Brooklyn Law Review

Volume 80 | Issue 2 Article 4

2015

Fitting a Square Peg in a Round Hole: Bitcoin, Money Laundering, and the Fifth Amendment Privilege Against Self-Incrimination

Nicholas J. Ajello

NOTES

Fitting a Square Peg in a Round Hole

BITCOIN, MONEY LAUNDERING, AND THE FIFTH AMENDMENT PRIVILEGE AGAINST SELF-INCRIMINATION

INTRODUCTION

Although money laundering is not new, the use of digital currencies to launder money is. Virtual currencies like Bitcoins, Litecoins, Liberty Reserve, Perfect Money, and WebMoney, just to name a few, have grown in popularity over the last four years.[1] None of these digital currencies has been more popular than Bitcoin. Bitcoin is a digital currency in which transactions can be completed without the need for a central bank. In a very short period of time, Bitcoin has moved from a niche currency into what some believe will soon be a mainstream currency.[2] The rapid proliferation of the currency has raised concerns among regulated businesses and the government alike that fear the insidious and socially destructive nature of money laundering.[3]

Money laundering is the process of taking "dirty money," earnings gleaned by way of illegal activity, and making the

---

[1] *See* THOMSON REUTERS FRAUD & INVESTIGATION UNIT, TECHNOLOGY IN THE FIGHT AGAINST MONEY LAUNDERING IN THE NEW DIGITAL CURRENCY AGE (2013), *available at* http://trmcs-documents.s3.amazonaws.com/cfbf4386891bc6cb7ee26f9690294222_20130617083834_AML%20White%20Paper.pdf [hereinafter REUTERS WHITE PAPER]; *see also* Emily Flitter & Brett Wolf, *Digital Currency Firms Rush to Adopt Anti-Money Laundering Rules*, REUTERS (May 31, 2012), http://www.reuters.com/article/2013/05/31/us-digitalcurrency-regulation-bitcoin-idUSBRE94U17X20130531.

[2] Dave Thier, *Why This Entrepreneur Thinks Bitcoins Are Here to Stay*, FORBES (Oct. 24, 2013, 12:08 PM), http://www.forbes.com/sites/davidthier/2013/10/24/why-this-entrepeneur-thinks-bitcoins-are-here-to-stay/.

[3] Dr. Robert Stokes, *Anti-Money Laundering Regulation and Emerging Payment Technologies*, BANKING & FIN. SERVICES POL'Y REP., May 2013, at 1.

money appear "clean" or legitimate.[4] Although not codified as a specific crime until the mid-1980s, money laundering has a much more extensive history.[5] While money laundering is technically a non-violent crime, successful money laundering and the criminal activities it buttresses can have a far reaching impact as it frequently supports illicit activities including drug trafficking and terrorism.[6] As a result, "[e]ffective anti-money laundering . . . regimes are essential to protect the integrity of markets and of the global financial framework."[7]

Although it is likely the government will avoid a prohibition of Bitcoin,[8] recent developments indicate that the United States government will attempt to regulate Bitcoin through existing anti-money laundering statutes.[9] Regardless of one's opinion on this course of action, it appears that the government's first step in thwarting digital currency money laundering will be effectively jamming the "modern square peg [of Bitcoin] . . . into round regulatory holes meant for ancient business models."[10]

To effectively regulate the inherent money laundering risks of Bitcoin, the United States government will likely need to utilize key disclosure laws.[11] These laws would require Bitcoin owners to divulge their private key, which is similar to a password and provides access to a user's bitcoins. The use of such laws may raise opposition from Bitcoin users, administrators, and exchangers, as well as challenges from privacy rights advocates who will likely argue that disclosure of private keys infringe upon

---

[4] *History of Anti-Money Laundering Laws*, FINCEN, http://www.fincen.gov/news_room/aml_history.html (last visited Feb. 14, 2015).

[5] Madelyn J. Daley, *Effectiveness of United States and International Efforts to Combat International Money Laundering*, 2000 ST. LOUIS-WARSAW TRANSATLANTIC L.J. 175, 179 (2000).

[6] Shawn Turner, Note, *U.S. Anti-Money Laundering Regulations: An Economic Approach to Cyberlaundering*, 54 CASE W. RES. L. REV. 1389, 1390 (2004).

[7] *Factsheet: The IMF and the Fight Against Money Laundering and the Financing of Terrorism*, INTERNATIONAL MONETARY FUND (Sept. 5, 2014), http://www.imf.org/external/np/exr/facts/aml [hereinafter *Factsheet*].

[8] John Aziz, *We Know How Bitcoin Prohibition Would End*, THE WEEK (Feb. 28, 2014), http://theweek.com/article/index/257120/we-know-how-bitcoin-prohibition-would-end.

[9] *See* FIN. CRIMES ENFORCEMENT NETWORK, U.S. DEP'T OF THE TREASURY, FIN-2013-G001, APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES (2013), *available at* http://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf.

[10] Marco Santori, *Bitcoin Law: What US Businesses Need to Know*, COINDESK (Aug. 17, 2013, 8:52 AM), http://www.coindesk.com/bitcoin-law-what-us-businesses-need-to-know/.

[11] Jon Matonis, *Key Disclosure Laws Can be Used to Confiscate Bitcoin Assets*, FORBES (Sept. 12, 2012), www.forbes.com/sites/jonmatonis/2012/09/12/key-disclosure-laws-can-be-used-to-confiscate-bitcoin-assets.

the Fifth Amendment right against self-incrimination.[12] This note will argue that courts will hold that the Fifth Amendment right against self-incrimination is violated through the compelled production of a Bitcoin user's private key, thus disabling the government's tool to thwart money laundering.

Part I explains Bitcoin's traits and use and how these traits increase the risk of money laundering. Part II briefly describes money laundering. Part III illustrates the steps that have been taken by regulatory bodies to control Bitcoin money laundering and the government's likely regulatory solution to Bitcoin money laundering. Finally, Part IV analyzes the collateral legal issue regarding the Fifth Amendment privilege against self-incrimination that will present itself by virtue of the implementation of compelled private key disclosure.

I. BITCOIN: TRAITS AND USAGE

Bitcoin has emerged as a buzzword illustrative of the burgeoning technology boom. Despite the increased prevalence of the currency in the news and on blogs, the masses are largely naïve as to how the currency works. Bitcoin's complex design, the inherent characteristics of the currency, and the Bitcoin ecosystem require examination before there can be any meaningful discussion of policy matters and projections for future regulation of Bitcoin money laundering.

A. Bitcoin's Design

In 1998, Wei Dai wrote an article proposing an anonymous digital currency that could operate without the need for an intermediary and where government interjection would be "permanently forbidden and permanently unnecessary."[13] Just over 10 years later, and shortly after the financial crisis, Dai's idea was effectuated by Satoshi Nakamoto.[14] Nakamoto, widely considered an alias for either an anonymous programmer or group of programmers,[15] launched an open-source software

---

[12] *Id.*; *see also* U.S. CONST. amend. V.

[13] *See* Wei Dai, *B-Money*, http://www.weidai.com/bmoney.txt (last visited Feb. 14, 2015).

[14] SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM, *available at* http://www.bitcoin.org/bitcoin.pdf (last visited Feb. 20, 2015).

[15] *See* Joshua Davis, *The Crypto-Currency*, NEW YORKER, Oct. 10, 2011, at 62, *available at* http://www.newyorker.com/magazine/2011/10/10/the-crypto-currency; Benjamin Wallace, *The Rise and Fall of Bitcoin*, WIRED (Nov. 23, 2011, 2:52 PM), http://www.wired.com/2011/11/mf_bitcoin/all/.

program capable of creating an unbacked "electronic form of floating currency."[16] With the introduction of the software program in early 2009, Nakamoto had created Bitcoin.

Bitcoin is an online payment system whose unit of currency goes by the same name. It is a form of digital cryptocurrency that can be exchanged over the internet without the need for traditional financial institutions or third parties.[17] The client software relies entirely on a network of peer-to-peer technology for the creation, management, and distribution of the currency.[18] The Bitcoin network is comparable to networks that construct such services as BitTorrent[19] and Skype.[20]

Unlike traditional fiat currency, bitcoins are created through a computer-intensive process known as mining. The system utilizes an algorithm that runs on a peer-to-peer network of interconnected computers known as nodes.[21] The technology helps "ensure that . . . transactions are: (1) secure; (2) efficient; and (3) free of third party presence."[22] "[C]ryptographic proof" allows the system to be both secure and free of third party presence.[23] A cryptographic proof, also known as a "zero-knowledge proof" is a "mathematical method that can prove something is true without revealing why it's true."[24] "It allows for Bitcoin miners to independently try to find the next block, and once they do that miner [can] transmit[] the solution they

---

[16] Derek A. Dion, Note, *I'll Gladly Trade You Two Bits on Tuesday for a Byte Today: Bitcoin, Regulating Fraud in the E-Conomy of Hacker-Cash*, 2013 U. ILL. J.L. TECH. & POL'Y 165, 167 (2013).

[17] Emily Stephenson & Brett Wolf, *Regulators, Bitcoin Group Discuss Digital Currency*, REUTERS (Aug. 26, 2013 6:08 PM), http://www.reuters.com/article/2013/08/26/us-financial-regulation-bitcoin-idUSBRE97P0OO20130826.

[18] *See* Nikolei M. Kaplanov, Student Article, *Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against its Regulation*, 25 LOY. CONSUMER L. REV. 111, 115 (2012).

[19] BitTorrent is a peer-to-peer file sharing protocol that distributes file transfers across multiple systems. This lessens the average bandwidth used by each computer. *BitTorrent,* TECHTERMS.COM, http://www.techterms.com/definition/bittorrent (last visited Feb. 20, 2015).

[20] Skype is an internet video and telephone service that uses proprietary protocols that incorporate a peer-to-peer structure. *Encyclopedia,* PC MAG., http://www.pcmag.com/encyclopedia/term/51443/skype (last visited Feb. 20, 2015); *see also* T.S., *How Does Bitcoin Work?*, ECONOMIST (Apr. 11, 2013, 10:50 PM), http://www.economist.com/blogs/economist-explains/2013/04/economist-explains-how-does-bitcoin-work.

[21] Joshua J. Doguet, Comment, *The Nature of the Form: Legal and Regulatory Issues Surrounding the Bitcoin Digital Currency System*, 73 LA. L. REV. 1119, 1125 (2013).

[22] Kaplanov, *supra* note 18, at 116.

[23] NAKAMOTO, *supra* note 14, at 1.

[24] Jacob Aron, *Crypotgraphic Proof Paves Way for Nuke-Free World*, NEW SCIENTIST (June 25, 2014), http://www.newscientist.com/article/mg22229753.200-cryptographic-proof-paves-way-for-nukefree-world.html#.VCpxuSldVFp.

found throughout the network."[25] While cryptographic proof nearly guarantees security and the absence of third party intervention; cryptographic proof alone neither guarantees the privacy of those engaging in the transaction, nor does it avert the same user from double spending the same bitcoin.[26]

To keep transactions private, Bitcoin utilizes public-key encryption.[27] The Bitcoin client software generates two strings of mathematically related numbers, also known as cryptographic keys.[28] One key is private and forms the foundation of the user's electronic wallet.[29] The other key, known as the Bitcoin address, is public.[30] The public key is used to accept Bitcoin payments. It is often compared to an e-mail address, "public and available to everyone[,whereas] the private key is like the password needed to authorize messages (in this case bitcoins) to go in and out."[31] The entire Bitcoin community is able to tell that a transaction has taken place, but there is no information connecting the transaction to an individual.[32]

To solve the double-spending problem, an intensive system-wide approval process ensues immediately after the transaction is signed with the private key.[33] The transaction is relayed to each node on the Bitcoin network for approval.[34] Once the transaction is approved through a computationally intensive process known as Bitcoin mining, whereby each node attempts to solve a cryptographic puzzle, the transaction is time-stamped and added to a block chain.[35] The "block chain is a public record of Bitcoin transactions in chronological order."[36] The node or "miner" that solves the puzzle is rewarded with 25 bitcoins, thereby creating a Bitcoin ecosystem that is completely self-sufficient without any intervention by outside parties.[37] Valid transactions are then broadcasted to the public

---

[25] *Proof of Work System,* LEARN CRYPTOGRAPHY, http://learncryptography.com/proof-of-work-system/ (last visited Feb. 20, 2015).

[26] Kaplanov, *supra* note 18, at 116.

[27] *Id.* at 117.

[28] Kaplanov, *supra* note 18, at 117; Stokes, *supra* note 3, at 2.

[29] *See* Dion, *supra* note 16; Doguet, *supra* note 21.

[30] Doguet, *supra* note 21, at 1126.

[31] Kaplanov, *supra* note 18, at 117.

[32] NAKAMOTO, *supra* note 14, at 6.

[33] Dion, *supra* note 16, at 168.

[34] Doguet, *supra* note 21, at 1127.

[35] *Id.* at 1127-28.

[36] *Some Bitcoin Words You Might Hear,* BITCOIN, https://bitcoin.org/en/vocabulary#block-chain (last visited Feb. 20, 2015).

[37] J.P., *Virtual Currency: Bits and Bob*, ECONOMIST (June 13, 2011, 8:30 PM), http://www.economist.com/blogs/babbage/2011/06/virtual-currency.

ledger.[38] The entire process provides "incontestable proof of the ownership and transactional history of each Bitcoin."[39] Further, "the computational force required to alter the blockchain ensures that transactions cannot be undone and that the same coin cannot be spent twice."[40]

The process of rewarding users who solve the complicated puzzles with bitcoins creates an incentive for the user "to support the network" while simultaneously "provid[ing] a way to initially distribute coins into circulation."[41] However, limits have been placed on the creation of new bitcoins.[42] The value of the reward received by miners will be halved for every 210,000 bitcoins created.[43] The software automatically limits the market to "no more than 21 million bitcoins in circulation" at one time.[44] This removes the need for third-party intervention while simultaneously creating stability in the market.[45] The currency is not subject to the "inflationary whim of whatever Federal Reserve chief decides to print more money."[46] Further, the lack of third-party intervention drastically lowers transaction costs.[47]

B. How Bitcoin is Utilized

Bitcoins can be obtained through the process of mining[48] as described above or alternatively, via purchase at an online exchange.[49] The inherent traits of the Bitcoin system rely on intrinsic values that fluctuate based upon supply and demand.[50] Regardless, Bitcoin is "currently traded on exchanges where the price of bitcoin floats against other currencies."[51] On these exchanges, users can exchange national fiat currencies (e.g. USD, GBP, or Yen) for bitcoins.[52]

---

[38] Doguet, *supra* note 21, at 1128.

[39] *Id.*

[40] *Id.*

[41] NAKAMOTO, *supra* note 14, at 4.

[42] Stokes, *supra* note 3, at 2.

[43] Kaplanov, *supra* note 18, at 121.

[44] *Id.*

[45] *Id.*

[46] Andy Greenberg, *Crypto Currency*, FORBES (Apr. 20, 2011, 6:00 PM), http://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html.

[47] *How Bitcoin Works*, FORBES (Aug. 1, 2013, 12:25 PM), http://www.forbes.com/sites/investopedia/2013/08/01/how-bitcoin-works/.

[48] *See supra* note 35.

[49] J.P., *supra* note 37.

[50] *Id.*

[51] Kaplanov, *supra* note 18, at 121.

[52] *Id.* at 122.

Most Bitcoin exchanges operate in a very similar fashion, although some offer various niche services.[53] One of the most prominent of these Bitcoin exchanges is Bitstamp.[54] On Bitstamp, a user adds fiat currency to their account to conduct an exchange for bitcoins.[55] The user may also cash out their bitcoins and receive their dollar value. Additionally, each exchange requires users to enter into a service agreement that lays out the rights and obligations of each party.[56]

Bitcoins can also be purchased directly for cash or through PayPal or Dwolla.[57] In a typical cash transaction, the parties meet face-to-face and the owner of the bitcoins will transfer the bitcoins over the internet, usually through e-mail, and the purchaser will pay the agreed upon amount.[58] Users can even obtain bitcoins by using a Bitcoin ATM[59] and are available for exchange on eBay and Craigslist.[60] During the first eight days that the world's first Bitcoin ATM began operation in a coffee shop in Vancouver, people bought and sold over $100,000 in Bitcoin, with approximately 80 percent of transactions involving Bitcoin purchases and the other 20 percent involving sales of Bitcoins for cash.[61]

No matter how the bitcoins are garnered, they must be stored on a personal computer, online service, or mobile application[62] known as an electronic wallet.[63] The "wallet is . . . a free open-source software program that . . . generate[s]" the private cryptographic key and public address.[64] Since there is no cost to obtain a new electronic wallet with a new address, it is

---

[53] *Id. at* 121.

[54] BITCOIN EXCHANGE GUIDE, http://bitcoinexchangeguide.com/ (last visited Feb. 20, 2015).

[55] Vitalik Buterin, *Introducing the Exchanges: Bitstamp*, BITCOIN MAG. (Feb. 13, 2013), http://bitcoinmagazine.com/3275/introducing-the-exchanges-bitstamp/.

[56] *Terms of Use*, BITSTAMP, https://www.bitstamp.net/terms-of-use/ (last visited Feb. 16, 2015).

[57] Dion, *supra* note 16, at 168.

[58] Kaplanov, *supra* note 18, at 123.

[59] Timothy B. Lee, *People Have Bought or Sold Over $100,000 in Bitcoins from a Vancouver ATM, Firm Says*, WASH. POST (Nov. 6, 2013, 4:16 PM), http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/06/people-have-bought-or-sold-100000-in-bitcoins-from-a-vancouver-atm-firm-says/.

[60] *See* REUTERS WHITE PAPER, *supra* note 1; Michael Carney, *An Expensive Lesson Against Selling Bitcoin on eBay*, PANDO DAILY (Aug. 27, 2013), http://pandodaily.com/2013/08/27/an-expensive-lesson-against-selling-bitcoin-on-ebay/.

[61] Lee, *supra* note 59.

[62] Kaplanov, *supra* note 18, at 116; *A Briefing on Bitcoin*, USA TODAY (Nov. 8, 2013, 12:35 PM), http://www.usatoday.com/story/news/nation/2013/10/21/bitcoin-q-and-a/3144889/.

[63] Dion, *supra* note 16, at 167.

[64] *How Bitcoin Works*, *supra* note 47.

extremely common for Bitcoin owners to "create a new address for each transaction as a means of ensuring privacy and enhancing security."[65] Anonymity is one of the most attractive attributes of Bitcoin; the structure and ease of utilizing multiple electronic wallets ensures that parties can engage in transactions without divulging their user information.[66]

As a consequence of the growing demand for Bitcoin, there has been a growth in the acceptance of Bitcoin in legal, non-nefarious contexts.[67] Bitcoin has been accepted by several organizations including WikiLeaks for charitable donations.[68] Further, Bitcoin is now being accepted by a number of retailers, both on the Internet and in brick-and-mortar facilities.[69] The list includes websites Etsy and OKCupid, as well as bars in London and New York City.[70]

Despite the government shutdown of a large illegal drug network only accepting Bitcoin as consideration[71] and the collapse of what was the world's largest Bitcoin exchange,[72] the Bitcoin market is robust, with the value of a single bitcoin reaching $582.[73] At the moment, there are over 13 million bitcoins in circulation with a market capitalization of approximately $6.4 billion.[74]

II. MONEY LAUNDERING: DEFINING THE PROBLEM

The anonymous, near-untraceable nature of Bitcoin has undoubtedly attracted criminals to the currency.[75] These traits have also garnered the attention of Senators Charles Schumer and Joe Manchin, who declared Bitcoin "an online form of money laundering used to disguise the source of the money," in a June 2011 letter to the Attorney General of the United States, the Drug Enforcement Agency, and the Department of

---

[65] *Id.*

[66] Kaplanov, *supra* note 18, at 126.

[67] *See* Dion, *supra* note 16, at 169.

[68] *Id.*

[69] Andre Byrne & Will Hallatt, *Bitcoin or Bitcon?*, CYBERSPACE LAW., Sept. 2013, at 13.

[70] *Id.*

[71] *See* Kim Zetter, *How the Feds Took Down the Silk Road Drug Wonderland*, WIRED (Nov. 18, 2013 6:30 AM), http://www.wired.com/2013/11/silk-road/.

[72] *See* Robert McMillan, *The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster*, WIRED (Mar. 3, 2014 6:30 AM), http://www.wired.com/2014/03/bitcoin-exchange/.

[73] *See, e.g.*, BITCOIN WATCH, http://bitcoinwatch.com/ (value listed as of Sept. 5, 2014).

[74] *Id.*

[75] Kurt Mattson, *Senate Committee Looks Into Virtual Currencies*, BSA/AML UPDATE 1 (Oct. 15, 2013).

Justice.[76] This letter put Bitcoin under the national spotlight. While it is likely that the money laundering risks raised by the government and private citizens have been overstated,[77] there is certainly reason for concern.

Originally, Bitcoin was only used by proficient computer nerds or hackers seeking anonymous payment for tasks performed on the internet.[78] Many early users also used the currency as a statement against traditional fiat currency.[79] However, the currency quickly became a mainstay in the "underbelly of the Internet, also known as the Deep Web."[80] The anonymous nature of the Deep Web is intimately linked to nefarious activities like "drug trafficking, arms trafficking, terrorism and child pornography."[81]

The most famous of the Deep Web sites connected to Bitcoin is Silk Road.[82] Silk Road was known to deal in illegal services and drug sales, only accepting Bitcoin as payment.[83] The extremely popular site was shut down on October 2, 2013 by the United States government.[84] The owner, Ross Ulbricht, was arrested several months after his pseudonym Dread Pirate Roberts was indicted in Maryland.[85] It remains unclear exactly how the F.B.I. unmasked Ulbricht given the indictment is sealed.[86] After his arrest, Mr. Ulbricht's bitcoins were confiscated.[87] Despite the indictment and arrest of Mr. Ulbricht, alternative illegal goods and service websites accepting Bitcoin immediately proliferated, including the reincarnation of Silk Road.[88]

---

[76] *Schumer Pushes to Shut Down Online Drug Marketplace*, NBC NEW YORK (June 5, 2011, 2:53 PM), http://www.nbcnewyork.com/news/local/123187958.html (quoting Senator Charles Schumer) (internal quotation marks omitted); *see also* Doguet, *supra* note 21, at 1142.

[77] Andrea Castillo, *Bitcoin: Understated Benefits and Overstated Risks*, THE HILL (Aug. 21, 2013, 3:00 PM), http://thehill.com/blogs/congress-blog/technology/317875-bitcoin-understated-benefits-and-overstated-risks.

[78] Dion, *supra* note 16, at 169.

[79] *Id.*

[80] REUTERS WHITE PAPER, *supra* note 1.

[81] *Id.*

[82] Byrne & Hallatt, *supra* note 69.

[83] Greg Thomas, *The Silk Road is Shut Down, and the Owner is in Custody*, VICE (Oct. 2, 2013), http://motherboard.vice.com/read/the-silk-road-is-shut-down-and-the-owner-is-in-custody.

[84] *Id.*

[85] Matthew Goldstein, *Silk Road Case Began with Hunt for a John Doe*, N.Y. TIMES DEALB%K (Mar. 21, 2014), http://dealbook.nytimes.com/2014/03/21/silk-road-case-began-with-hunt-for-a-john-doe/?_php=true&_type=blogs&_r=0.

[86] *Id.*

[87] Thomas, *supra* note 83.

[88] John Ribiero, *Silk Road Drug Marketplace Rises from the Grave After Legal Smackdown*, PC WORLD (Nov. 7, 2013 6:04 AM), http://www.pcworld.com/article/2061800/silk-road-online-drug-marketplace-resurfaces.html.

A. The Ins and Outs of Money Laundering

"Money laundering is a process by which the illicit source of assets obtained . . . by criminal activity is concealed to obscure the link between the funds and the original criminal activity."[89] These "operations generally boil down to 'a . . . complex process often using the latest technology, of sanitising money in such a manner that its true nature, source or use is concealed, thereby creating an apparent justification for . . . possessing the laundered money.'"[90] Consequently, "[m]oney laundering is often a secondary process—preceded by an illegal activity."[91] The Financial Action Task Force (FATF), "an international policy-making and standard-setting body dedicated to combating money laundering and terrorist financing,"[92] estimates the amount of money laundered per year is somewhere between 1.3 and 3.4 trillion dollars.[93]

The archetypal model for laundering money is a three-step process. First, dirty money is placed into a legitimate enterprise.[94] Second, the money is layered through several transactions.[95] Last, the funds are integrated "into the 'legitimate financial world.'"[96] Historically, financial institutions and front operations were the enterprises of choice for criminals when laundering their money.[97] Today, advancements in technology have shifted the paradigm. Digital currencies are now a viable and attractive option for criminals looking to launder their money.[98]

Although money laundering is technically a non-violent and usually "victimless" crime, its undertaking has destructive social consequences. FinCEN, a bureau of the Department of Treasury whose mission includes "safeguard[ing] the financial

---

[89] *Factsheet*, *supra* note 7.

[90] GUY STESSENS, MONEY LAUNDERING: A NEW INTERNATIONAL LAW ENFORCEMENT MODEL 83 (2000) (quoting Secretary-General of the UN, *Note Strengthening Existing International Cooperation*, at 4) (omissions in original).

[91] REUTERS WHITE PAPER, *supra* note 1.

[92] Resource Center, *Financial Action Task Force*, U.S. DEP'T OF THE TREASURY (Dec. 3, 2010, 9:30 PM), http://www.treasury.gov/resource-center/terrorist-illicit-finance/Pages/Financial-Action-Task-Force.aspx.

[93] REUTERS WHITE PAPER, *supra* note 1.

[94] Turner, *supra* note 6, at 1392.

[95] *Id.*

[96] *Id.* (quoting *Money Laundering*, 39 AM. CRIM. L. REV. 839, 840 (2002)).

[97] *Id.*

[98] NAT'L DRUG INTELLIGENCE CTR, U.S. DEP'T OF JUSTICE, NO. 2008-R0709-003, MONEY LAUNDERING IN DIGITAL CURRENCIES (June 2008).

system from illicit use and combat[ing] money laundering"[99] provides a bevy of harmful consequences spurred from money laundering. "[M]oney laundering provides the fuel for drug dealers, terrorists, arms dealers, and other criminals to operate and expand their criminal enterprises."[100] For instance, analysts from the U.S. Department of Treasury determined that a single money laundering operation was responsible for supplying Al Qaeda, the terrorist organization responsible for the September 11, 2001 attacks, with between 15 million dollars and 20 million dollars each year.[101] Further, money laundering can have a devastating economic impact. The International Monetary Fund suggests that money laundering "can undermine the integrity and stability of financial institutions and systems, discourage foreign investment, and distort international capital flows,"[102] thereby disrupting a country's economic stability.

In light of the extreme negative consequences attributed to money laundering, the United States and several international partners have taken a strong approach in their anti-money laundering strategies, which are governed by several key statutes. In 1970, the United States passed the Bank Secrecy Act (BSA) whereby any "money services businesses" (defined below) must report financial transactions in excess of $10,000.[103] The act has since been amended several times in response to the ever-shifting money laundering landscape. In 1986, Congress passed the Money Laundering Control Act (MLCA), which made money laundering a federal felony accompanied by stiff fines and lengthy jail time.[104] In 1989, the International Monetary Fund formed the FATF.[105] The FATF consists of 36 countries working in conjunction to create a global standard for anti-money laundering.[106] In 1994, Congress passed the Money Laundering

---

[99] *What We Do*, FINCEN, http://www.fincen.gov/about_fincen/wwd/ (last visited Nov. 2, 2013).

[100] *Frequently Asked Questions*, FINCEN, http://www.fincen.gov/about_fincen/wwd/faqs.html (last visited Feb. 16, 2015).

[101] *The Financial War on Terrorism and the Administration's Implementation of the Anti-Money Laundering Provisions of the USA Patriot Act: Hearings Before the S. Banking Comm.*, 107th Cong. (2002) (testimony of Kenneth W. Dam, Deputy Sec'y, U.S. Dept. of the Treasury), *available at* 2002 WL 110357.

[102] *Factsheet*, *supra* note 7.

[103] *See Bank Secrecy Act Requirements: A Quick Reference Guide for Money Services Businesses*, FINCEN, http://www.fincen.gov/financial_institutions/msb/materials/en/bank_reference.html, (last visited Feb. 16, 2015).

[104] 18 U.S.C. § 1956 (2012).

[105] REUTERS WHITE PAPER, *supra* note 1.

[106] *Id.*

Suppression Act that required each Money Services Business (MSB) to be registered by an owner or controlling person of the MSB.[107] Operating an unregistered MSB became a federal crime.[108] In response to the attacks on September 11, 2001, Congress enacted the USA PATRIOT Act that required banks to more closely monitor transactions with the threat of greater civil and criminal penalties.[109] More recently, in November 2012, the United States Treasury Department created a new anti-money laundering task force to deal with the "'remarkable change' occurring in the financial industry, driven by technological and financial innovation."[110]

Bitcoin money laundering shares much in common with archetypal money laundering. There are similarities in the overall process of laundering funds and subsequent consequences of such actions. However, as a vehicle for money laundering, the currency's unique attributes have created difficult regulatory problems.

B. Bitcoin as a Vehicle for Money Laundering

Several risks inherent to Bitcoin make it a prime vehicle for laundering money. First, Bitcoin users can transfer instruments with financial value to one another without the intervention of any third-party, including that of banks or other financial institutions.[111] This is troublesome given that the traditional approach to thwarting money laundering is through the use of banks or other key professionals as a policing force. The banks or other professionals guard against money laundering by reporting suspicious activity and "limiting the ability of criminals to transfer value without scrutiny."[112] The risk is even greater due to the lack of face-to-face contact in completing these transactions. In more common-place monetary transactions, "enhanced due-diligence is required where the customer is not physically present for identification purposes."[113] That safeguard proves impossible given the inherent traits of the Bitcoin ecosystem.

A second, interrelated issue is user anonymity in completing transactions. As mentioned above, every Bitcoin transfer is published to the public ledger, however, private keys

---

[107] 31 U.S.C. § 5330 (2011).

[108] *Id.*

[109] *Id.* §§ 5311-14, 5316-32.

[110] REUTERS WHITE PAPER, *supra* note 1. These provisions are discussed in greater detail and an analysis of their effect on Bitcoin and its users is in Part III *infra.*

[111] Stokes, *supra* note 3, at 2.

[112] *Id.* at 2-3.

[113] *Id.* at 3.

remain anonymous and "there are no records linking any public address to an individual or organization."[114] Compounding this issue is the ease with which a user can obtain a new public address.[115] Bitcoin users typically have multiple electronic wallets and addresses, thereby muddying the evidentiary waters and making it very difficult for law enforcement to efficiently and properly investigate potential money laundering violations.

A third money laundering risk relates to the relative "speed and ease with which Bitcoin transactions can be carried out."[116] Unlike cash, the traditional anonymous vehicle utilized to launder money,[117] money launderers utilizing Bitcoin need not worry about cumbersome physical limitations.[118] The electronic process serves a dual feature for money launderers: it allows them to complete domestic or international transactions within 10 minutes while simultaneously "allow[ing] for [a] considerably easier payment structur[e] [known as] 'smurfing' so as to avoid suspicion."[119]

Although the inherent traits of Bitcoin pose substantial problems for regulators,[120] these problems are not insurmountable and do not warrant a complete prohibition of Bitcoin. The remainder of this note will discuss the government's burgeoning approach to the money laundering problem through the use of anti-money laundering provisions that have already been enacted. The government's archetypal approach is likely to raise collateral, constitutional consequences.[121]

III. THE REGULATORY RESPONSE TO BITCOIN: FITTING A SQUARE PEG IN A ROUND HOLE

The meteoric rise in the value and popularity of Bitcoin in conjunction with the growing problem of money laundering has led regulators to turn their attention to addressing the perceived problem of Bitcoin as a vehicle for money laundering.[122] Despite the increased attention, United States regulators have not explicitly cleared up the legal confusion surrounding regulating

---

[114] *Id.*

[115] *Id.*

[116] *Id.*

[117] Castillo, *supra* note 77.

[118] Stokes, *supra* note 3, at 3.

[119] *Id.*

[120] Regulators are faced with a dual-identification problem. First, law enforcement officials must be able to identify suspicious transactions. Second, if a transaction is deemed suspicious, officials must identify the near-anonymous user or users who completed the transaction. *Id.* at 2-3, 5.

[121] *See* REUTERS WHITE PAPER, *supra* note 1.

[122] *Id.*

Bitcoin.[123] Recent developments from United States federal courts and regulatory bodies indicate that the existing money laundering regulatory framework will guide Bitcoin regulation.

A. Regulatory Indications from the Federal Courts

The first case indicating the United States government's approach to thwarting digital currency money laundering followed the indictment of the proprietors of E-Gold by the United States Department of Justice.[124] On April 24, 2007, shortly before the advent of Bitcoin, digital currency enterprise E-Gold and their owners were indicted on four criminal charges.[125] Each owner was indicted "with one count of conspiracy to launder monetary instruments, one count of conspiracy to operate an unlicensed money transmitting business, one count of operating an unlicensed money transmitting business under federal law and one count of money transmission without a license under D.C. law."[126] The indictment and subsequent guilty plea of the owners and directors of E-Gold illustrate the interplay between Section 1960,[127] the BSA,[128] and the MLCA,[129] all tools that will likely be used against Bitcoin.[130]

Section 1960 imposes penalties on anyone who "knowingly conducts, controls, manages, supervises, directs or owns all or part of an unlicensed money transmitting business."[131] This statute directly relates to the BSA that requires "a wide-swath of otherwise unregulated financial institutions to register with the government, implement anti-money laundering procedures, keep data, and report certain transactions and other data."[132] The term "money services business" is defined as:

---

[123] Timothy B. Lee, *New Money Laundering Guidelines are a Positive Sign for Bitcoin*, FORBES (Mar. 19, 2013), www.forbes.com/sites/timothylee/2013/03/19/new-money-laundering-guidelines-are-a-positive-sign-for-bitcoin/.

[124] *Bitcoiners: Remember What Happened to eGold*, ECON. POL'Y J. (Apr. 10, 2013), http://www.economicpolicyjournal.com/2013/04/bitcoiners-remember-what-happened-to.html.

[125] Press Release, U.S. Dep't of Justice, Digital Currency Business E-Gold Indicted for Money Laundering and Illegal Money Transmitting (Apr. 27, 2007), *available at* http://www.justice.gov/opa/pr/2007/April/07_crm_301.html.

[126] *Id.*

[127] 18 U.S.C. § 1960 (2010).

[128] 31 U.S.C. § 5330 (2012).

[129] 18 U.S.C. § 1956.

[130] United States v. E-Gold, Ltd., 550 F. Supp. 2d 82, 86 (D.D.C. 2008).

[131] *Id.*

[132] Reuben Grinberg, *Bitcoin: An Innovative Alternative Digital Currency*, 4 HASTINGS SCI. & TECH. L.J. 159, 204 (2012).

> A person wherever located doing business . . . in one or more of the [following] capacities[:]. . . .(1) Dealer in foreign exchange . . . . (2) Check casher . . . . (3) Issuer or seller of traveler's checks or money orders . . . . (4) Provider of prepaid access . . . . (5) Money transmitter . . . . (6) U.S. Postal Service . . . . [or] (7) Seller of prepaid access.[133]

In *E-Gold*, the defendants argued they were not a "money transmitting business" under the BSA and therefore could not be held liable under Section 1960.[134] The court rejected the defendants' argument, holding that the legislative intent of Section 5330, a statute laying forth money transmitting business registration requirements, "expose[s] an intent to regulate 'financial institutions,' not just 'currency transmitters' or 'financial institutions that engage in currency transactions.'"[135] Precedent had been set that one does not need to engage in cash transactions to qualify as a money transmitting business.

Prosecutors also brought charges against E-Gold under the Money Control Act of 1986.[136] Generally, this statute "applies to individuals who conduct a financial transaction involving dirty money, knowing that the money is dirty, with the intent of promoting certain kinds of illegal activities, concealing the dirty money's origin, or avoiding a reporting requirement."[137] The scienter requirement can be met through the concept of willful blindness.[138] The charges were brought and sustained based on the fact that E-Gold "allowed its users to remain anonymous, maintained staff without financial experience, and did not respond to customer complaints concerning fraud."[139]

Although the case did not make it to trial, *E-Gold* indicated that certain digital currency businesses—"even those located abroad—must register under both federal . . . law or face criminal penalties."[140] Additionally, the court indicated that digital currency businesses or individuals who "knowingly process dirty money, make a profit on those transactions, and do nothing to stop processing those transactions, . . . may be guilty of money laundering."[141] Although the facts relating to *E-Gold* and the nature of E-Gold as a digital currency are clearly

---

133 31 C.F.R. § 1010.100 (ff) (2013).

134 *E-Gold, Ltd.*, 550 F. Supp. 2d at 86.

135 *Id.* at 97.

136 Grinberg, *supra* note 132, at 204.

137 *Id.* at 205.

138 Frans J. von Kaenel, *Willful Blindness: A Permissible Substitute for Actual Knowledge Under the Money Laundering Control Act?*, 71 WASH.U. L.Q. 1189, 1191 (1993).

139 Dion, *supra* note 16, at 179-80.

140 Grinberg, *supra* note 132, at 206.

141 *Id.*

distinguishable from Bitcoin, the ruling was the first opinion from the federal courts regarding the status of digital currency providers as MSBs. The opinion is also an indication that regulatory bodies will likely treat Bitcoin miners and exchanges as MSBs in their attempt to inhibit digital currency money laundering in the future.

B. Regulatory Indications from FinCEN

In the years following *E-Gold*, FinCEN "amend[ed] definitions and other regulations relating to money services businesses."[142] In early 2013, the government became active regarding the regulation of Bitcoin. On March 18, 2013, FinCEN[143] issued interpretative guidance "to clarify the applicability of the regulations implementing the Bank Secrecy Act to persons creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies."[144] This guidance coincided with the astronomical gains in both the intrinsic worth and the notoriety of Bitcoin.

Without mentioning Bitcoin by name, FinCEN provided its opinion of how to read Bitcoin into the statutory provisions. In essence, a "user who obtains convertible virtual currency and uses it to purchase real or virtual goods or services is **not** an MSB under FinCEN's regulations."[145] However, administrators and exchangers of virtual currency are money transmitters under FinCEN's regulations.[146] The guidance indicates that FinCEN is not interested in Bitcoin users or in regulating the Bitcoin network.[147] The guidance does indicate that digital currency exchanges, like Bitstamp are not exempt to the BSA or the MLCA. Additionally, the guidance seems to indicate that Bitcoin miners must register as MSBs.[148]

FinCEN's guidance has drawn a multitude of reactions. Some Bitcoin advocates believe that the paper is "the first step in a federal crackdown on Bitcoin."[149] Others feel that the

---

142 FINANCIAL CRIMES ENFORCEMENT NETWORK, *supra* note 9.

143 FinCEN has authority to issue guidance under its authority to administer the BSA. *See* Treas. Order 180-01 (Mar. 24, 2003).

144 FINANCIAL CRIMES ENFORCEMENT NETWORK, *supra* note 9.

145 *Id.*

146 *Id.*

147 Lee, *supra* note 123.

148 Bailey Reutzel, *Fincen Says Digital Currency Guidance Stands, but Talks Continue*, PAYMENTS SOURCE (Aug. 26, 2013, 5:09 PM), http://www.paymentssource.com/news/fincen-says-digital-currency-guidance-stands-but-talks-continue-3015241-1.html.

149 Lee, *supra* note 123.

guidelines are a clear indication that FinCEN is not interested in regulating the Bitcoin network, a seemingly positive sign.[150] Others in the Bitcoin community are confused by the guidance.[151] Individual and collective miners, extremely important facets of the Bitcoin ecosystem, are unsure of their regulatory requirements due to the ambiguity of the interpretive guidance.[152]

In the months following the release of FinCEN's guidance, Bitcoin began to grow in both popularity and value.[153] As mentioned above, the government indicted Ross Ulbricht and shut down his popular website known as the Silk Road shortly before the release of FinCEN's guidance.[154] In response, the Senate Committee on Homeland Security and Governmental Affairs "engaged in an investigation into the potential implications of virtual currencies."[155] On November 18, 2013, the Senate Committee held a fact-finding hearing where law enforcement officials and proponents of Bitcoin testified to both the potential promises and pitfalls of the digital currency.[156]

While some proponents of the virtual currency feared the congressional hearing on Bitcoin could result in a regulatory crackdown,[157] the government did not propound regulation any more stringent than the regulatory framework proposed in FinCEN's guidance.[158] During the hearing, the government described its "approach to virtual currencies, [its] recent successes in prosecuting criminals who use virtual currencies for illicit purposes, and some of the challenges [it]

---

[150] *Id.*

[151] Reutzel, *supra* note 148.

[152] Michael Carnery, *FinCEN to Bitcoin Miners: No Need to Register if the Bitcoins are for Your Own Use*, PANDO DAILY (Dec. 30, 2013), http://pando.com/2013/12/30/fincen-to-bitcoin-miners-no-need-to-register-if-the-bitcoins-are-for-your-own-use/.

[153] Jose Paglieri, *Senate Takes a Close Look at Bitcoin*, CNN MONEY (Nov. 18, 2013), http://money.cnn.com/2013/11/18/technology/bitcoin-regulation/.

[154] *See* Goldstein, *supra* note 85.

[155] *Beyond Silk Road: Potential Risks, Threats and Promises of Virtual Currencies: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 113th Cong. 1 (2013) [hereinafter *Beyond Silk Road*] (statement of Thomas R. Carper, Chairman, S. Comm. on Homeland Sec. & Governmental Affairs).

[156] Rob Wile, *Bitcoin Crosses $700 as Senate Hearing Wraps*, BUS. INSIDER (Nov. 18, 2013, 4:20 PM), http://www.businessinsider.com/senate-bitcoin-hearing-2013-11.

[157] Timothy B. Lee, *Here's How Bitcoin Charmed Washington*, WASH. POST (Nov. 21, 2013, 2:52 PM), http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/21/heres-how-bitcoin-charmed-washington//?print=1.

[158] *Compare* FINANCIAL CRIMES ENFORCEMENT NETWORK, *supra* note 9 (offering guidance that would require Bitcoin administrators and exchangers to comply with existing anti-money laundering regulations), *with Beyond Silk Road*, *supra* note 155, (statement of Mythili Raman, Acting Assistant Att'y Gen., Criminal Div. of the U.S., at 3) (stressing importance to law enforcement interests that virtual currency systems "comply with applicable anti-money laundering and know-your-customer controls").

face[s] as virtual currency systems continue to evolve."[159] Rather than being a tumultuous precursor to a crackdown on the virtual currency, the hearing was described as a "lovefest" between the government and Bitcoin proponents.[160]

Although "lovefest" may be an overstatement, the hearing was certainly cordial. In her testimony, Acting Assistant Attorney General, Mythili Raman, conceded that digital currency systems "offer legitimate financial services and have the potential to promote more efficient global commerce,"[161] while simultaneously recognizing the Department of Justice's law enforcement concerns and interests in these currencies.[162] According to Ms. Raman, the Department of Justice has two primary interests in regulating virtual currency: deterring and prosecuting individuals using virtual currencies to launder money and prosecuting virtual currency services that violate laws designed to thwart money laundering.[163] While acknowledging the inherent characteristics of Bitcoin—that is, its ability to "conduct transfers quickly, securely, and often with a . . . higher level of anonymity than . . . traditional financial services,"[164]—Ms. Raman stressed that law enforcement interests can be met as long as the Bitcoin ecosystem "compl[ies] with applicable anti-money laundering and know-your-customer controls."[165] While recognizing some unique challenges attributed to the currency, i.e. the need for international cooperation and the difficulties in obtaining customer records,[166] the Department of Justice indicated that it too would attempt to fit Bitcoin into the existing regulatory framework.[167]

IV. THE TENSION BETWEEN MONEY LAUNDERING REGULATIONS AND THE FIFTH AMENDMENT

In light of FinCEN's guidance and the recent Congressional hearing, it has become clear that the government's

---

[159] *Beyond Silk Road*, *supra* note 155, (statement of Mythili Raman, Acting Assistant Att'y Gen., Criminal Div. of the U. S., at 1).

[160] Lee, *supra* note 157.

[161] *Beyond Silk Road*, *supra* note 155, (statement of Mythili Raman, Acting Assistant Att'y Gen., Crim. Div. of the U.S., at 1).

[162] *Id.*

[163] *Id.*

[164] *Id.*

[165] *Id.*

[166] The difficulty of obtaining customer records is a larger problem than Ms. Raman has admitted. The Fifth Amendment issues associated with key disclosure laws are discussed in Section IV.A.

[167] *Beyond Silk Road*, *supra* note 155, (statement of Mythili Raman, Acting Assistant Att'y Gen., Crim. Div. of the U.S., at 5).

approach to thwarting "Bitcoin-centric" money laundering will center on existing anti-money laundering laws.[168] While the framework the government has signaled it will use to confront the money laundering problem will be partially successful, the approach will encounter potentially insurmountable challenges. Even if administrators and exchangers are forced to register and abide by existing anti-money laundering regulations and know-your-customer controls, the inherent structure of Bitcoin leaves serious problems for regulators.

Regulatory bodies and investigators will find it difficult both to track criminals using Bitcoin and to seize their criminal proceeds. Even if the government can locate the customer records they wish to obtain—a difficult task due to the lack of a central administering authority—the digital wallets that contain the valuable evidence and criminal proceeds will be encrypted with a private key.[169] The government will then be forced to utilize a subpoena duces tecum in order to obtain this evidence and effectively prosecute and eliminate money laundering. As one commentator has posited, "[k]ey disclosure laws may become the most important government tool in asset seizures and the war on money laundering."[170]

A. The Fifth Amendment

Although compelled key disclosure might "become the most important government tool"[171] in hampering Bitcoin as a vehicle for money laundering, forcing a suspect to provide the government with the private key necessary to decrypt the electronic wallet raises substantial self-incrimination issues. The Fifth Amendment provides that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself."[172] However, "the Fifth Amendment does not independently proscribe the compelled production of every sort of incriminating evidence."[173] It "protects a person . . . against being incriminated by his own compelled testimonial communications."[174] Consequently, the evidence must be testimonial in nature, meaning that the communication "itself, explicitly or implicitly,

---

168 *See infra* Part III.B.
169 *See supra* note 29.
170 Matonis, *supra* note 11.
171 *Id.*
172 U.S. CONST. amend. V.
173 Fisher v. United States, 425 U.S. 391, 408 (1976).
174 *Id.* at 409.

relate[s] a factual assertion or disclose[s] information."[175] Worded alternatively, it is "the attempt to force [an accused] 'to disclose the contents of his own mind' that implicates the Self-Incrimination Clause."[176] In many cases where the Fifth Amendment privilege against self-incrimination is asserted, the focus is simply on whether the act is testimonial.

B. Analogous Case Law

Several recent cases have considered whether the Fifth Amendment privilege against self-incrimination protects a defendant from being compelled to divulge his or her password of encryption key.[177] The first case to do so is *In re Grand Jury Subpoena to Sebastien Boucher*.[178] In 2006, Sebastien Boucher crossed the Canadian border at Derby Line, Vermont when a Customs and Border Protection inspector performed a secondary inspection of Mr. Boucher's car.[179] The inspector noticed a laptop in the car, "which Mr. Boucher acknowledged as his" own.[180] Upon searching the computer, a Special Agent for Immigration and Customs Enforcement uncovered files that appeared to contain child pornography.[181] Boucher admitted to downloading pornography and stated that he occasionally unintentionally downloaded child pornography, but quickly deleted the files upon realization of their contents.[182] Boucher showed the agent some of the files, several of which appeared to be child pornography.[183] He was arrested and the laptop was seized.[184]

When the government attempted to duplicate the contents of the laptop, they discovered the drive containing the pornographic images was encrypted and could only be accessed with a password.[185] The government sought a grand jury subpoena compelling Mr. Boucher to "produce the password."[186] "Boucher moved to quash the subpoena, arguing that the act of

---

[175] Doe v. United States, 487 U.S. 201, 210 (1988).

[176] *Id.* at 211 (quoting Curcio v. United States, 354 U.S. 118, 128 (1957)) (internal citation omitted).

[177] Matonis, *supra* note 11.

[178] *In re* Grand Jury Subpoena to Sebastien Boucher, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009).

[179] *Id.* at *1.

[180] *Id.*

[181] *Id.* at *2.

[182] *Id.*

[183] *Id.*

[184] *Id.*

[185] *Id.*

[186] *Id.*

production of this information would violate his Fifth Amendment privilege against self-incrimination."[187] The subpoena required Mr. Boucher to provide the government with an "unencrypted version" of the drive containing the images.[188] The magistrate judge granted Mr. Boucher's motion to quash and the government appealed.[189]

The issue presented for the District of Vermont on appeal was "whether requiring Boucher to produce an unencrypted version of his laptop . . . would constitute compelled testimonial communication."[190] In deciding the motion, the court relied on the foregone conclusion doctrine.[191] The doctrine states, "Where the existence and location of the documents are known to the government, 'no constitutional rights are touched,' because these matters are a 'foregone conclusion.'"[192] Because "the government . . . kn[ew] of the existence and location" of the incriminating files, and "providing access to the unencrypted [files] 'adds little or nothing to the sum total of the Government's information' about the existence and location of files that may contain incriminating information," Mr. Boucher had no Fifth Amendment privilege to refuse the subpoena.[193] As a "forgone conclusion," Mr. Boucher's sharing of the password was not testimonial in nature.

In 2010, a district court facing the same issue applied a similar analysis but did not use the term "foregone conclusion." In *United States v. Fricosu*,[194] the FBI executed a search warrant on Ramona Fricosu's residence.[195] During the search, the FBI seized six computers, one of which was password-protected by an encryption program.[196] Shortly after the execution of the search warrant, the police intercepted a phone call made between Ms. Fricosu and her ex-husband, who was incarcerated.[197] During the phone call, Ms. Fricosu tacitly acknowledged ownership of the computer and alluded to the presence of incriminating files on the encrypted hard drive.[198] As a result of the conversation, the government sought a court-ordered writ that would "requir[e] Ms.

---

187 *Id.* at *1.
188 *Id.* at *2.
189 *Id.* at *1.
190 *Id.* at *3.
191 *Id.*
192 *Id.*
193 *Id.* at *3-4 (quoting Fisher v. United States, 425 U.S. 391, 411 (1976)).
194 United States v. Fricosu, 841 F. Supp. 2d 1232 (D. Col. 2012).
195 *Id.* at 1234.
196 *Id.*
197 *Id.* at 1234-35.
198 *Id.* at 1235.

Fricosu to produce the unencrypted contents of the [laptop]."[199] Ms. Fricosu declined to produce the files asserting her Fifth Amendment privilege against self-incrimination.[200]

The District of Colorado ordered Ms. Fricosu to decrypt the hard drive, relying on the reasoning applied in *In re Grand Jury Subpoena to Sebastien Boucher*.[201] Without utilizing the phrase "foregone conclusion," the court applied the doctrine. In ordering the decryption of the drive, the court said, "the government kn[ew] of the existence and location of the computer's files. The fact that it d[id] not know the specific content of any specific documents [was] not a barrier to production."[202] The facts available to the government made the production of the files a foregone conclusion, and thus, not sufficiently testimonial to trigger the protection of the Fifth Amendment.

The most recent case to address whether a password is considered testimony is *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*.[203] In 2010, in the midst of a child pornography investigation, the FBI tracked John Doe to a hotel room and executed a search warrant for all of his digital media, seizing seven different devices.[204] FBI examiners were unable to access certain files due to their encryption.[205] The government served Doe with a grand jury subpoena that required him to produce the unencrypted contents of the files.[206]

Doe declined to comply with the subpoena, asserting that compliance would be in violation of his Fifth Amendment right against self-incrimination.[207] Doe claimed "by decrypting the contents, he would be testifying that he, as opposed to some other person, placed the contents on the hard drive, encrypted the contents, and could retrieve and examine them whenever he wished."[208] The Eleventh Circuit held "[t]he Fifth Amendment protects Doe's refusal to decrypt and produce the contents of the media devices because the act of decryption and production would be testimonial, and because the Government cannot show that the 'foregone conclusion' doctrine applies."[209]

---

199 *Id.*
200 *Id.*
201 *Id.* at 1237-38.
202 *Id.*
203 *In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335 (11th Cir. 2012).
204 *Id.* at 1339.
205 *Id.*
206 *Id.*
207 *Id.*
208 *Id.* at 1339-40.
209 *Id.* at 1349.

In deciding the case, the Eleventh Circuit utilized a two-step analysis.[210] First, the court must decide if what the government seeks to compel "is testimonial in character."[211] Second, if the produced content is testimonial in character, "the question becomes whether the purported testimony is a 'foregone conclusion.'"[212] In answering the first prong, the court determined that decryption and production is "tantamount to testimony by Doe of his knowledge of the existence and location of potentially incriminating files; of his possession, control, and access to the encrypted portions of the drives; and of his capability to decrypt the files."[213]

As to the second prong, the court determined that the testimony was not a "foregone conclusion."[214] In making this determination, the court said "[n]othing in the record . . . reveals that the Government knows whether any files exist and are located on the hard drives."[215] Additionally, "nothing in the record illustrates that the Government knows with reasonable particularity that Doe is even capable of accessing the encrypted portions of the drives."[216]

Relying on both the Ninth and D.C. Circuits,[217] the court said "[w]here the location, existence, and authenticity of the purported evidence is known with reasonable particularity, the contents of the individual's mind are not used against him, and therefore no Fifth Amendment protection is available."[218] Because the testimony was not a "foregone conclusion," Fifth Amendment protection was available for Doe.

---

[210] *Id.* at 1346.

[211] *Id.*

[212] *Id.* The analysis used by the court is very similar to the framework used in *In re Grand Jury Subpoena to Sebastien Boucher* and *United States v. Fricosu*. However, the opinion in *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011* is far more detailed and clear. This can likely be attributed to the fact the Court of Appeals took more time to craft an opinion it felt would be widely read and scrutinized.

[213] *In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1346 (11th Cir. 2012).

[214] *Id.*

[215] *Id.*

[216] *Id.*

[217] *See* United States v. Ponds, 454 F.3d 313, 320-21 (D.C. Cir. 2006); *In re* Grand Jury Subpoena Dated April 18, 2003, 383 F.3d 905, 910 (9th Cir. 2004).

[218] *In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d at 1344 (internal footnotes omitted).

C. The Fifth Amendment's Application to Bitcoin Private Keys

The government's approach to virtual currency prosecutions, regulatory interpretive guidance, and federal precedent in password decryption cases provide the roadmap for a future Bitcoin money laundering prosecution. It is quite likely the government will subpoena a Bitcoin administrator, exchanger, or user for a privacy key to decrypt their virtual wallet. There are three reasons this prediction will come to light. First, the United States government has recently turned its attention to both Bitcoin and thwarting money laundering where Bitcoin is the conduit. Second, the government has acknowledged the difficulty Bitcoin's encryption creates in both obtaining valuable evidence and seizing criminal proceeds.[219] Third, the government has signaled they will utilize existing regulations and laws to derail Bitcoin money laundering.[220] The eventual subpoena, compelling an accused Bitcoin money launderer to divulge their private key or decrypt their virtual wallet, will almost certainly be met with a Fifth Amendment challenge asserting a violation of one's privilege against self-incrimination. It is likely the court will protect the privilege, fettering law enforcement in its attempt to prosecute money laundering.[221]

Although the challenge will spawn a case of first impression and the case will turn heavily on its facts, synthesizing the three aforementioned cases provides a framework with which one can predict the outcome of the future Bitcoin private key disclosure cases. In a hypothetical case, the government will become aware of a potential money launderer, likely through the use of current anti-money laundering regulations and know-your-customer rules. If the government can locate the suspected money launderer, a difficult task because "[t]here are no records linking any public address to an individual or organization,"[222] they will likely bring criminal charges under the MLCA.[223] However, the government will be unable to access the alleged criminal proceeds located in the suspect's digital wallet. This is due to one of Bitcoin's crucial attributes as a cryptocurrency: the partial anonymity and privacy

---

[219] *Beyond Silk Road*, *supra* note 155, (statement of Mythili Raman, Acting Assistant Att'y Gen., Crim. Div. of the U.S., at 6).

[220] *See supra* Part III.

[221] Joe Palazzolo, *Court: Fifth Amendment Protects Suspects from Having to Decrypt Hard Drives*, WALL ST. J. (Feb. 23, 2012, 6:55 PM), http://blogs.wsj.com/law/2012/02/23/court-fifth-amendment-protects-suspects-from-decrypting-computers/.

[222] Stokes, *supra* note 3, at 3.

[223] Grinberg, *supra* note 132.

afforded by the need for a private key to decrypt the wallet.[224] Unable to access the alleged criminal proceeds, the government will subpoena the suspect.[225] The subpoena will be met with a Fifth Amendment challenge from the alleged money launderer.

Relying on analogous case law,[226] the court will first need to determine if the act of entering a private key or decrypting a Bitcoin wallet is a compelled testimonial act. It is likely the court will determine the requested production is testimonial in nature. The witness will be forced to disclose information that exists in the suspect's mind, a key factor in determining if an act is testimonial. [227] Further, "[c]ompelled testimony that communicates information that may 'lead to incriminating evidence' is privileged even if the information itself is not inculpatory."[228] The court would likely find the compulsion testimonial in nature, thus implicating the accused's Fifth Amendment privilege.

Next, the court would need to make a legal determination, based upon the facts, as to "whether the purported testimony is a 'foregone conclusion.'"[229] Given the anonymity of Bitcoin and the relative "speed and ease with which Bitcoin transactions can be carried out,"[230] it is likely the government will be scant on information regarding the alleged illegal transactions. The "foregone conclusion" doctrine applies when "any testimonial value derived from the act of production [is] already known to the Government and therefore [the production] add[s] nothing to its case."[231] Further, the Eleventh Circuit's input of the "reasonable particularity" doctrine into the "foregone conclusion" framework creates the likelihood that the first court to hear this case will use the more exacting standard.[232]

---

[224] *See* Kaplanov, *supra* note 18.

[225] *See In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335 (11th Cir. 2012); United States v. Fricosu, 841 F. Supp. 2d 1232 (D. Col. 2012); *In re* Grand Jury Subpoena to Sebastien Boucher, No. 2:06-mj-91, 2009 WL 4246473 (D. Vt. Feb. 29, 2009).

[226] *See* cases cited *supra* note 225.

[227] *See In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d at 1345.

[228] United States v. Hubbell, 530 U.S. 27, 38 (2000) (quoting Doe v. United States, 487 U.S. 201, 208 n.6 (1988)).

[229] *In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d at 1346.

[230] Stokes, *supra* note 3, at 3.

[231] *In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d at 1346 (citing *In re* Grand Jury Subpoena to Sebastien Boucher, No. 2:06-mj-91, 2009 WL 4246473, at *3-4 (D. Vt. Feb. 19, 2009)).

[232] *Id.* at 1346.

Given the Bitcoin ecosystem's inherent characteristics,[233] it will be quite difficult for the government to "show with 'reasonable particularity' that, at the time it sought to compel the act of production, it already knew of the materials, thereby making any testimonial aspect a 'foregone conclusion.'"[234] It is likely the Fifth Amendment privilege against self-incrimination protects a suspected Bitcoin money launderer against compelled divulgence of a private key or decrypted password to their virtual wallet.

CONCLUSION

According to the Chairman of the Senate Committee on Homeland Security and Governmental Affairs, "Bitcoin[has] captured the imagination of some, struck fear among others, and confused the heck out of many of us."[235] His assertion is correct. The mostly anonymous, very secure, and extremely liquid cryptocurrency has skyrocketed in both value and allure since its introduction to the internet in 2009. With its increased value and allure, Bitcoin has "seen increased attention from regulators, law enforcement, investors, and entrepreneurs."[236] Regulators and law enforcement officials are primarily concerned with Bitcoin's potential for money laundering and the devastating economic and social consequences associated with money laundering, while investors and entrepreneurs are excited by the potential advent of a valuable and stable global currency.[237]

The United States government has yet to crackdown on Bitcoin. In recent months, government officials have signaled that they will take a "wait and see" approach while concomitantly utilizing existing anti-money laundering laws including the MLCA, the BSA, and know-your-customer laws to combat the money laundering problem. There appears to be an attempt to balance the potentially valuable attributes of Bitcoin, including its ability to add financial stability in developing countries, lower transaction costs, and remove third-party intermediaries, with its potential for nefarious activities, including money laundering, drug trafficking, and

---

[233] *See supra* Part I.

[234] *In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d at 1346.

[235] *Beyond Silk Road*, *supra* note 155 (statement of Thomas R. Carper, Chairman, S. Comm. on Homeland Sec. & Governmental Affairs, at 1).

[236] *Id.*

[237] *Id.*

child exploitation.[238] There is little doubt the government will not wait to use the tools currently at their disposal to thwart Bitcoin money laundering.[239]

A crucial tool the government will likely utilize is its subpoena power in an attempt to access a suspected money launderer's virtual wallet to obtain evidence and seize potentially criminal proceeds. This subpoena will be met with a Fifth Amendment challenge from the accused. Although there are no cases directly on point, other cases involving the forced compulsion of passwords or decrypted files provide a serviceable analog with which to predict the outcome of the inevitable Bitcoin case. It is my belief that the forced compulsion of a private Bitcoin key violates the Fifth Amendment privilege against self-incrimination "because the act of decryption and production would be testimonial, and because the [g]overnment [will not be able to] show that the 'foregone conclusion' doctrine applies."[240]

It is unclear whether Bitcoin will "prove to be a boom or a bust,"[241] but the potential for Bitcoin's impact on both the American economy and jurisprudence is immense and perhaps harmful without effective regulation. Although Bitcoin's future is far from certain, the currency deserves the attention it has received and will continue to receive from regulators, law enforcement officials, academics, entrepreneurs, and curious people alike.

Nicholas J. Ajello[†]

---

[238] *Id.*

[239] *Id.*

[240] *In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1349 (11th Cir. 2012).

[241] *Beyond Silk Road*, *supra* note 155 (statement of Thomas R. Carper, Chairman, S. Comm. on Homeland Sec. & Governmental Affairs, at 2).

[†] J.D. Candidate, 2015, Brooklyn Law School. B.A., Economics, Wesleyan University, 2010. I would like to thank the members of the *Brooklyn Law Review* for their thorough and incisive comments and edits. Additionally, I want to express my interminable gratitude to my family, John, Dolores, and Christopher for their love, support, and reassurance not only during law school, but throughout the entirety of my life.