-shipwreck-explained/> (describing how Silk Road's hidden presence in the “deep web” caused difficulties for the FBI in tracing its operations)..

12 See Amrutha Gayathri, *From Marijuana to LSD, Now Illegal Drugs Delivered on your Doorstep*, INT'L BUS. TIMES (Jun. 11, 2011, 3:31 AM), <http://www.ibtimes.com/marijuana-lsd-now-illegal-drugs-delivered-your-doorstep-290021> (describing the effect that Silk Road has on black market trade).

13 See Ryan Broderick, *Traveling Down the Silk Road to Buy Drugs with Bitcoins*, MOTHERBOARD BETA, <http://motherboard.vice.com/blog/traveling-down-the-silkroad-to-buy-drugs-with-bitcoins> (last visited Oct. 18, 2013) (explaining that Tor masks a user's IP address by routing their query through a different IP address and allowing a user to access .onion sites that make up the “Deep Web”).

guns to hacking tools.¹⁴ The website's assets and alleged owner clandestinely operated for over two years before a multi-agency task force seized both in October 2013.¹⁵

Following months of hearings with regulators, academics, and finance and technology representatives, however, Congress has neither held further hearings, nor has it proposed legislation to mitigate the risks of decentralized digital currencies.¹⁶ In the absence of a distinct legislative path forward, executive and state agencies, as well as the judiciary, have led the charge on explaining virtual currencies to the government and to the public.¹⁷ Agencies have strained to fit Bitcoin and similar platforms into existing legal buckets that are decades old.¹⁸ Congress is in the process of acknowledging a new world where decentralized virtual currency has become increasingly popular, and is exploring how virtual currency can be properly exchanged while mitigating its attractiveness for criminals.¹⁹

At the same time, regulators face vocal proponents of systems like Bitcoin who argue their valid use for political, philosophical, and financial reasons.²⁰ Advocacy groups, led by the Bitcoin Foundation,²¹ have welcomed the opportunity to explain decentralized virtual currency's promise to representatives from the Department of the Treasury (Treasury) and Department of Homeland Security (DHS),²² but have expressed fears of excessive regulatory measures in the United States

14 See Adrien Chen, *Now You Can Buy Guns on the Online Underground Marketplace*, GAWKER (Jan. 27, 2012, 1:45 PM), <http://gawker.com/5879924/now-you-can-buy-guns-on-the-online-underground-marketplace>; see also Michael Mimoso, *FBI Takes Down Billion-Dollar Silk Road Online Drug and Hacking Marketplace*, THREAT POST (Oct. 2, 2013, 1:55PM), <http://threatpost.com/fbi-takes-down-billion-dollar-silk-road-online-drug-and-hacking-marketplace>.

15 See Complaint ¶ 1, *United States v. Ulbricht*, No. 13 MAG 02328, 2013 WL 5460023 (S.D.N.Y. Sept. 27, 2013) (charging Silk Road's alleged owner, Ross William Ulbricht, with conspiracy to commit narcotics trafficking, computer hacking, and money laundering in violation of 21 U.S.C. § 846, 18 U.S.C. §§ 1030, 1956); see also Sealed Verified Complaint ¶ 1, *United States v. Ulbricht*, No. 13 CIV 6919, 2013 WL 5467929 (S.D.N.Y. Sept. 30, 2013) (stating that Ross William Ulbricht must forfeit his assets pursuant to his criminal case).

16 See Warmbrodt, *supra* note 2 (arguing that regulators need to act soon to control risks imposed by these markets, including the risk of later overregulating).

17 See Elizabeth Ploshay, *Bitcoin Shakes Up Congress*, BITCOIN MAGAZINE (Aug. 13, 2013), <http://bitcoinmagazine.com/6354/bitcoin-shakes-up-congress/> ("The U.S. Senate is now looking to rein in regulators to ensure that Congress has a full understanding of Bitcoin and additional digital cryptocurrencies prior to any further regulation.").

18 See *All Things Considered: Lawmakers, Banking Regulators Take on Bitcoin*, NPR (Aug. 13, 2013, 4:32PM), <http://www.npr.org/2013/08/13/211735430/lawmakers-banking-regulators-take-on-bitcoin> ("Whenever there's a new disruptive technology, like Bitcoin, regulators look at it and they try to fit it into one of their preexisting buckets. And Bitcoin really doesn't fit neatly into any of these buckets, as you say.").

19 See Warmbrodt, *supra* note 2.

20 See Fergal Reid & Martin Harrigan, *An Analysis of Anonymity in the Bitcoin System*, in 2 2011 IEEE INT'L CONF. ON PRIVACY, SECURITY, RISK, & TRUST, & IEEE INT'L CONF. ON SOC. COMPUTING 1318, 1318 (2011), available at <http://users.encs.concordia.ca/~clark/biblio/bitcoin/Reid%202011.pdf> (asserting that people have switched to Bitcoin for pragmatic, philosophical, and political reasons).

21 See Michael del Castillo, *Bitcoin Foundation Meets with the Federal Reserve, FBI, Secret Service*, UPSTART BUS. J. (Aug. 26, 2013, 4:22PM), <http://upstart.bizjournals.com/money/loot/2013/08/26/bitcoin-foundation-meets-federal-reserve.html?page=all> ("Today, one of the most influential Bitcoin organizations met with leaders in Washington D.C."); see also Patrick Murck, *Today, We Are All Money Transmitters . . . (No, Really!)*, THE BITCOIN FOUND. BLOG (Mar. 19, 2013), <https://bitcoinfoundation.org/blog/?p=152> ("The BSA was never intended to apply this broadly and reach this far into people's everyday lives. Perhaps a little more guidance is needed").

22 See Robert McMillan, *Sure, You Can Steal Bitcoins. But Good Luck Laundering Them*, WIRED (Aug. 27, 2013, 6:30AM),

and abroad stifling the currency's growth.²³ Proponents of virtual currency claim it represents an "essential privacy-preserving technology."²⁴ This conflict is reflected by a release from the New York Department of Financial Services (DFS) that proclaimed the state's long history of promoting technological innovation while simultaneously noting that society and the virtual currency industry should share a common need to "[take] steps to root out illegal activity . . . [as] a legal and business imperative."²⁵

Part I of this article provides an overview of the federal government's definitions of virtual currency and a background on the Bitcoin platform in particular. Part II considers recent developments regarding the Silk Road as it relates to governmental treatment of virtual currencies. Part III discusses the implications of virtual decentralized currencies on the national security community and the authorities currently drawn upon by law enforcement. Part IV analyzes how legislators are rethinking unique financial technologies that affect national security and welfare as they become entrenched in the U.S. market. This Part also examines whether Bitcoin and other tools can be adequately retrofitted under current law or if tailored legislation is necessary to mitigate their risks. The Article concludes by finding that federal law enforcement and regulators, led by the Treasury and Department of Justice (DOJ), should continue setting precedent through the application of the USA PATRIOT Act and Bank Secrecy Act (BSA) and their specialized knowledge of financial crime to prevent the future use of virtual currency in facilitating online crime.

I: VIRTUAL CURRENCY IN CURRENT GOVERNMENT TERMS

Bitcoin is "the world's first completely decentralized digital currency."²⁶ Without a central monetary authority controlling exchanges on and uses of the platform, it fails to fit easily into the current BSA framework developed by the Treasury Financial Crimes Enforcement Network (FinCEN), according to industry and academic sources.²⁷

FinCEN was founded in 1990 to support all levels of government by monitoring financial trails

http://www.wired.com/wiredenterprise/2013/08/bitocoin_anonymity/ ("The Foundation — the group that oversees development of the core Bitcoin software — wants to see if it can come to an understanding with government authorities.").

23 See, e.g., Charles Arthur, *Bitcoin Dealers Seek Official Regulation for Digital Tokens*, THE GUARDIAN (Sept. 5, 2013, 1:20PM), <http://www.theguardian.com/technology/2013/sep/05/bitcoin-dealers-regulation-downing-street> ("Bitcoin companies told officials that big banks are blocking the creation of business accounts for money remittance because of fears over financial crime.").

24 Parker Higgins, *Why You Can't Blame Bitcoin for Silk Road Shadiness*, GIZMODO (Oct. 5, 2013, 5:00PM), <http://gizmodo.com/why-you-cant-blame-bitcoin-for-silk-road-shadiness-1441572365>.

25 See Notice of Inquiry on Virtual Currencies, Benjamin M. Lawsky, Superintendent of Fin. Servs., N.Y. State Dep't of Fin. Servs. (Aug. 12, 2013), available at <http://dfs.ny.gov/about/press2013/memo1308121.pdf>.

26 See BRITO & CASTILLO, *supra* note 5, at 1.

27 See Kavya Sukumar, *Government Eyes Regulation of 'Bitcoins'*, USA TODAY (Aug. 26, 2013, 5:18 PM), <http://www.usatoday.com/story/news/politics/2013/08/26/bitcoin-virtual-currency-regualtions/2702653/>.

left behind by criminals.²⁸ FinCEN is tasked with “analyzing and disseminating [financial transactions data] for law enforcement purposes”²⁹ while regulating the nation’s financial system under the Currency and Financial Reporting Act of 1970, as amended by Title III of the USA PATRIOT Act of 2001.³⁰ Together, these Acts constitute the current BSA of 1970, the “first and most-comprehensive” federal anti-money laundering and counterterrorism financing statute.³¹ Its findings on virtual currency provide a good starting point for understanding the basics of Bitcoin.

A. Virtual Currency

Real currency is “legal tender . . . that circulates and is customarily used and accepted as a medium of exchange.”³² Bitcoin has no managing authority and is not a legal tender in any nation.³³ As an initial step, FinCEN developed federal guidance in March 2013 differentiating virtual currency from real currency and explaining scenarios in which the BSA would regulate parties in a digital transaction.³⁴ Virtual currency is defined by FinCEN as “a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency. [It] does not have legal tender status in any jurisdiction.”³⁵ Decentralized virtual currencies including Bitcoin “[have] no central repository and no single administrator, and . . . may [be obtained] by [a person’s] own computing or manufacturing effort.”³⁶ Centralized virtual currencies, including the Royal Canadian MintChip and Amazon Coins, have a unified repository and administrator with whom users exchange real currency for a substitute.³⁷

To fall under FinCEN’s authority, a person must either create virtual currency for the purposes of selling it for real currency, or accept virtual currency from one source and transmit it to another

28 See *Overview*, U.S. DEP’T OF THE TREASURY, FIN. CRIMES ENFORCEMENT NETWORK, http://www.fincen.gov/law_enforcement/ (last visited Oct. 18, 2013).

29 See *What We Do*, U.S. DEP’T OF THE TREASURY, FIN. CRIMES ENFORCEMENT NETWORK, http://www.fincen.gov/about_fincen/wwd/ (last visited Oct. 18, 2013).

30 See *FinCEN’s Mandate from Congress*, U.S. DEP’T OF THE TREASURY, FIN. CRIMES ENFORCEMENT NETWORK, http://www.fincen.gov/statutes_regs/bsa/ (last visited Oct. 20, 2013).

31 See *What We Do*, *supra* note 29.

32 31 C.F.R. § 1010.100(m) (2011).

33 See Matt Clinch, *Bitcoin Recognized by Germany as ‘Private Money’*, CNBC (Aug. 19, 2013, 10:25AM), <http://www.cnbc.com/id/100971898>; see also FIN. CRIMES ENFORCEMENT NETWORK, APPLICATION OF FINCEN’S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES (2013), available at http://fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf (explaining that Bitcoin is a financial instrument, rather than e-money or a foreign currency).

34 See FIN. CRIMES ENFORCEMENT NETWORK, *supra* note 33.

35 *Id.*

36 *Id.*

37 See WILMERHALE, FINTECHWEBINAR SERIES: BITCOIN AND OTHER VIRTUAL CURRENCIES 7 (2013), available at http://www.wilmerhale.com/uploadedFiles/WilmerHale_Shared_Content/WilmerHale_Files/Events/WH-FinTech-webinar-bitcoin-26SEP13.PDF; see also *id.* at 20 (“The acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means.”).

source for currency, funds, or another substitute for currency.³⁸ By operating an unlicensed money transmission service, an exchanger or administrator is subject to fines and criminal prosecution under the racketeering statute 18 U.S.C. § 1960.³⁹ FinCEN distinguishes “users,” “exchangers,” and “administrators” of virtual currencies in the same guidance.⁴⁰ Users “obtain virtual currency to purchase goods or services.”⁴¹ Exchangers are “engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency,”⁴² and administrators are “engaged as a business in issuing virtual currency, and [have] the authority to redeem such virtual currency,”⁴³ thus providing money transmission services. Those providing money transmission services must maintain transaction records under the BSA.⁴⁴ The BSA also obligates exchangers and administrators to file suspicious activity reports for users who appear to be undermining money laundering and terrorist financing laws.⁴⁵

The courts have jurisdiction in the virtual currency realm as well. In *SEC v. Shavers*,⁴⁶ the District Court for the Eastern District of Texas held that it had subject matter jurisdiction to determine whether the Securities Act of 1933 applied to a Ponzi scheme case involving Bitcoins.⁴⁷ Because it found that the defendant’s investments constituted securities under 15 U.S.C. § 77(b)⁴⁸ and that “it [was] clear that [Bitcoins] can be used as money,” the Securities and Exchange Commission could proceed with its case.⁴⁹

Shavers’ political implications for Bitcoin businesses were immediately clear to legal advisers, who noted that regulators are gathering information on virtual currency and remain open to industry input, but remain silent on whether current law fits the technology or if they will enact different regulatory schemes in the future, with more market control.⁵⁰ Since a court deemed Bitcoins to be a security instrument, lawmakers on the federal and state level have aligned their focus on virtual

38 *Id.* at 19 (“If an entity is a Money Services Business (MSB) it must register with FinCEN.”).

39 *Id.* at 23.

40 See FIN. CRIMES ENFORCEMENT NETWORK, *supra* note 33.

41 *Id.*

42 *Id.*

43 *Id.*

44 31 C.F.R. § 1010.100(ff) (2011).

45 *Answers to Frequently Asked BSA Questions*, U.S. DEP’T OF THE TREASURY, FIN, CRIMES ENFORCEMENT NETWORK, http://www.fincen.gov/statutes_regs/bsa/bsa_faqs.html (last visited Oct. 18, 2013) (“One of the purposes of filing [Suspicious Activity Reports] is to identify violations or potential violations of law to the appropriate law enforcement authorities for criminal investigation. This is accomplished by the filing of a SAR that identifies the activity of concern.”).

46 No. 4:13-CV-416, 2013 WL 4028182 (E.D. Tex. Aug. 6, 2013).

47 *Id.* at *2

48 15 U.S.C. § 78c(a)(10) (2006) (defining security as “any note, stock, treasury stock, security future, security-based swap, bond, debenture... or, in general, any instrument commonly known as a ‘security’”).

49 *Shavers*, 2013 WL 4028182, at *2

50 See PERKINS COIE, CLIENT UPDATE: VIRTUAL CURRENCY: GOVERNMENT SCRUTINY CONTINUES TO GROW 2 (2013), available at http://www.perkinscoie.com/files/upload/08_21_2013_DVC_Update.pdf (“It remains to be seen whether virtual currency companies will be forced to mold their businesses to fit within the confines of financial regulations already on the books, or will be subject to an entirely new regulatory scheme designed with the technological complexities of virtual currency in mind.”).

currency issues, and Congress has begun its own investigation into the digital market.⁵¹ It remains unclear how Congress intends to proceed. After meeting with Bitcoin representatives, a HSGAC aide stated, “Talk to anyone in Silicon Valley or in New York— we don’t have the best reputation here of being ahead of the curve on a lot of these issues.”⁵²

B. Bitcoin Protocol

The Bitcoin cryptocurrency launched in late 2008 after Nakamoto released his concept paper.⁵³ Before this development, programmers had long-attempted to develop a method to resolve the double-spending problem particularly tied to virtual currencies.⁵⁴ Double spending occurs when a buyer can transfer his currency to a seller while retaining the original reserve. Without a central authority to validate transactions, there is a high risk of spending a unit of currency more than once. When real currency is traded, everyone involved can physically examine the currency, and counterfeiters face serious consequences.⁵⁵

The Bitcoin monetary supply is created by the amount of users who utilize the platform, releasing quantities in a block chain.⁵⁶ The platform has a finite limit of supplying twenty-one million Bitcoins over time; any further currency releases or transactions on the block chain must undergo a cycle of encryption and logging through the Bitcoin software.⁵⁷ The first link of the block chain is created by Bitcoin “miners” who race to solve a cryptographic equation by executing an intensive computer task known as a brute force crack.⁵⁸ By solving this progressive puzzle, the program

51 *Id.* at 1.

52 *See* Warmbrodt, *supra* note 2.

53 *See* SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM, *available at* <http://bitcoin.org/bitcoin.pdf> (last visited Nov. 7, 2013).

54 *See* Erik Bonadonna, *Bitcoin and the Double-Spending Problem*, COURSE BLOG FOR INFO 4220, CORNELL UNIV. (Mar. 29, 2013), <http://blogs.cornell.edu/info4220/2013/03/29/bitcoin-and-the-double-spending-problem/> (“Satoshi Nakamoto, the designer of the Bitcoin protocol, had anticipated this problem, and built in a mechanism to verify each transaction that a Bitcoin goes through.”).

55 *See* 18 U.S.C. § 471 (2006) (stating that the intent to defraud with any false obligation or other security shall be fined or imprisoned, or both).

56 *See* John Biggs, *Blockchain Smashers*, TECHCRUNCH (Oct. 16, 2013), <http://techcrunch.com/2013/10/16/blockchain-smashers/> (“Bitcoin is a mix of three monetary processes. First, it handles its own transaction processing (think credit card companies,) fraud prevention (the SEC and security firms), and currency issuance (the treasury.) In a real world these things are very complex systems with many moving parts. The beauty of Bitcoin is that each of these systems are reduced to very simple, very powerful cryptographic methods that ensures that each step in the chain verifies the next.”).

57 *See* BRITO & CASTILLO, *supra* note 5, at 7.

58 Ryan Broderick, *How to Get Rich on Bitcoin, by a System Administrator Who’s Secretly Growing Them on His School’s Computers*, MOTHERBOARD BETA, <http://motherboard.vice.com/blog/how-to-get-rich-on-bitcoin-by-a-system-administrator-who-s-secretly-growing-them-on-his-school-s-computers> (last visited Oct. 18, 2013) (“You can download the official Bitcoin software and just click a little check box that says ‘generate coins.’ From there your computer will try and solve a block. And if it solves the whole block, you get 50 Bitcoins. But, depending on the speed of your computer, it might take you a year or longer to solve a block. There is a service called ‘pooled mining,’ which splits up a bunch of these problems into little tiny problems and then everyone in the mining pool splits the reward based on how much they helped.”).

proves each peer-to-peer link is legitimate.⁵⁹ Miners are rewarded with Bitcoins after creating a block chain and when further transactions are added to the miner's block chain.⁶⁰ After Bitcoins are traded by users, another equation for decryption is added to the block chain.⁶¹

Bitcoin transactions are verified through a two-part cryptographic process.⁶² A seller creates a virtual message containing a buyer's public key and signs it with the seller's private key.⁶³ The time-stamped transfer is recorded on the block chain.⁶⁴ This time stamp contains only enough user information to prevent fraud, and results in an encrypted wallet that can be used to purchase goods or exchange for real currency through an intermediary.⁶⁵ Because of the computational power needed to form a new block chain and the public log from each transaction, the peer-to-peer exchange can be confidently verified.⁶⁶

At the nadir of the global financial crisis,⁶⁷ real currency holders were attracted to Bitcoin's transparency, ease, cheap transmission costs, and security.⁶⁸ The platform has been implemented in a range of industries from Berlin cafes accepting Bitcoins for a cup of coffee⁶⁹ to an exchange-traded fund administered by the Winklevoss twins of Facebook fame.⁷⁰

C. Tor

Tor was developed to be a "tool for free expression, privacy, and human rights."⁷¹ It anonymizes

59 *Id.*

60 *Id.*

61 *Id.*

62 *See* BRITO & CASTILLO, *supra* note 5, at 5. ("Transactions are verified, and double-spending is prevented, through the clever use of public-key cryptography.")

63 *Id.*

64 *Id.*

65 *Id.*

66 *Id.*

67 *See As Regulators Circle Bitcoin, Virtual Money Men Ante Up for the Digital Currency*, WASH. POST, Oct. 11, 2013, http://www.washingtonpost.com/business/as-regulators-circle-bitcoin-virtual-money-men-ante-up-for-the-digital-currency/2013/10/10/76519964-2d50-11e3-97a3-ff2758228523_story.html ("Bitcoin originated at the height of the financial crisis in November 2008, when a programmer or group of programmers known only as "Satoshi Nakamoto" released an academic paper outlining the design for a new peer-to-peer electronic cash system that removes the need to deal with third parties such as banks.")

68 *See* Chamath Palihapitya, *Why I Invested in Bitcoin*, THE TICKER, BLOOMBERG.COM (May 30, 2013, 12:06PM), <http://www.bloomberg.com/news/2013-05-30/bitcoin-the-perfect-schmuck-insurance.html> ("The point is that this fundamental trust [in the financial services industry] no longer exists; in its place, rises Bitcoin.")

69 *See* Monika Mueller-Kroll, *Berlin Restaurant Experiments With Virtual Currency*, NPR (June 1, 2012, 11:36 AM), <http://www.npr.org/2012/06/01/154140277/berlin-restaurant-experiments-with-virtual-currency> (describing the motivation of a coffee shop owner for allowing Bitcoin as a form of payment for customers).

70 *See* Linette Lopez, *The Winklevoss Twins Just Gave a Presentation on Bitcoin to a Room Full of Investors*, BUS. INSIDER (Sept. 17, 2013, 10:04AM), <http://www.businessinsider.com/winklevoss-bitcoin-bitcoin-presentation-2013-9> ("In short: There are a lot of possibilities here. What about remittances, they suggest. Or even better, a Bitcoin e-mail address that serves as a bank for people that are underbanked? What about micropayments—'it's generally understood that sending under \$2 over the Internet is impossible,' said one of the Twins.")

71 *See Tor Legal FAQ*, ELEC. FRONTIER FOUND. (Aug. 24, 2011), <https://www EFF.ORG/torchallenge/legal-faq/>.

users' internet protocol (IP) addresses by redirecting the original query through exit relays that can be located anywhere in the world.⁷² Originally sponsored by the Naval Research Laboratory,⁷³ Tor is currently distributed by the Department of State and the Broadcasting Board of Governors (BBG) Anti-Censorship Division to aid foreign dissidents and journalists.⁷⁴ Up until October 2012, the BBG directly funded Tor through this Division.⁷⁵

Tor has also caused headaches for American investigators seeking to seize webhosts of illicit materials and to identify uploaders and downloaders.⁷⁶ By working with internet service providers after identifying an IP address, law enforcement can determine a user's physical location.⁷⁷ Tor inhibits this ability by cloaking the source of an IP query.⁷⁸ Criminals may utilize Tor to attain the same anonymity desired by a human rights activist, so it is statistically likely that Tor facilitates illegal activity.⁷⁹ Since properly-configured relays provide little useful data for investigators,⁸⁰ exploiting information transmitted through Tor remains a priority for agencies including the Federal Bureau of Investigation (FBI) and National Security Agency (NSA).⁸¹ In a recent presentation entitled "Tor Stinks," NSA authors wrote "[the NSA] will never be able to de-anonymize all Tor users all the time,

72 See *What is a Tor Relay?*, ELEC. FRONTIER FOUND., <https://www.eff.org/torchallenge/what-is-tor> (last visited Oct. 18, 2013).

73 See ROGER DINGLEDINE, ET AL., TOR: THE SECOND-GENERATION ONION ROUTER (2004) (Aug. 9-13, 2004), available at https://www.usenix.org/legacy/events/sec04/tech/full_papers/dingledine/dingledine.pdf (implying that the Naval Research Laboratory was instrumental in developing Tor); see also *Tor: Overview*, THE TOR PROJECT, (last visited Nov. 3, 2013), <https://www.torproject.org/about/overview.html.en> (discussing the inception of Tor at the Naval Research Laboratory).

74 See Shane Harris & John Hudson, *Not Even the NSA Can Crack the State Dept's Favorite Anonymous Network*, FOREIGN POLICY (Oct. 4, 2013, 9:01 PM), http://thecable.foreignpolicy.com/posts/2013/10/04/not_even_the_nsa_can_crack_the_state_departments_online_anonymity_tool ("For years, the U.S. government has offered tools and training to help foreign dissidents and journalists circumvent detection by repressive governments.").

75 *Id.* ("The board also has worked with the Tor Solutions Group to develop "several enhancements" to its usability and performance for users subject to censorship. The BBG's budget for Internet anti-censorship issues runs a little over \$10 million a year"); see also *Internet Anti-Censorship*, BROAD. BD. OF GOVERNORS, <http://www.bbg.gov/wp-content/media/2013/05/Anti-Censorship-Fact-Sheet-May-2013.pdf> (last visited Oct. 18, 2013) ("The BBG is working with the Tor Solutions Group to significantly increase the number of high-speed Tor exit relays and bridges to improve the speed of the Tor network.").

76 See, e.g., Lisa Vaas, *FBI Claims that Tor Stymied Child Abuse Investigation*, NAKED SEC. (June 14, 2012), <http://nakedsecurity.sophos.com/2012/06/14/fbi-tor-child-abuse-investigation/> ("In at least one case, the US police's hunt for online child abuse images has been stymied by Tor, a Freedom of Information Act (FOI) request has revealed.").

77 See Bradley Mitchell, *Does IP Address Location (Geolocation) Really Work?*, ABOUT.COM, http://compnetworking.about.com/od/traceipaddresses/f/ip_location.htm (last visited Oct. 18, 2013).

78 See *Tor Legal FAQ*, ELEC. FRONTIER FOUND. (Aug. 24, 2011), <https://www.eff.org/torchallenge/legal-faq/>.

79 *Id.*

80 *Id.*

81 See Timothy B. Lee, *Everything You Need to Know About the NSA and Tor in One FAQ*, THE SWITCH, WASHIN. POST (Oct. 4, 2013, 3:36PM), <http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/04/everything-you-need-to-know-about-the-nsa-and-tor-in-one-faq/> ("The FBI recently admitted that it had taken control of Freedom Hosting, a company that provides Tor hidden services, in July. The server began serving malware that 'exploited a security hole in Firefox to identify users of the Tor Browser Bundle.' That apparently allowed the NSA to identify people who had been browsing a Tor hidden service...").

but with manual analysis we can de-anonymize a very small fraction [of users].”⁸² Investigations can grind to a halt if law enforcement can monitor traffic, but not isolate the correct IP address.⁸³

II: SILK ROAD’S EFFECT ON REGULATION OF VIRTUAL CURRENCIES

On June 1, 2011, blogger Adrian Chen posted an article about a new hidden website called Silk Road, where users “can buy any drug imaginable.”⁸⁴ Five days later, U.S. Senators Charles Schumer and Joe Manchin III “urged” Attorney General Eric Holder and Drug Enforcement Administration (DEA) Administrator Michelle Leonhart to immediately seize the Silk Road network.⁸⁵ The Attorney General is authorized to confiscate entities involved in the illegal online delivery and distribution of controlled substances under the Ryan Haight Online Pharmacy Consumer Protection Act.⁸⁶

Silk Road, a dark website hidden from the typical internet browser, provided an anonymous marketplace for buyers of illegal drugs, weapons, and malware, exclusively using Bitcoins.⁸⁷ The website further advised sellers on shipping methods to avoid detection.⁸⁸ To put Silk Road’s extensiveness in perspective of the total Bitcoin market, there are approximately 11.75 million Bitcoins in existence, and Silk Road’s revenues approached 9.5 million Bitcoins. Accordingly, much of the global Bitcoin supply was being spent on illicit activities available through the website.⁸⁹

The Senators’ letter recommended that the DOJ request a court to order the seizure of the website’s domain name.⁹⁰ Silk Road, however, operated on the Tor network, which adds randomly generated characters⁹¹ to the actual domain name.⁹² An internet user could find the current Tor ad-

82 See *‘Tor Stinks’ Presentation – Read the Full Document*, THE GUARDIAN (Oct. 4, 2013, 10:49PM), <http://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document>.

83 See Lisa Vaas, *FBI Claims that Tor Stymied Child Abuse Investigation*, NAKED SEC. (June 14, 2012), <http://nakedsecurity.sophos.com/2012/06/14/fbi-tor-child-abuse-investigation/>

84 See Adrien Chen, *The Underground Website Lets You Buy Any Drug Imaginable*, KOTAKU (June 1, 2011, 4:20 PM), <http://kotaku.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160>.

85 Press Release, Senator Joe Manchin, Manchin Urges Federal Law Enforcement to Shut Down Online Black Market for Illegal Drugs, (June 6, 2011), <http://www.manchin.senate.gov/public/index.cfm/press-releases?ID=284ae54a-acf1-4258-be1c-7acee1f7e8b3>.

86 Ryan Haight Online Pharmacy Consumer Protection Act of 2008, Pub. Law No. 110-425, § 2, 122 Stat. 4280 (2008).

87 See Kevin Dolak, *Silk Road Arrest Shines Light on ‘Dark Web’*, ABC NEWS (Oct. 3, 2013,), <http://abcnews.go.com/Technology/silk-road-arrest-shines-light-dark-web/story?id=20460774> (“The FBI’s takedown of a billion-dollar black market website that allowed users to sell and purchase illegal items has shined a spotlight on the ‘dark Web,’ which masks users’ online identities while providing a shield for everyone from hackers to journalists and the police.”).

88 See Press Release, Senator Joe Manchin, *supra* note 88 (“After completing online purchases, users are instructed to disguise shipments and vacuum seal drugs that may be detected by odor.”)

89 See Raddacla Wakeman, *Take the Drugs, But Don’t Take the People’s Bitcoins*, NEW REPUBLIC (Oct. 9, 2013), <http://www.newrepublic.com/article/115086/tor-snowden-and-battle-over-bitcoin>.

90 See 18 U.S.C. § 982(a)(1) (2006) (allowing for the forfeiture to the U.S. of any real or personal property involved in or traceable to certain financial crimes).

91 See, e.g., Mathew J. Schwartz, *Tor Anonymity Cracked; FBI Porn Investigation Role Questioned*, INFO. WEEK SEC., (Aug. 5, 2013 11:25 AM), <http://www.informationweek.com/security/encryption/tor-anonymity-cracked-fbi-porn-investiga/240159424> (discussion how the Tor service hides services by using randomly generated domain names).

92 See Complaint ¶ 12(b), *United States v. Ulbricht*, No. 13 MAG 02328, 2013 WL 5460023 (S.D.N.Y. Sept. 27, 2013)

dress posted by Silk Road users on forums.⁹³ Silk Road's servers were also hosted in several foreign countries.⁹⁴ By employing a “tumbler”⁹⁵ to further obfuscate Bitcoin transactions and protect users and administrators, Silk Road was able to generate an estimated \$1.2 billion in sales and \$80 million in commissions.⁹⁶

According to the criminal complaint of Silk Road's alleged owner, the special agent in charge of the investigation claimed the marketplace “emerged as the most sophisticated and extensive criminal marketplace on the Internet today.”⁹⁷ It took over two years for law enforcement agents from the DOJ, FBI, DEA, DHS Homeland Security Investigations, and Treasury Internal Revenue Service (IRS) Criminal Investigation to confiscate Silk Road and to identify and arrest the website's owner for federal money laundering, computer hacking, and narcotics trafficking conspiracies under 21 U.S.C. § 846, 18 U.S.C. §§ 1030 and 1956.⁹⁸ It was the improper implementation of Tor by the site's contended owner that granted the task force the opportunity to match his IP address to old forum posts and execute an arrest.⁹⁹ Separately, a random package search by DHS that discovered forged identification documents allegedly addressed to the defendant arriving from Canada resulted in a positive photo identification of the suspect and a separate charge.¹⁰⁰

Important details regarding law enforcement's methodology used to seize Silk Road remain unclear. According to the criminal complaint, a mutual legal assistance treaty (MLAT)¹⁰¹ request to an unconfirmed sovereign allowed the FBI to copy a Silk Road server on July 23, 2013.¹⁰² Icelandic enforcement confirmed their assistance to U.S. authorities and their confiscation of a server and three

(claiming that defendant added a Bitcoin tumbler to Silk Road to make the illegal transactions untraceable).

93 See Andrew Coutts, *TorSearch Makes Finding the Next Silk Road a Lot Easier*, DIGITAL TRENDS (Oct. 11, 2013), <http://www.digitaltrends.com/web/torsearch-tor-network-hidden-services/> (“One of the things that keeps Tor's “hidden services” websites hidden is that they are often difficult to find through normal avenues. It was beneath this veil that online drug supermarket Silk Road, which was recently seized by the FBI, operated for two and half years. And it's where the illegal drug sites that have risen in prominence since Silk Road's fall currently exist.”).

94 See Complaint ¶ 22, *Ulbricht*, 2013 WL 5460023 (No. 13 MAG 02328).

95 Parker Higgins, *Why You Can't Blame Bitcoin for Silk Road Shadiness*, GIZMODO (Oct. 5, 2013, 5:00PM), <http://gizmodo.com/why-you-cant-blame-bitcoin-for-silk-road-shadiness-1441572365> (“According to the complaint, ‘the only function served by such ‘tumblers’ is to assist with the laundering of criminal proceeds.’ Really, the purpose of a tumbler is to attempt to make a bitcoin transaction as anonymous and private as cash.”); see also Complaint ¶ 21, *Ulbricht*, 2013 WL 5460023 (No. 13 MAG 02328) (stating that Silk Road uses a tumbler to process Bitcoin transactions in a “manner designed to frustrate the tracking of individual transactions through the [block chain], sending all payments through a complex, semi-random series of dummy transactions... making it nearly impossible to link your payment with any coins leaving the site.”).

96 Complaint ¶ 16, *Ulbricht*, 2013 WL 5460023 (No. 13 MAG 02328).

97 *Id.*

98 See Joseph Goldstein, *Arrest in U.S. Shuts Down a Black Market for Narcotics*, N.Y. TIMES (Oct. 2, 2013), <http://www.nytimes.com/2013/10/03/nyregion/operator-of-online-market-for-illegal-drugs-is-charged-fbi-says.html>; see also Complaint, *Ulbricht*, 2013 WL 5460023 (No. 13 MAG 02328).

99 See Complaint ¶ 24, *Ulbricht*, 2013 WL 5460023 (No. 13 MAG 02328).

100 See *id.* ¶ 28; see also 18 U.S.C. § 1028 (2006) (describing the crime and penalties related to false identification possession and trafficking).

101 2012 INCSR: *Treaties and Agreements*, U.S. DEP'T OF STATE BUREAU OF INT'L NARCOTICS AND LAW ENFORCEMENT AFFAIRS (Mar. 7, 2012), <http://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm>.

102 Complaint ¶ 22, *Ulbricht*, 2013 WL 5460023 (No. 13 MAG 02328).

million Bitcoins,¹⁰³ but Iceland is not a signatory to any MLAT.¹⁰⁴ By copying the server, authorities gained access to private messages between Silk Road's administrators and users that may be used to identify specific transactions of illicit goods if matched to "Blockchain" public logs.¹⁰⁵ Even though the Silk Road server has been captured, the Bitcoin transactions it and the suspect's wallet contain remain difficult for law enforcement to decrypt due to the tumbler used, delaying the identification of buyers and sellers of illegal materials and liquidation of criminal proceeds.¹⁰⁶

III. NATIONAL SECURITY IMPLICATIONS OF DECENTRALIZED VIRTUAL CURRENCIES AND CURRENT FEDERAL AUTHORITY

As the Silk Road saga demonstrated to frustrated policymakers¹⁰⁷ and law enforcement agents¹⁰⁸ from the local level up to the international, combining Bitcoin's peer-to-peer technology with Tor can increase users' chances of remaining anonymous.¹⁰⁹ If fully anonymous, using virtual currency can be the online equivalent of strangers trading cash for illicit goods on the street: untraceable. The New York Department of Financial Services¹¹⁰ declared that unregulated virtual currencies are a "Wild West for narcotraffickers and other criminals, that . . . threaten . . . national security."¹¹¹

Realizing the urgent threat to communities an easily-accessible anonymous drug trade presents, the DEA became a lead agency in confronting what Senator Manchin III described as a constant

103 See Adrianne Jeffries, *Lessons from Silk Road: Don't Host Your Virtual Illegal Drug Bazaar in Iceland*, THE VERGE (Oct. 14, 2013, 11:47AM), <http://www.theverge.com/2013/10/14/4836994/dont-host-your-virtual-illegal-drug-bazaar-in-iceland-silk-road>.

104 *International Narcotics Control Strategy Report Vol. II: Money Laundering and Financial Crimes*, U.S. DEP'T OF STATE BUREAU FOR INT'L NARCOTICS AND LAW ENFORCEMENT AFFAIRS (Mar. 2013), <http://www.state.gov/documents/organization/204280.pdf>.

105 See Jeffries, *supra* note 103 ("While the country may have protected WikiLeaks from the Americans, it's not harboring the recently busted illegal drug bazaar Silk Road."); see also Complaint ¶ 19, *Ulbricht*, 2013 WL 5460023, (No. 13 MAG 02328) (describing that the "Blockchain" was a public ledger stored on peer-to-peer networks).

106 See Omar Dieb, *Bitcoin After Silk Road*, THE STANFORD DAILY (Oct. 12, 2013), <http://www.stanforddaily.com/2013/10/12/bitcoin-after-silk-road/> ("In order to obscure the flow of Bitcoin, people often run Bitcoins through Bitcoin tumblers. Tumblers hide the true origin of your money by replacing your Bitcoins with a mixture of random Bitcoins with different transaction histories.").

107 See *The Internet Poses Unique Challenges for Drug Prohibition*, THE CONVERSATION (Apr. 5, 2012), <http://theconversation.com/the-internet-poses-unique-challenges-for-drug-prohibition-6262> ("It's unclear whether any policy responses to control Silk Road have been effective.").

108 See Michael George, *'Silk Road' Website Called the Amazon, eBay of Heroin, Cocaine, Drug Trafficking*, ABC ACTION NEWS (June 10, 2011), http://www.abcactionnews.com/dpp/news/local_news/investigations/silk-road-website-called-the-amazon-ebay-of-heroin-cocaine-drug-trafficking ("The DEA wouldn't confirm to ABC Action News whether or not they're investigating Silk Road. Captain Robert Alfonso of the Pinellas County Sheriff's Office says the law on websites like Silk Road is still vague.").

109 See BRITO & CASTILLO, *supra* note 5, at 8 ("To increase the chances of remaining pseudonymous, one would have to employ anonymizing software like Tor, and take care never to transact with Bitcoin addresses that could be tied back to one's identity.").

110 See Jeff Cox, *Bitcoin Bonanza: Cyprus Crisis Boosts Digital Dollars*, CNBC (Mar. 27, 2013, 12:53PM), <http://www.cnbc.com/id/100597242>.

111 Notice, Lawsky, *supra* note 25.

“[narcotics] scourge . . . whether it’s an online black market or in . . . pill mills.”¹¹² Under the auspices of the Controlled Substances Act, the DEA made the earliest confirmed federal arrest of an alleged Silk Road dealer of Adderall, Dexedrine, Vyvanse, Klonopin, and Suboxone in August 2013.¹¹³ Having already created a Bitcoin wallet, the DEA published an Official Notification announcing that for the first time the federal government had seized and transferred into its possession 11.02 Bitcoins, or \$814.22.¹¹⁴ The Bitcoin public log let observers view the exact time of the seizure and the transfer recipients.¹¹⁵ It is possible either that the suspect’s computer with an unencrypted wallet was forensically analyzed, or more likely, if the user’s private key was unknown, that the DEA created its own Silk Road account, accepted the Bitcoin transfer, and arrested the alleged dealer at a later point.¹¹⁶ In 2012, the DOJ and DEA consolidated regulations for seizures, including the pre-forfeiture disposition of property liable to be greatly reduced in value¹¹⁷ under 28 C.F.R. § 8.14 (2011). Bitcoins are subject to extreme fluctuations in value,¹¹⁸ dropping twenty percent in only three hours after Silk Road shut down a few weeks after the DEA operation.¹¹⁹

The USA PATRIOT Act § 311 allows FinCEN to designate an institution a money launderer of primary concern, prohibiting U.S. banks from maintaining relationships with foreign institutions. This law has proven to be a useful tool for the Treasury and DOJ in setting precedent for disconnecting illegally-operated virtual currency exchangers from the U.S. economy.¹²⁰ Building upon FinCEN guidance, DHS Immigration and Customs Enforcement issued a seizure warrant on May 14, 2013 to Japan-based Mt. Gox’s U.S. subsidiary for allegedly failing to register with FinCEN as a money transmitting business dealing in Bitcoins.¹²¹ In exchange for depositing dollars with a payment processor based in Iowa, Mt. Gox would disburse Bitcoins to users and register transactions in

112 Press Release, Manchin, *supra* note 88.

113 See Jamie Condliffe, *Drug Enforcement Agency Seizes First Bitcoins from Silk Road Dealer*, GIZMODO (June 27, 2013, 3:50AM), <http://gizmodo.com/drug-enforcement-agency-seizes-first-bitcoins-from-silk-595189571>.

114 Brian Cohen & Adam B. Levine, *Users Bitcoins Seized by DEA*, LET’S TALK BITCOIN (July 9, 2013), <http://letstalkbitcoin.com/users-bitcoins-seized-by-dea/#.U14HBFDEoYM>.

115 *Id.*

116 See *id.* (indicating that Bitcoin protocol was not violated, and that the money was seized through a sting operation, rather than directly from a user’s wallet).

117 See Consolidation of Seizures and Forfeiture Regulations, 77 Fed. Reg. 56,093 (Sept. 12, 2012) (to be codified at 21 C.F.R. pt. 1316 and 28 C.F.R. pts. 8-9) (publishing the final rule consolidating seizure and forfeiture regulations from DOJ Drug Enforcement Agency).

118 See Lauren Orsini, *What’s Bitcoin Worth in the Real World?*, READWRITE (Aug. 8, 2013), <http://readwrite.com/2013/08/08/whats-bitcoin-worth-in-the-real-world#awesm=~ompVJzergXj9Xd> (proffering that Bitcoin’s value is its scarcity).

119 See Nathan Mattise, *Amid Silk Road Uncertainty, Bitcoin Value Drops Over 20% in 3 Hours*, ARSTECHNICA (Oct. 2, 2013, 3:03PM), <http://arstechnica.com/information-technology/2013/10/amid-silk-road-uncertainty-bitcoin-value-drops-over-20-in-3-hours/> (noting that Bitcoin was “experiencing a period of extreme volatility” in the wake of the Silk Road shutdown).

120 See Peter Cohan, *After Liberty Reserve Shutdown, is Bitcoin Next?*, FORBES (May 29, 2013, 7:55AM), <http://www.forbes.com/sites/petercohan/2013/05/29/after-liberty-reserve-shut-down-is-bitcoin-next/> (noting the Treasury Department’s efforts to sever Liberty Reserve’s access to the U.S. financial system).

121 See Jeremy Kirk, *Mt. Gox Accused of Violating US Money Transfer Regulations*, PCWORLD (May 16, 2013, 7:14 AM), <http://www.pcworld.com/article/2038858/mt-gox-accused-of-violating-us-money-transfer-regulations.html> (ascribing the subsequent seizure to Mt. Gox’s failure to comply with federal regulations).

a central database; it did not however sign mandatory FinCEN forms declaring the subsidiary to be an exchanger.¹²² On May 28, 2013 the federal government went a step further when U.S. Attorney Preet Bharara announced the indictment¹²³ of the then-popular virtual currency exchange Liberty Reserve, which actively hid its register of users' activities.¹²⁴ Unlike Mt. Gox, Liberty Reserve would exchange users' dollars for LR, another virtual currency, allowing "traffickers . . . computer hackers for hire . . . unregulated gambling enterprises; and underground drug-dealing websites"¹²⁵ to send LR to third-parties for transfer back into real currency without a financial trail. FinCEN Director Jennifer Calvery invoked § 311 of the PATRIOT Act,¹²⁶ a first for a virtual currency exchange case.¹²⁷ Criminals had opened accounts under patently false names such as "Russia Hackers" or simply "cocaine," and Liberty Reserve would charge a commission and privacy fee to hide users' account numbers on each transaction.¹²⁸ Bharara called the company a "hub for fraudsters, hackers, and traffickers" after an investigation spanning seventeen countries.¹²⁹ DOJ charged the firm with a \$6 billion money laundering scheme, completing fifty-five million suspected criminal transactions while it acted as an unlicensed money transmitting business.¹³⁰

Threats to the national welfare are deeply entwined with threats to national security.¹³¹ The Foreign Account Tax Compliance Act of 2010 ("FATCA") is intended to combat offshore tax

122 See Jeremy Kirk, *Document Cloud: In the Matter of the Seizure of the Contents of One Dwolla Account*, IDG NEWS SERVICE, <https://www.documentcloud.org/documents/701175-mt-gox-dwolla-warrant-idg-news-service.html> (last visited Oct. 19, 2013) (explaining that Dwolla is the payment processor for Mt. Gox and its U.S. subsidiary Mutum Sigillum LLC).

123 Press Release, U.S. Attorney's Office S.D.N.Y., Manhattan U.S. Attorney Announces Charges Against Liberty Reserve, One of World's Largest Digital Currency Companies, And Seven of its Principals and Employees for Allegedly Running a \$6 Billion Money Laundering Scheme (May 28, 2013), <http://www.justice.gov/usao/nys/pressreleases/May13/LibertyReservePR.php>.

124 See Marc Santora, William K. Rashbaum & Nicole Perloth, *Online Currency Exchange Accused of Laundering \$6 Billion*, N.Y. TIMES (May 28, 2013), <http://www.nytimes.com/2013/05/29/nyregion/liberty-reserve-operators-accused-of-money-laundering.html?pagewanted=1&r=3&hpw&> (proffering that Liberty Reserve allowed members' to conduct their activities with virtual anonymity).

125 Sealed Indictment ¶ 20, United States v. Liberty Reserve S.A., 13 Crim 368 (S.D.N.Y. May 23, 2013), *available at* <http://www.justice.gov/usao/nys/pressreleases/May13/LibertyReserveetalDocuments/Liberty%20Reserve,%20et%20al.%20Indictment%20-%20Redacted.pdf>.

126 See Press Release, U.S. Dep't of the Treasury, Treasury Identifies Virtual Currency Provider Liberty Reserve as a Financial Institution of Primary Money Laundering Concern under USA Patriot Act Section 311, (May 28, 2013), <http://www.treasury.gov/press-center/press-releases/Pages/jl1956.aspx> (using § 311 of the PATRIOT Act to list Liberty Reserve as an "financial institution of primary money laundering concern").

127 See Cohan, *supra* note 120 ("The Treasury Department set a precedent in using the 2001 Patriot Act against a virtual currency to sever the link between Liberty Reserve and the U.S. financial system.").

128 *Id.*

129 Press Release, U.S. Attorney's Office S.D.N.Y., *supra* note 123. The seventeen countries involved included Costa Rica, the Netherlands, Spain, Morocco, Sweden, Switzerland, Cyprus, Australia, China, Norway, Latvia, Luxembourg, the United Kingdom, Russia, Canada, and the United States. *Id.*

130 *Id.*

131 See Bob Killebrew & Jennifer Bernal, *Crime Wars: Gangs, Cartels and U.S. National Security*, CTR. FOR A NEW AM. SECURITY (Sept. 2010), http://www.cnas.org/files/documents/publications/CNAS_CrimeWars_KillebrewBernal_3.pdf ("Crime, terrorism and insurgency are interwoven in new and dangerous ways that threaten not just the welfare but also the security of societies in the Western Hemisphere.").

evasion,¹³² which is estimated to account for \$150 billion of lost revenue each year.¹³³ FATCA § 6103 permits “disclosure of [income tax] return information to apprise appropriate officials of criminal or terrorist activities or emergency circumstances.” The Supreme Court has held that bank customers do not have a privacy interest in personal records maintained by a bank, which are in fact the institution’s business records.¹³⁴ A letter written to IRS Commissioner Douglas Shulman by Senator Carl Levin in January 2012 relies on this reasoning to demonstrate the validity of a subpoena for customers’ documents in the investigation of a financial or terrorist crime.¹³⁵ There is evidence that Bitcoin has been used by those avoiding taxes and unwanted attention by exchanging small amounts of dollars from multiple bank accounts to a single Bitcoin wallet offshore, an activity typical of those attempting to hide their wealth.¹³⁶ By doing so, it is possible that criminals along with tax evaders¹³⁷ can slip through the cracks of FATCA, not only preventing the IRS from generating revenue¹³⁸ but also depriving security agencies of a valuable source of intelligence on crime and terror activity.¹³⁹ Combating terrorism by interpreting bank documents remains a priority for

132 See *The Foreign Account Tax Compliance Act (FATCA)*, DLA PIPER, <http://www.dlapiper.com/files/Uploads/Documents/FATCA-Alert.pdf> (last visited Oct. 19, 2013) (“This legislation is a direct result of the focus by the United States (and other industrialized and developing countries) on combating offshore tax evasion and recouping much needed tax revenues.”).

133 See Phineas Baxandall & Dan Smith, *Picking Up the Tab 2013: Average Citizens and Small Businesses Pay the Price for Offshore Tax Havens*, U.S. PUB. INTEREST RESEARCH GRP. (Apr. 2013), http://uspirg.org/sites/pirg/files/reports/Picking_Up_the_Tab_2013_USPIRG.pdf.

134 *United States v. Miller*, 424 U.S. 435, 445-46 (1976) (holding that the BSA does not violate Fourth Amendment rights, and is intended to facilitate the use of a proper, long-standing law enforcement technique by insuring records are available when needed.)

135 See Letter from Senator Carl Levin to the Honorable Douglass H. Shulman, Commissioner of the Internal Revenue Service, and Emily McMahon, Acting Assistant Secretary for Tax Policy, U.S. Dep’t of the Treasury, Notice 2011-34: Implementing the Foreign Account Tax Compliance Act (Jan. 11, 2012), <http://bsmlegal.com/PDFs/CarlLevin.pdf> (“Finally, one additional issue is critical to successful implementation of FATCA’s disclosure obligations: treating FATCA offshore account information as non-tax return information to ensure its accessibility to law enforcement and national security communities combating crimes other than tax evasion.”).

136 See Lauren French & Zachary Warmbrodt, *Bitcoin: Tax Haven of the Future*, POLITICO (Aug. 10, 2013, 6:45PM), <http://www.politico.com/story/2013/08/bitcoin-tax-haven-95420.html> (“[T]he Bitcoin economy is already seeing signs that the currency is being used to hide wealth. Some buyers, for example, will use multiple bank accounts to buy trivial amounts of the coins, which are then sent to a central account. “These are characteristics of individuals who want to avoid paying taxes.”).

137 See Brian Kindle, *FATCA May Identify Tax Cheats, But Its Dragnet for Financial Criminals May Produce an Even Bigger Yield*, ASS’N OF CERTIFIED FIN. CRIME SPECIALISTS (Mar. 1, 2012), <http://www.acfcs.org/fatca-may-identify-tax-cheats-but-its-dragnet-for-financial-criminals-may-produce-an-even-bigger-yield/> (“The Act gives the IRS unprecedented new power to catch tax evaders worldwide, but its concurrent dragnet for financial criminals may be an equally desirable endgame.”).

138 See U.S. GOV’T ACCOUNTABILITY OFFICE, GAO-13-516: VIRTUAL ECONOMIES AND CURRENCIES: ADDITIONAL IRS GUIDANCE COULD REDUCE TAX COMPLIANCE RISKS HIGHLIGHTS OF GAO-13-516 (2013), available at <http://gao.gov/assets/660/654620.pdf> (“Because of the limited reliable data available on their size, it is difficult to determine how significant virtual economy and currency markets may be or how much tax revenue is at risk through their usage. Some experts with whom we spoke indicated a potential for growth in the use of virtual currencies.”).

139 See Matt Welch, *How the IRS Can Share Your Bank Info with Security Agencies*, REASON (July 26, 2013, 10:02 AM), <http://reason.com/blog/2013/07/26/how-the-irs-can-share-your-bank-info-wit> (“Title 26, Section 6103 of the tax

the U.S. intelligence community,¹⁴⁰ which FACTA Intergovernmental Agreements¹⁴¹ abroad intend to remedy at lower risk and cost to the public than covert action.¹⁴² If Bitcoins become a tool for bypassing FACTA, important bank secrets may remain unrevealed.

Concerns about the government's ability to detect terrorist group financing have also been raised.¹⁴³ A FBI intelligence assessment specifically pinpointed Bitcoin as "likely [to] continue to attract cybercriminals who view it as a means to transfer, launder, or steal funds as well as a means of making donations to groups participating in illegal activities."¹⁴⁴ The same assessment warns that as Bitcoin develops into a mainstream means of exchange, it will become increasingly prevalent in illegal uses throughout the internet.¹⁴⁵ These anonymous financial transfers hinder the government's ability to detect illicit financing.¹⁴⁶ Bitcoin mining software exportation is restricted by the Department of Commerce Bureau of Industry and Security due to its encryption capabilities,¹⁴⁷ but sanctioned nationals have discovered methods to obtain the virtual currency through e-commerce.¹⁴⁸ Iranians,¹⁴⁹ for example, have avoided Treasury Office of Foreign Assets Control sanctions¹⁵⁰ and the effects of inflation by swapping Bitcoins for normally unobtainable U.S. dollars and keeping

code opens doors that allow US government agencies, including intelligence agencies, and even Congress, to gain access to information obtained through FATCA. For instance, ACFCS notes, Section 6103 'permits disclosure of "return information" to certain Federal officers and employees and law enforcement agencies for purposes of combating terrorism."').

140 See Alexi Mostrous & Ian Cobain, *CLAs Secret UK Bank Trawl May Be Illegal*, THE GUARDIAN (Aug. 20, 2006), <http://www.theguardian.com/uk/2006/aug/21/business.currentaccounts> (acknowledging that the agency has received financial records from the Belgium co-operative that processes money transfers from banks around the world, a program that was initiated after September 11, 2011, and had included details of an estimated 4.6 million British banking transactions); see also *Follow the Money: NSA Spies on International Payments*, DER SPIEGEL (Sep. 16, 2013) (describing the NSA's "own financial databank" called Tracfin).

141 See Resource Center: *Foreign Account Tax Compliance Act (FATCA)*, U.S. DEP'T OF THE TREASURY, <http://www.treasury.gov/resource-center/tax-policy/treaties/Pages/FATCA.aspx> (last visited on Oct. 19, 2013)

142 See Terri Eyden, *FATCA: United States and Switzerland Issue Joint Statement Re: Tax Evasion Investigations*, ACCOUNTING WEB (Aug. 20, 2013), <http://www.accountingweb.com/article/fatca-united-states-and-switzerland-issue-joint-statement-re-tax-evasion-investigations>.

143 See BRITO & CASTILLO, *supra* note 5 at 21 ("Another concern is that Bitcoin can be used to launder money for financing terrorism and trafficking in illegal goods. Although these worries are currently more theoretical than evidential, Bitcoin could indeed be an option for those who wish to discreetly move ill-gotten money.").

144 See *Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Illicit Activity*, FEDERAL BUREAU OF INVESTIGATION DIRECTORATE OF INTELLIGENCE (Apr. 24, 2012), <http://cryptome.org/2012/05/fbi-bitcoin.pdf>.

145 *Id.*

146 See Eyden, *supra* note 142 (stating law enforcement's interests in detecting illicit financing).

147 See Jon Matonis, *As Inflation Rages in Iran, Bitcoin Software Not Available*, FORBES (Oct. 9, 2012, 3:01PM), <http://www.forbes.com/sites/jonmatonis/2012/10/09/as-inflation-rages-in-iran-bitcoin-software-not-available/> (referencing Andresen, the Chief Scientist for the Bitcoin Foundation, who noted that Bitcoin "compiles against" the OpenSSL library); see also 15 C.F.R. § 742.15 (2012).

148 See Max Raskin, *Dollar-Less Iranians Discover Virtual Currency*, BLOOMBERG BUSINESSWEEK (Nov. 29, 2012), <http://www.businessweek.com/articles/2012-11-29/dollar-less-iranians-discover-virtual-currency>.

149 *Id.* (highlighting that Iranians can use Bitcoins to buy music at an online store).

150 See *What You Need to Know About U.S. Economic Sanctions*, U.S. DEP'T OF THE TREASURY OFFICE OF FOREIGN ASSETS CONTROL, <http://www.treasury.gov/resource-center/sanctions/Programs/Documents/iran.pdf> (last visited on Oct. 19, 2013).

their holdings outside of the country.¹⁵¹ Israel and other foreign governments are taking the threat of untraceable online transactions seriously, finding that decentralized virtual currencies may be used as a discrete method for financing terror groups.¹⁵²

IV: FITTING TWENTY-FIRST CENTURY CRIMES INTO OLD LAWS

The federal government has become increasingly aware that virtual currencies like Bitcoin represent a promising technology, but they also deserve increased scrutiny due to possible risks to national security.¹⁵³ In August 2013, the HSGAC began an inquiry¹⁵⁴ into emerging virtual currency technology seeking a whole-government approach to understand the market, and to provide a practical framework for their regulation.¹⁵⁵ Regulators and law enforcement are reportedly “worried virtual currency markets could be used for money laundering and tax avoidance,”¹⁵⁶ even though block chain transactions are publicly available. The Committee’s inquiry represents the most substantial Congressional interest since Bitcoin’s inception, with letters sent to the DHS, DOJ, Treasury, Federal Reserve, SEC, Commodity Futures Trading Commission (CFTC), and White House Office of Management and Budget.¹⁵⁷ Some officials who have spoken to HSGAC claim that agencies have made comments that “seem not to be sort of in line with what another department said.”¹⁵⁸ The Chief Executive of Coinsetter, a virtual currency firm, stated that “regulatory uncertainty right now is the bottleneck for innovation in this space.”¹⁵⁹

This interest has resulted, so far, in no concrete action. Multiple Executive agencies are instead “mulling”¹⁶⁰ over whether Bitcoin and other currencies should fall under their rules, resulting in several groups claiming jurisdiction. Without central guidance, it is unclear to the public and other regulators what responsibilities and options for enforcement exist. The CFTC Board is determining whether there is a federal role in the virtual currency market, but Commissioner Bart Chilton stated that the CFTC could regulate Bitcoin if the Board wanted.¹⁶¹ Vice Chairwoman Janet Yellen

151 Raskin, *supra* note 148.

152 See Tav Pavel, *Bitcoins: Currency for Criminals?*, AL-MONITOR (Sept. 30, 2013), <http://www.al-monitor.com/pulse/originals/2013/09/israel-bitcoin-currency-banks-terror-drug.html> (recognizing that virtual currency can be used by criminals and terrorists as currency to fund their activities anonymously, out of the reach of the authorities)

153 See Margo Tank, *Regulatory Alert: Emerging Payment Providers Can Learn from Liberty Reserve and Mt. Gox*, PAYMENTS JOURNAL (July 2, 2013), http://www.paymentsjournal.com/Content/Blogs/Industry_Blog/16892/ (commenting that financial regulators are looking at Bitcoins to determine whether it undermines the current protections on the financial system).

154 See *Virtual Currency Letter (Redacted)*, U.S. SENATE COMMITTEE ON HOMELAND SEC. AND GOVERNMENTAL AFFAIRS (Aug. 12, 2013), <http://www.hsgac.senate.gov/download/letter-to-secretary-napolitano-on-virtual-currencies>.

155 *Id.*

156 See Warmbrodt, *supra* note 2.

157 *Id.*

158 *Id.*

159 See Chris Evans, *Certain Regulations for Bitcoins in the U.S. on Focus*, BITCOIN GAMBLING GUIDE, <http://www.bitcoingg.com/certain-regulations-for-bitcoins-in-the-u-s-on-focus/> (last visited Oct. 19, 2013).

160 See Douwe Miedema, *Regulator Mulls Setting Rules for Digital Currency Bitcoin*, REUTERS (May 6, 2013, 6:32PM), <http://www.reuters.com/article/2013/05/06/net-us-bitcoin-regulation-idUSBRE9450Y520130506>.

161 *Id.*

disclosed that the Federal Reserve is researching the potential negative effects of Bitcoin on the U.S. financial system.¹⁶² The IRS is rumored¹⁶³ to be deploying additional guidance on the use of virtual currencies after a Government Accountability Office report recommended low-cost methods to introduce tax-reporting requirements.¹⁶⁴ The DHS, DOJ, and SEC are already in the midst of financial crime and narco-trafficking probes related to Bitcoin usage.

Relying on further regulation of third-party exchangers as seen in FinCEN guidance, however, would be an inadequate solution. The peer-to-peer nature of decentralized cryptocurrency bypasses third-parties completely, undermining this regulatory path.¹⁶⁵ The FBI, for example, has proposed¹⁶⁶ that third-party Bitcoin exchangers already subject to FinCEN guidance should further require valid identification or bank information to complete transactions so law enforcement can quickly identify malicious actors. Requiring domestic exchangers to add verification measures to transactions may help weed out illegal users of virtual currencies. It is also difficult to see how U.S. regulations on foreign third-party exchangers could be properly enforced without similar measures being adopted abroad.

Other agencies are questioning whether their current laws can be adapted to virtual currency, or if new measures are needed. New York is one of the first states¹⁶⁷ to test the waters on decentralized virtual currency regulations with a forward-thinking mindset toward this new technology. DFS Superintendent Benjamin Lawsky has already sent subpoenas to twenty-two of the leading virtual currency companies¹⁶⁸ as DFS weighs the implementation of “guardrails” to protect consumers and national security.¹⁶⁹ This information-gathering will enable DFS to determine whether newly-

162 See *The Fed is Studying the Risks of Bitcoin*, BUSINESS INSIDER/AGENCE FRANCE PRESSE (June 4, 2013, 11:35 AM), <http://www.businessinsider.com/the-federal-reserve-is-officially-studying-the-risks-of-bitcoin-2013-6>.

163 See Timothy Lavin, *The SEC Shows Why Bitcoin is Doomed*, BLOOMBERG (Aug. 8, 2013, 11:11 AM), <http://www.bloomberg.com/news/2013-08-08/did-the-sec-just-validate-bitcoin-no-.html>.

164 See U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 138, at 17 (noting that low-cost steps might be available to mitigate tax avoidance).

165 See EUROPEAN CENT. BANK, VIRTUAL CURRENCY SCHEMES 43 (2012), available at <http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> (“In the particular case of Bitcoin, which is a decentralised peer-to-peer virtual currency scheme, there is not even a central point of access, i.e. there is no server that could be shut down if the authorities deemed it necessary.”).

166 See *Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Illicit Activity*, FEDERAL BUREAU OF INVESTIGATION DIRECTORATE OF INTELLIGENCE (Apr. 24, 2012), <http://cryptome.org/2012/05/fbi-bitcoin.pdf> (“Although Bitcoin does not have a centralized authority, the FBI assesses with medium confidence that law enforcement can discover more information about, and in some cases identify, malicious actors, if the actors convert their Bitcoins into a fiat currency. Third-party Bitcoin services may require customers to submit valid identification or bank information to complete transactions.”).

167 See Kashmir Hill, *Every Important Person in Bitcoin Just Got Subpoenaed by New York's Financial Regulator*, FORBES (Aug. 12, 2013), <http://www.forbes.com/sites/kashmirhill/2013/08/12/every-important-person-in-bitcoin-just-got-subpoenaed-by-new-yorks-financial-regulator/> (“Things are getting serious for Bitcoin this month: a federal judge declared it real money, Bloomberg gave it an experimental ticker (XBT), and New York's financial regulator announced an interest in regulating it.”).

168 See Greg Farrell, *N.Y. Subpoenas Bitcoin Firms in Probe on Criminal Risk*, BLOOMBERG (Aug. 12, 2013, 2:27 PM), <http://www.bloomberg.com/news/2013-08-12/n-y-regulator-subpoenas-firms-over-bitcoin-crime-risks.html>.

169 Notice, Lawsky, *supra* note 25.

tailored regulatory guidelines are needed for virtual currencies¹⁷⁰ rather than attempting to apply existing money transmission guidelines to new technology.¹⁷¹

Attorney General Holder announced that after a lengthy review of its law enforcement policies DOJ is focusing on efforts to maximize diminishing resources by focusing on protecting national security and fighting against financial crime, and directing U.S. Attorneys to develop specific guidelines for determining when federal charges should be filed.¹⁷² New black marketplaces¹⁷³ on the dark web are being launched in place of Silk Road on a regular basis.¹⁷⁴ The FBI and DEA have proven that thorough coordination within DOJ can protect the public from ongoing internet threats by applying new and old investigatory techniques despite the anonymity provided by Bitcoin and Tor.¹⁷⁵ U.S. Attorneys have additionally raised the stakes for suspected illegal dark website owners and users by pressing strict charges against identifiable criminals, who can face massive fines and jail time for trafficking, money laundering, tax evasion, and even terrorist financing.¹⁷⁶

Treasury laid the groundwork for DOJ by issuing the first federal guidance for decentralized virtual currencies.¹⁷⁷ FinCEN took the unprecedented step of applying USA PATRIOT Act § 311 to a flagrant violator of money laundering laws, completely isolating a virtual currency exchange from the global market and allowing for the seizure of its criminal proceeds.¹⁷⁸ In the long-run, FinCEN's actions will widen the gap between legitimate uses and illegal applications of Bitcoin, which in turn may lead legislators to appreciate the promises of decentralized virtual currencies.

On the international stage, the German Ministry of Finance classified Bitcoin as a financial instrument, legalizing its use for the trade of commodities and stocks in the market.¹⁷⁹ This results in a traceable, verifiable exchange that can also be taxed.¹⁸⁰ On the other side of the spectrum, the Central Bank of Thailand has entirely banned the trade of Bitcoins based on the reasoning that no existing Thai laws allow for the regulation of virtual currency¹⁸¹ and cryptocurrencies “straddle mul-

170 *Id.*

171 *Id.*

172 *Attorney General Eric Holder Delivers Remarks at the Annual Meeting of the American Bar Association's House of Delegates*, U.S. DEP'T OF JUSTICE (Aug. 12, 2013), <http://www.justice.gov/iso/opa/ag/speeches/2013/ag-speech-130812.html>.

173 Alex Hern, *Silk Road Replacement Black Market Reloaded Briefly Closed*, THE GUARDIAN (Oct. 18, 2013, 6:24 AM), <http://www.theguardian.com/technology/2013/oct/18/silk-road-black-market-reloaded-closed>

174 Samuel Gibbs, *Silk Road Underground Market Closed – But Others Will Replace It*, THE GUARDIAN (Oct. 3, 2013, 10:24 AM).

175 *See* Complaint ¶ 13, *United States v. Ulbricht*, No. 13 MAG 02328, 2013 WL 5460023 (S.D.N.Y. Sept. 27, 2013) (attesting that the FBI worked closely with DEA, the IRS, and DHS in this investigation).

176 *See* Press Release, U.S. Dep't of the Treasury, *supra* note 126 (noting that the indictment fell under the umbrella of the PATRIOT Act); *see also* Complaint ¶¶ 1-45, *Ulbricht*, 2013 WL 5460023 (No. 13 MAG 02328).

177 *See supra* notes 28–31 and accompanying text (noting that FinCEN was founded in 1990 to monitor the financial trails left behind by criminals).

178 *See supra* notes 125–135 and accompanying text.

179 *See* Kyle Chaka, *Why Bitcoin Regulation Isn't a Crackdown*, PACIFIC STANDARD (Sept. 20, 2013), <http://www.psmag.com/business-economics/bitcoin-regulation-isnt-crackdown-66570/>.

180 *See Germany Recognizes Bitcoin as 'Private Money'*, RUSSIA TODAY (Aug. 18, 2013, 6:13PM), <http://rt.com/news/bitcoin-germany-recognize-currency-641/> (“Berlin has acknowledged the virtual tender as a “currency unit” and “private money,” according to German newspaper Die Welt. The classification means that some commercial profits on Bitcoin related endeavors may be taxable, but personal use of the currency will remain tax-free, the paper reported.”).

181 *See Trading Suspended Due to Bank of Thailand Advisement*, BITCOIN CO. LTD. (July 29, 2013), <https://bitcoin.co.th/>

multiple financial facets.”¹⁸² Unlike Germany, Thai authorities’ refusal to legislate this emerging technology may deprive their economy of taxable revenue, and will likely not prevent the use of Bitcoin by individuals as seen in Iran.

Treasury could follow Germany’s lead by creating an environment where virtual transactions are taxed and traced to law-abiding users.¹⁸³ If Treasury and Congress can determine an effective method of applying the BSA to Bitcoin without over-relying on third-party verification, national security agencies will also gain a source of intelligence to prevent financial crime as is part of FATCA’s legislative intent.

V. CONCLUSION

The key to establishing a balance between the risks and benefits of decentralized virtual currency use is further interagency cooperation on combating digital crime and simultaneously establishing clear jurisdictional lines and guidance for the virtual currency industry.¹⁸⁴ The time may be ripe for further congressional consideration of legislating this issue in HSGAC and relevant committees.¹⁸⁵ The infamous Silk Road case should serve as a reminder to both legislators and regulators of what occurs when a new technology is not quickly realized as a potential national security and economic threat to the American people.¹⁸⁶ Until regulators and law enforcement determine their legal powers in monitoring the use of virtual currencies, it is critical that agencies with specialized knowledge of the market step up to the task of protecting the nation’s security and promoting its economic interests.¹⁸⁷

trading-suspended-due-to-bank-of-thailand-advisement/ (“Based on such a broad and encompassing advisement, Bitcoin Co. Ltd. therefore has no choice but to suspend operations until such as time that the laws in Thailand are updated to account for the existance of Bitcoin. The Bank of Thailand has said they will further consider the issue, but did not give any specific timeline.”).

182 See Olivia Solon, *Thai Central Bank Rules Bitcoin to be Illegal*, WIRED UK (July 28, 2013), <http://www.wired.co.uk/news/archive/2013-07/29/bitcoin-illegal-in-thailand>.

183 See Chaka, *supra* note 179 (recognizing the benefits that Germany reaps by allowing, and taxing, Bitcoins).

184 See *supra* notes 116–147 and accompanying text (describing how DOJ and Treasury can and do work hand-in-hand to combat new cyber- and financial crime threats using their specialized knowledge of the virtual currency market).

185 See *supra* Part IV (stating that Congress has yet to take concrete legislative steps towards instituting a clear regulatory framework for decentralized virtual currencies, although progress has been signified by hearings from industry, academic, and law enforcement leaders held in the summer of 2013).

186 See *supra* Part III (explaining that millions of illicit virtual currency transactions in a variety of criminal activities can quickly become a national security and welfare threat if left unchecked without regulation, as demonstrated by Silk Road’s allegedly extensive use in the Bitcoin market).

187 See *supra* notes 15, 49, 122 and accompanying text (demonstrating DOJ, Treasury, and DHS’ particular effectiveness in taking down the websites and seizing the assets of illegal users, administrators, and exchangers of decentralized virtual currencies).



The National Security Law Brief
Washington College of Law
American University
4801 Massachusetts Avenue NW
Washington DC 20016



The American University National Security Law Brief welcomes submissions on relevant national security law topics at all times. To send a submission or request information on submission guidelines, please email submissions@nationalsecuritylawbrief.com.

Opinions expressed in issues of the National Security Law Brief represent only the views of the author; they do not represent the views of American University Washington College of Law or the views of members of the National Security Law Brief. Copyright © 2012 by the Am. U. Nat'l Security Law Brief. All Rights Reserved. No part of this publication may be reproduced without the express written consent of the copyright owner. Requests should be sent via email to info@nationalsecuritylawbrief.com.