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

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

JARED A. KLEIMAN

“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) Aide

INTRODUCTION

As pseudonymous Bitcoin programmer Satoshi Nakamoto prepares to celebrate his creation’s fifth-anniversary in 2014, 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.


4 See Maria Santos, Sato’s Outpost Invited You to Celebrate Bitcoin’s Fifth Birthday, BITCOIN EXAMINEr (Oct. 12, 2013), http://bitcoineaminer.org/seans-outpost-invites-you-to-celebrate-bitcoins-fifth-birthday/


6 What is a Remittance Transfer, CONSUMER FED. PROT. BUREAU (Aug. 2, 2013), http://www.consumerfinance.gov/about gc/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”).


10 Id.


12 See Amrutha Guappan, From Marijuana to LSD, Now Illegal Drugs Delivered by your Doorstep, EATON'S BUS. TIMES (Jun. 11, 2011, 1:31 AM), http://www.eatonsbusiness.com/marijuana-had-now-illegal-drugs-delivered-your-doorstop-298921 (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 BLOG, http://motherboard .vice.com/blog/traveling-down-the-silk-road-to-buy-drugs-with-bitcoins (June 18, 2013, 18:13), (explaining that Silk Road makes its user’s IP address by routing their query through a different IP address and allowing a user to access anions sites that make up the “Deep Web”).

14 guns to hacking tools. 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. 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.

16 Authorities have strained to fit Bitcoin and similar platforms into existing legal buckets that are decades old. 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.

17 At the same time, regulators face vocal proponents of systems like Bitcoin who argue their valid use for political, philosophical, and financial reasons. Advocacy groups, led by the Bitcoin Foundation, 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), but have expressed fears of excessive regulatory measures in the United States.


20 See Warmbier, supra note 2 (arguing that regulators need to act soon to control risks imposed by these markets, including the risk of later overregulating).
peer-to-peer cryptocurrency, is a remittance tool with a market capitalization of over $1.7 billion as of October 2013. Bitcoin represents an emerging platform with unprecedented benefits, from low-cost international transfers to completely private charitable donations and complex investment trusts. These same qualities allow criminal enterprises to potentially circumvent law enforcement and evade taxes; establishing clear dangers to U.S. national security and welfare. The infamous dark website, Silk Road, exemplifies the regulatory riddle unique to a decentralized virtual currency marketplace made up of administrators, sellers, and buyers contributing to an Amazon.com of illegal goods fuelled by Bitcoin transactions. Launched in February 2011 and accessible only through the anonymizing internet browser, The Onion Router (Tor), Silk Road facilitated the trade of an estimated $1.2 billion worth of illicit goods ranging from heroin and handguns to hacking tools. The website’s assets and alleged owner clandestinely operated for over two years before a multi-agency task force seized both in October 2013. 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. 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. Agencies have strained to fit Bitcoin and similar platforms into existing legal buckets that are decades old. 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. 

At the same time, regulators face vocal proponents of systems like Bitcoin who argue their valid use for political, philosophical, and financial reasons. Advocacy groups, led by the Bitcoin Foundation, 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), but have expressed fears of excessive regulatory measures in the United States.


6 What is a Remittance Transfer, CONSUMER FED. PROT. BUREAU (Aug. 2, 2013), http://www.consumerfinance.gov/askcfp/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”).


8 See Andrea Castillo, Bitcoins Underserved and overestimated risks, THE HILL’S CONGRESS BLOG (Aug. 23, 2013, 11:00 AM), http://thehill.com/blogs/congress-blog/technology/317875-bitcoin-underserved-benefits-and-overestimated-risks (explaining that Bitcoin has many benefits, such as lowering transaction costs); see also Syria Herbas-Byluk, 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-idUSB9G8X2320130917 (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).


10 Id.


13 See Ryan Broderick, Traveling Down the Silk Road to Buy Drugs with Bitcoins, MOTHERBOARD BLOG, http://motherboard.vice.com/traveling-down-the-silk-road-to-buy-drugs-with-bitcoins (last updated Oct. 18, 2013) (explaining that Silk Road masks a user’s IP address by routing their query through a different IP address and allowing a user to access online sites that make up the “Deep Web”).
and abroad stifling the currency's growth. Proponents of virtual currency claim it represents an "essential privacy-preserving technology." 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." 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." 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.

FinCEN was founded in 1990 to support all levels of government by monitoring financial trails left behind by criminals. FinCEN is tasked with "analyzing and disseminating [financial transactions data] for law enforcement purposes" 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. Together, these Acts constitute the current BSA of 1970, the "first and most-comprehensive" federal anti-money laundering and counterterrorism financing statute. 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." Bitcoin has no managing authority and is not a legal tender in any nation. 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. 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." 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." 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. 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

---

31 See What's New, supra note 29.
34 See FIN. CRIMES ENFORCEMENT NETWORK, supra note 33.
35 Id.
and abroad stifling the currency's growth. Proponents of virtual currency claim it represents an "essential privacy-preserving technology." 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." 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 explores 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." 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.

FinCEN was founded in 1990 to support all levels of government by monitoring financial trails and enforcing anti-money laundering and counterterrorism financing statute.

A. Virtual Currency

Real currency is "legal tender . . . that circulates and is customarily used and accepted as a medium of exchange." Bitcoin has no managing authority and is not a legal tender in any nation. 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. 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." 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." 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.

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 left behind by criminals. FinCEN is tasked with "analyzing and disseminating [financial transactions data] for law enforcement purposes" 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. Together, these Acts constitute the current BSA of 1970, the "first and most-comprehensive" federal anti-money laundering and counterterrorism financing statute. Its findings on virtual currency provide a good starting point for understanding the basics of Bitcoin.

31 See What It's Do, supra note 29.
32 31 C.F.R. § 1010.100(q) (2011).
34 See FIN. CRIMES ENFORCEMENT NETWORK, supra note 33.
35 Id.
36 Id.
37 See WILMERHALE, FINTECH WEBINAR SERIES: BITCOIN AND OTHER VIRTUAL CURRENCIES (2015), 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.\textsuperscript{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.\textsuperscript{39} FinCEN distinguishes “users,” “exchangers,” and “administrators” of virtual currencies in the same guidance.\textsuperscript{40} Users “obtain virtual currency to purchase goods or services.”\textsuperscript{41} Exchangers are “engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency;”\textsuperscript{42} and administrators are “engaged as a business in issuing virtual currency, and [have] the authority to redeem such virtual currency;”\textsuperscript{43} thus providing money transmission services. Those providing money transmission services must maintain transaction records under the BSA.\textsuperscript{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.\textsuperscript{45}

The courts have jurisdiction in the virtual currency realm as well. In \textit{SEC v. Shavers},\textsuperscript{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.\textsuperscript{47} Because it was clear that Bitcoins can be used as money,\textsuperscript{48} the Securities and Exchange Commission could try input, but remain silent on whether current law fits the technology or if they will enact different regulatory schemes.\textsuperscript{49} The Bitcoin monetary supply is created by the amount of users who utilize the platform, releasing quantities in a block chain.\textsuperscript{50} 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.\textsuperscript{51} 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.\textsuperscript{52} By solving this progressive puzzle, the program

\begin{itemize}
    \item source for currency, funds, or another substitute for currency.
    \item 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. FinCEN distinguishes “users,” “exchangers,” and “administrators” of virtual currencies in the same guidance. Users “obtain virtual currency to purchase goods or services.” Exchangers are “engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency;” and administrators are “engaged as a business in issuing virtual currency, and [have] the authority to redeem such virtual currency;” thus providing money transmission services. Those providing money transmission services must maintain transaction records under the BSA. 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.
    \item The courts have jurisdiction in the virtual currency realm as well. In \textit{SEC v. Shavers}, 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. Because it was clear that Bitcoins can be used as money, the Securities and Exchange Commission could try input, but remain silent on whether current law fits the technology or if they will enact different regulatory schemes.

\end{itemize}
source for currency, funds, or another substitute for currency. 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. FinCEN distinguishes “users,” “exchangers,” and “administrators” of virtual currencies in the same guidance. Users “obtain virtual currency to purchase goods or services.” Exchangers are “engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency,” and administrators are “engaged as a business in issuing virtual currency, and [have] the authority to redeem such virtual currency,” thus providing money transmission services. Those providing money transmission services must maintain transaction records under the BSA. 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.

The courts have jurisdiction in the virtual currency realm as well. In SEC v. Shavers, 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. Because it found that the defendant’s investments constituted securities under 15 U.S.C. § 77(b) and that “it [was] clear that [Bitcoins] can be used as money,” the Securities and Exchange Commission could proceed with its case.

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. Since a court deemed Bitcoins to be a security instrument, lawmakers on the federal and state level have aligned their focus on virtual currency for real currency, funds, or other virtual currency, and administrators are “engaged as a business in issuing virtual currency, and [have] the authority to redeem such virtual currency,” thus providing money transmission services. Those providing money transmission services must maintain transaction records under the BSA. 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.

The courts have jurisdiction in the virtual currency realm as well. In SEC v. Shavers, 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. Because it found that the defendant’s investments constituted securities under 15 U.S.C. § 77(b) and that “it [was] clear that [Bitcoins] can be used as money,” the Securities and Exchange Commission could proceed with its case.

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. Since a court deemed Bitcoins to be a security instrument, lawmakers on the federal and state level have aligned their focus on virtual currency for real currency, funds, or other virtual currency, and administrators are “engaged as a business in issuing virtual currency, and [have] the authority to redeem such virtual currency,” thus providing money transmission services. Those providing money transmission services must maintain transaction records under the BSA. 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.

The courts have jurisdiction in the virtual currency realm as well. In SEC v. Shavers, 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. Because it found that the defendant’s investments constituted securities under 15 U.S.C. § 77(b) and that “it [was] clear that [Bitcoins] can be used as money,” the Securities and Exchange Commission could proceed with its case.

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. Since a court deemed Bitcoins to be a security instrument, lawmakers on the federal and state level have aligned their focus on virtual currency for real currency, funds, or other virtual currency, and administrators are “engaged as a business in issuing virtual currency, and [have] the authority to redeem such virtual currency,” thus providing money transmission services. Those providing money transmission services must maintain transaction records under the BSA. 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.

The courts have jurisdiction in the virtual currency realm as well. In SEC v. Shavers, 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. Because it found that the defendant’s investments constituted securities under 15 U.S.C. § 77(b) and that “it [was] clear that [Bitcoins] can be used as money,” the Securities and Exchange Commission could proceed with its case.

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. Since a court deemed Bitcoins to be a security instrument, lawmakers on the federal and state level have aligned their focus on virtual currency for real currency, funds, or other virtual currency, and administrators are “engaged as a business in issuing virtual currency, and [have] the authority to redeem such virtual currency,” thus providing money transmission services. Those providing money transmission services must maintain transaction records under the BSA. 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.

The courts have jurisdiction in the virtual currency realm as well. In SEC v. Shavers, 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. Because it found that the defendant’s investments constituted securities under 15 U.S.C. § 77(b) and that “it [was] clear that [Bitcoins] can be used as money,” the Securities and Exchange Commission could proceed with its case.

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. Since a court deemed Bitcoins to be a security instrument, lawmakers on the federal and state level have aligned their focus on virtual currency for real currency, funds, or other virtual currency, and administrators are “engaged as a business in issuing virtual currency, and [have] the authority to redeem such virtual currency,” thus providing money transmission services. Those providing money transmission services must maintain transaction records under the BSA. 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.

The courts have jurisdiction in the virtual currency realm as well. In SEC v. Shavers, 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. Because it found that the defendant’s investments constituted securities under 15 U.S.C. § 77(b) and that “it [was] clear that [Bitcoins] can be used as money,” the Securities and Exchange Commission could proceed with its case.

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. Since a court deemed Bitcoins to be a security instrument, lawmakers on the federal and state level have aligned their focus on virtual currency for real currency, funds, or other virtual currency, and administrators are “engaged as a business in issuing virtual currency, and [have] the authority to redeem such virtual currency,” thus providing money transmission services. Those providing money transmission services must maintain transaction records under the BSA. 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.

The courts have jurisdiction in the virtual currency realm as well. In SEC v. Shavers, 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. Because it found that the defendant’s investments constituted securities under 15 U.S.C. § 77(b) and that “it [was] clear that [Bitcoins] can be used as money,” the Securities and Exchange Commission could proceed with its case.

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. Since a court deemed Bitcoins to be a security instrument, lawmakers on the federal and state level have aligned their focus on virtual currency for real currency, funds, or other virtual currency, and administrators are “engaged as a business in issuing virtual currency, and [have] the authority to redeem such virtual currency,” thus providing money transmission services. Those providing money transmission services must maintain transaction records under the BSA. 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.

The courts have jurisdiction in the virtual currency realm as well. In SEC v. Shavers, 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. Because it found that the defendant’s investments constituted securities under 15 U.S.C. § 77(b) and that “it [was] clear that [Bitcoins] can be used as money,” the Securities and Exchange Commission could proceed with its case.

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. Since a court deemed Bitcoins to be a security instrument, lawmakers on the federal and state level have aligned their focus on virtual currency for real currency, funds, or other virtual currency, and administrators are “engaged as a business in issuing virtual currency, and [have] the authority to redeem such virtual currency,” thus providing money transmission services. Those providing money transmission services must maintain transaction records under the BSA. 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.

The courts have jurisdiction in the virtual currency realm as well. In SEC v. Shavers, 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. Because it found that the defendant’s investments constituted securities under 15 U.S.C. § 77(b) and that “it [was] clear that [Bitcoins] can be used as money,” the Securities and Exchange Commission could proceed with its case.

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. Since a court deemed Bitcoins to be a security instrument, lawmakers on the federal and state level have aligned their focus on virtual currency for real currency, funds, or other virtual currency, and administrators are “engaged as a business in issuing virtual currency, and [have] the authority to redeem such virtual currency,” thus providing money transmission services. Those providing money transmission services must maintain transaction records under the BSA. 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.
proves each peer-to-peer link is legitimate. Miners are rewarded with Bitcoins after creating a block chain and when further transactions are added to the miner’s block chain. After Bitcoins are traded by users, another equation for decryption is added to the block chain. Bitcoin transactions are verified through a two-part cryptographic process. A seller creates a virtual message containing a buyer’s public key and signs it with the seller’s private key. The timestamped transfer is recorded on the block chain. 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. 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.

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

C. Tor

Tor was developed to be a “tool for free expression, privacy, and human rights.” It anonymizes users’ internet protocol (IP) addresses by redirecting the original query through exit relays that can be located anywhere in the world. Originally sponsored by the Naval Research Laboratory, 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. Up until October 2012, the BBG directly funded Tor through this Division.

Tor has also caused headaches for American investigators seeking to seize webhosts of illicit materials and to identify uploaders and downloaders. By working with internet service providers after identifying an IP address, law enforcement can determine a user’s physical location. Tor inhibits this ability by cloaking the source of an IP query. 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. Since properly-configured relays provide little useful data for investigators, exploiting information transmitted through Tor remains a priority for agencies including the Federal Bureau of Investigation (FBI) and National Security Agency (NSA). 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.”

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/schneier/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/overviewhtml.htm (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), https://theatlantic.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, BROADCAST BOARD OF GOVERNORS, http://www.bloggings/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 Van, FBI Claims That Tor Spyming Child Abuse Investigation, NAKED SECURITY, June 14, 2012, http://nakedsecurity.sophos.com/2012/06/14/us-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.”).
proves each peer-to-peer link is legitimate. Miners are rewarded with Bitcoins after creating a block chain and when further transactions are added to the miner’s block chain. After Bitcoins are traded by users, another equation for decryption is added to the block chain.

Bitcoins transactions are verified through a two-part cryptographic process. A seller creates a virtual message containing a buyer’s public key and signs it with the seller’s private key. The time-stamped transfer is recorded on the block chain. 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. 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 confidentially verified.

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

C. Tor

Tor was developed to be a “tool for free expression, privacy, and human rights.” It anonymizes users’ internet protocol (IP) addresses by redirecting the original query through exit relays that can be located anywhere in the world. Originally sponsored by the Naval Research Laboratory, 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. Up until October 2012, the BBG directly funded Tor through this Division.

Tor has also caused headaches for American investigators seeking to seize webhosts of illicit materials and to identify uploaders and downloaders. By working with internet service providers after identifying an IP address, law enforcement can determine a user’s physical location. Tor inhibits this ability by cloaking the source of an IP query. 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. Since properly-configured relays provide little useful data for investigators, exploiting information transmitted through Tor remains a priority for agencies including the Federal Bureau of Investigation (FBI) and National Security Agency (NSA). 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/sched/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.thetorproject.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://theatlantic.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, BROADCAST BOARD OF GOVERNORS, http://www.bbgi.org/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 Yuan, FBI Claims That Tor Shielded Child Abuse Investigation, NAKED SECURITY (June 14, 2012), http://nakedsecurity.sophos.com/2012/06/14/this-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.”).
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.” Four 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. 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.89 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. The website further advised sellers on shipping methods to avoid detection.86 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.87

The Senators’ letter recommended that the DOJ request a court to order the seizure of the website’s domain name.88 Silk Road, however, operated on the Tor network, which adds randomly generated characters to the actual domain name.89 An internet user could find the current Tor address by typing “*.onion” into their browser.90

After the fall of Silk Road, investigators continue to use manual analysis as a means to achieve de-anonymization.91 For example, on October 5, 2013, investigative officials from the Department of Justice (DOJ), Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), and Treasury Internal Revenue Service (IRS) launched a major international operation against the leading cannabinoid marketplace on the Internet today.92

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.”93 It took over two years for law enforcement agents from the DOJ, FBI, DEA, HHS, Homeland Security Investigations, and Treasury Internal Revenue Service (IRS) to investigate 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 1956.94 It was the improper implementation of Tor by the site’s intended owner that granted the task force the opportunity to match his IP address to old forum posts and execute an arrest.95 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.96

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)97 request to an unconfirmed sovereign allowed the FBI to copy a Silk Road server on July 23, 2013.98 Icelandic enforcement confirmed their assistance to U.S. authorities and their confiscation of a server and three dress posted by Silk Road users on forums.99 Silk Road’s servers were also hosted in several foreign countries.100 By employing a “tumbler”101 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.102

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

3. See Andrew Coston, 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 supermarkety 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.”).


5. Parker Higgins, Why You Can’t Blame Bitcoin for Silk Road Shadiness, GIZOMOD (Oct. 5, 2013, 5:00PM), http://gizmodo.com/why-you-can’t-blame-bitcoin-for-silk-roads-shadiness-1441572563 (“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.”).


7. Id.


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 characters 91 to the actual domain name. 92 An internet user could find the current Tor ad

83 See Lisa Vaas, FBI Claims that Tor Spied on Child Abuse Investigation, NAKED SECURITY (June 14, 2012), http://nakedsecurity.sophos.com/2012/06/14/the-tor-child-abuse-investigation/
86 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 take down of a billion-dollar black market website that allows 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.”).
87 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.”).
91 See Complaint ¶ 12(b), United States v. Ulbricht, No. 13 MAG 02328, 2013 WL 5460023 (SD.N.Y. Sept. 27, 2013) (claiming that defendant added a Bitcoin tumbler to Silk Road to make the illegal transactions untraceable).
92 See Andrew Cotsen, 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 supermarkets 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.”).
93 See Complaint ¶ 22, Ulbricht, 2013 WL 5460023 (No. 13 MAG 02328).
94 See Parker Higgins, Why You Can’t Blame Bitcoins for Silk Road Shutdown, GIZMODO (Oct. 5, 2013, 5:00PM), http://gizmodo.com/why-you-cant-blame-bitcoins-for-silk-road-shutdown-1441572636 (“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.”).
95 See id. ¶ 28; id. ¶ 22, 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 sets of dummy transactions... making it nearly impossible to link your payment with any coins left sitting in the block.”).
96 See id. ¶ 16, Ulbricht, 2013 WL 5460023 (No. 13 MAG 02328).
97 See id. ¶ 28; see also id. ¶ 16, 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 sets of dummy transactions... making it nearly impossible to link your payment with any coins left sitting in the block.”).
100 See id. ¶ 28; see also id. ¶ 16, 18 U.S.C. § 1028 (2006) (defining the crime and penalties related to false identification possession and trafficking).
102 See Complaint ¶ 22, Ulbricht, 2013 WL 5460023 (No. 13 MAG 02328).
million Bitcoins,105 but Iceland is not a signatory to any MLAT.106 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.107 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 tumblers used, delaying the identification of buyers and sellers of illegal materials and liquidation of criminal proceeds.108

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 . . . threatens . . . 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 "[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 Notice 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 value" under 28 C.F.R. § 8.11 (2014). Bitcoins are subject to extreme fluctuations in value,117 dropping twenty percent in only three hours after Silk Road shut down a few weeks after the DEA operation.118

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 illegitimately-operated virtual currency exchangers from the U.S. economy.119

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.120 In exchange for depositing dollars with a pay-mention processor based in Iowa, Mr. Gox would disburse Bitcoins to users and register transactions in "Bitcoin After Silk Road"


See Strategic Financial Crimes, 2012 Annual Report, supra note 77


Ibid. See § 311 (allowing 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 illegitimately-operated virtual currency exchangers from the U.S. economy.119 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.120 In exchange for depositing dollars with a pay-mention processor based in Iowa, Mr. Gox would disburse Bitcoins to users and register transactions in...
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

105 See Jeffries, supra note 103 (“While the country may have protected Wálí’s leaks from the Americans, it’s not harboring the recently busted illegal drug bazaar Silk Road?”); see also Complaint ¶ 19, Ubridge, 2013 WL 5460023, (No. 13 MAG 02328) (describing that the “Blockchain” was a public ledger stored on peer-to-peer networks).
106 See Omar Dieh, Bitcoin: After Silk Road, THE STANFORD DAILY (Oct. 12, 2013), http://stanforddaily.com/2013/10/12/bitcoin-after-silk-road/ (“In order to obscure the flow of Bitcoin, people often run Bitcoins through Tor 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, But Heroin, Cocaine, Drug Trafficking, ABC ACTION NEWS (June 10, 2013), http://abcactionnews.com/dpp/news/local_news/investigations/silk-road-website-called-the-amazon-ebay-of-heroin-coke-dope-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 Brita & Castells, 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.”).
111 Notice, Lawsuit, supra note 25.
a central database; it did not however sign mandatory FinCEN forms declaring the subsidiary to be an exchanger. On May 28, 2013 the federal government went a step further when U.S. Attorney Preet Bharara announced the indictment of the then-popular virtual currency exchange Liberty Reserve, which actively hid its register of users’ activities. 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” 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, a first for a virtual currency exchange case. 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. Bharara called the company a “hub for fraudsters, hackers, and traffickers” after an investigation spanning seventeen countries.

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.

Threats to the national welfare are deeply entwined with threats to national security. The Foreign Account Tax Compliance Act of 2010 (“FATCA”) is intended to combat offshore tax evasion, which is estimated to account for $150 billion of lost revenue each year. 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.

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. 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. By doing so, it is possible that criminals along with tax evaders can slip through the cracks of FATCA, not only preventing the IRS from generating revenue but also depriving security agencies of a valuable source of intelligence on crime and terror activity.

Combating terrorism by interpreting bank documents remains a priority for security communities combating crimes other than tax evasion.

Interceptor: The effort to require financial institutions to share customers’ account information as non-tax return information to ensure its accessibility to law enforcement and national security communities combating crimes other than tax evasion.

How the IRS Can Share Your Bank Info with Security Agencies

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 recoupment needed tax revenues.")
a central database; it did not however sign mandatory FinCEN forms declaring the subsidiary to be an exchanger. On May 28, 2013 the federal government went a step further when U.S. Attorney Preet Bharara announced the indictment of the then-popular virtual currency exchange Liberty Reserve, which actively hid its register of users’ activities. 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” 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, a first for a virtual currency exchange case. 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. Bharara called the company a “hub for fraudsters, hackers, and traffickers” after an investigation spanning seventeen countries. 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. Threats to the national welfare are deeply intertwined with threats to national security. The Foreign Account Tax Compliance Act of 2010 (“FATCA”) is intended to combat offshore tax evasion, which is estimated to account for $150 billion of lost revenue each year. FATCA § 6103 permits “disclosure of [income tax] return information to appraise 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. 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. 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. By doing so, it is possible that criminals along with tax evaders can slip through the cracks of FATCA, not only preventing the IRS from generating revenue but also depriving security agencies of a valuable source of intelligence on crime and terror activity. Combating terrorism by interpreting bank documents remains a priority for 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.”


127 See Colan, 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 included Costa Rica, the Netherlands, Spain, Morocco, Sweden, Switzerland, Cyprus, Australia, China, Norway, Latvia, Luxembourg, the United Kingdom, Russia, and Canada, and the United States. Id.

130 Id.


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.”)


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 Douglas 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 Freid & Zachary Warmbrod, Bitwise Tax Haven of its Future, POLITICO (Aug. 10, 2013, 6:54PM), 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.”).


138 See U.S. GOVERNMENT ACCOUNTABILITY OFFICE, GAO-13-516: VIRTUAL ECOCNOMIES AND CURRENCIES: ADDITIONAL IRS Guidance Could Reduce Tax Compliance Risks Highlights of GAO-13-516, available at http://i2e.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 Mark 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-with (“Title 26, Section 6103 of the tax
the U.S. intelligence community, which FACTA Intergovernmental Agreements abroad intend to remedy at lower risk and cost to the public than covert action. 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. 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.” 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. These anonymous financial transfers hinder the government’s ability to detect illicit financing. Bitcoin mining software exportation is restricted by the Department of Commerce Bureau of Industry and Security due to its encryption capabilities, but sanctioned nations have discovered methods to obtain the virtual currency through e-commerce. Iranians, for example, have avoided Treasury Office of Foreign Assets Control sanctions and the effects of inflation by swapping Bitcoins for normally unobtainable U.S. dollars and keeping

code opens doors that allow U.S. 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 Alex Mostow & Ian Cobain, CIA’s Secret UK Bank Trawl May Be Illegal, THE GUARDIAN (Aug. 20, 2006), http://www.theguardian.com/sik/2006/aug/21/business.currentaccounts (acknowledging that the agency has received financial records from the Belgian co-operative that processes money transfers from banks around the world, a program that was initiated after September 11, 2001, and had included details of an estimated 4.6 million British banking transactions).

141 See also Takedown the Money: NX-Asia On International Payments, DR. SPEELER (Sep. 16, 2013) (describing the SNA’s “own financial databank” called Tracfin).


144 See BRTIN & CASTELLA, 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.”).


146 Id.

147 See Eysen, supra note 142 (stating law enforcement’s interests in detecting illicit financing).


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


152 Their holdings outside of the country.

153 India 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.

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 desire increased scrutiny due to possible risks to national security. In August 2013, the HSGAC began an inquiry into emerging virtual currency technology seeking a whole-government approach to understand the market, and to provide a practical framework for their regulation. Regulators and law enforcement are reportedly “worried virtual currency markets could be used for money laundering and tax avoidance,” 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. 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.” The Chief Executive of Coinsetter, a virtual currency firm, stated that “regulatory uncertainty right now is the bottleneck for innovation in this space.”

This interest has resulted, so far, in no concrete action. Multiple Executive agencies are instead “mulling” 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 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. Vice Chairwoman Janet Yellen


155 See Morgan Tank, Regulatory Alert: Emerging Payment Providers Can Learn from Liberty Reserve and Mt. Gox, PAYMENTS JOURNAL (July 2, 2013), http://www.paymentjournal.com/Content/Blogs/Industry_Blog/16092/ (commenting that financial regulators are looking at Bitcoins to determine whether it undermines the current protections on the financial system).


157 Id.

158 Id.


161 Id.
the U.S. intelligence community, which FACTA Intergovernmental Agreements abroad intend to remedy at lower risk and cost to the public than covert action. 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. 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.” 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. These anonymous financial transfers hinder the government’s ability to detect illicit financing. Bitcoin mining software exportation is restricted by the Department of Commerce Bureau of Industry and Security due to its encryption capabilities, but sanctioned nations have discovered methods to obtain the virtual currency through e-commerce. For example, Iranians, have avoided Treasury Office of Foreign Assets Control sanctions and the effects of inflation by swapping Bitcoins for normally unobtainable U.S. dollars and keeping their holdings outside of the country. 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.

The federal government has become increasingly aware that virtual currencies like Bitcoin represent a promising technology, but they also desire increased scrutiny due to possible risks to national security. In August 2013, the HSGAC began an inquiry into emerging virtual currency technology seeking a whole-government approach to understand the market, and to provide a practical framework for their regulation. Regulators and law enforcement are reportedly “worried virtual currency markets could be used for money laundering and tax avoidance,” even though block chain transactions are public. 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. 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.” The Chief Executive of Cointsetter, a virtual currency firm, stated that “regulatory uncertainty right now is the bottleneck for innovation in this space.”

This interest has resulted, so far, in no concrete action. Multiple Executive agencies are instead “mulling” 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. Vice Chairwoman Janet Yellen

---

144 FBI Intelligence Assessment, supra note 142.
145 Id.
146 Id.
147 Id.
148 Id.
149 Id.
150 Id.
151 Id.
152 Id.
153 Id.
154 Id.
155 Id.
156 Id.
157 Id.
158 Id.
159 Id.
160 Id.
161 Id.
162 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 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-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 investigative 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 guideline 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. 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 currency180 and cryptocurrencies “straddle mul-

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 Central Bank, Virtual Currency Schemes 43 (2012), available at http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201211en.pdf (“In the particular case of Bitcoin, which is a decentralized peer-to-peer virtual currency scheme, there is no 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.”).
169 Notice, Lawsky, supra note 25.
170 Id.
171 Id.
175 See Complaint ¶ 13, United States v. Ulbricht, No. 13 MAG 0238, 2013 WL 5460023 (SD.NY. 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.
180 See Germany Recognizes Bitcoin as ‘Private Money’, Russia Today (Aug. 18, 2013, 6:13PM), http://russia.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’s Action, Bitcoin Co. Ltd. (July 29, 2013), https://bitcoin.co.th/
disclosed that the Federal Reserve is researching the potential negative effects of Bitcoin on the U.S. financial system. The IRS is rumored 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. The DHS, DOJ, and SEC are already in the midst of financial crime and narcotrafficking probes related to Bitcoin usage. Relying on further regulation of third-party exchanges 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. The FBI, for example, has proposed that third-party Bitcoin exchanges 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 exchanges 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 exchanges 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 states 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 companies as DFS weighs the implementation of “guardrails” to protect consumers and national security.

This information-gathering will enable DFS to determine whether newly-tailored regulatory guidelines are needed for virtual currencies rather than attempting to apply existing money transmission guidelines to new technology. 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. New black marketplaces on the dark web are being launched in place of Silk Road on a regular basis. The FBI and DEA have proven that thorough coordination within DOJ can protect the public from ongoing internet threats by applying new and old investigative techniques despite the anonymity provided by Bitcoin and Tor.

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.

Treasury laid the groundwork for DOJ by issuing the first federal guidance for decentralized virtual currencies. 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. 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. This results in a traceable, verifiable exchange that can also be taxed. 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 currency and cryptocurrencies “straddle multiple financial systems.”

tiple financial facets.” 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. 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. The time may be ripe for further congressional consideration of legislating this issue in HSGAC and relevant committees. 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. 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.

---

183 See 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 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.