

2015

## The New Wild West: Preventing Money Laundering in the Bitcoin Network

Kavid Singh

*University of Texas School of Law*

---

### Recommended Citation

Kavid Singh, *The New Wild West: Preventing Money Laundering in the Bitcoin Network*, 13 NW. J. TECH. & INTELL. PROP. 37 (2015).  
<https://scholarlycommons.law.northwestern.edu/njtip/vol13/iss1/2>

This Article is brought to you for free and open access by Northwestern Pritzker School of Law Scholarly Commons. It has been accepted for inclusion in Northwestern Journal of Technology and Intellectual Property by an authorized editor of Northwestern Pritzker School of Law Scholarly Commons.

N O R T H W E S T E R N  
JOURNAL OF TECHNOLOGY  
AND  
INTELLECTUAL PROPERTY

**The New Wild West: Preventing Money  
Laundering in the Bitcoin Network**

*Kavid Singh*



---

February 2015

VOL. 13, NO. 1

# The New Wild West: Preventing Money Laundering in the Bitcoin Network

By Kavid Singh \*

*Bitcoin is the most popular, decentralized virtual currency in the world. Businesses both large and small have begun to accept bitcoins as a legal form of payment. In addition, Bitcoin currency exchanges, which trade bitcoins for real currency, have quickly arisen because of the currency's growing popularity.*

*But Bitcoin's evolution has also been marred with criminality. Hundreds of millions of dollars' worth of bitcoins have been stolen from businesses and large Bitcoin currency exchanges. The infamous "Silk Road"—an illegal, online drug market, which the FBI took down in 2013—dealt in this currency. The use of bitcoins for illicit purposes not only facilitates criminal activity throughout the world, but also undermines the security of individuals using bitcoins for legitimate purposes, such as users who send remittances to family members abroad.*

*The Financial Crimes Enforcement Network (FinCEN), a bureau of the U.S. Department of the Treasury, stands at the forefront of Bitcoin regulation. FinCEN was the first federal agency to address convertible virtual-currency regulation, providing legal guidance (the Guidance) explaining how the Bank Secrecy Act applies to convertible virtual currencies. For this reason, this Article analyzes and evaluates the Guidance's standards regarding convertible virtual currencies.*

*This Article proposes a refined regulatory framework that both deters money laundering in Bitcoin—a pervasive problem in the world of decentralized virtual currencies—and allows the recognized benefits of this virtual currency to develop free from innovation-stifling regulation. Among other benefits, Bitcoin increases access to financing in impoverished areas, provides an avenue for low-cost remittances, lowers transaction costs for businesses burdened with high credit-card fees, and perhaps most importantly, creates a global platform for financial and technological innovation to flourish. While authorities recognize these advantages, the potential for criminal abuse nevertheless remains salient. This Article seeks to provide the optimal balance between these often-conflicting interests.*

---

\* J.D. Candidate, 2015, The University of Texas School of Law. Special thanks to Professor Henry Hu for helping me devise this topic and structure the Article. Additional thanks to my friend, Alex Ingraham, for taking the time to read and extensively comment on what was to be the final draft. Finally, I would like to express my gratitude to George McHugh and the UT Mises Circle for explaining various aspects of Bitcoin and introducing me to various texts on the topic.

## TABLE OF CONTENTS

I.	Introduction.....	38
II.	How Bitcoin Works .....	40
	A. The Double-Spending Problem .....	40
	B. How a Bitcoin Transaction Occurs.....	41
	C. The Function of Miners and the Mining Process.....	42
	1. Updating the Public Ledger with New Transactions .....	43
	2. The Introduction of New Bitcoins into Circulation .....	43
	3. Mining and the Prevention of Double Spending.....	44
III.	The Bank Secrecy Act .....	45
	A. Explanation .....	45
	B. Importance .....	46
	C. FinCEN’s Interpretive Guidance .....	47
IV.	Refining FinCEN’s Interpretive Guidance .....	48
	A. Bitcoin Regulation: The Detriment of Overly Burdensome Regulation .....	48
	B. Redefining FinCEN’s “User” Definition.....	50
	1. FinCEN’s Clarification .....	50
	2. Continuing Uncertainty .....	52
	3. FinCEN’s Definition of User Should Be Replaced.....	54
	4. Redefining FinCEN’s Definition of User .....	54
	C. Alternative Solution: Treating All Miners as Money Transmitters .....	55
	1. Mining as a Money-Laundering Technique Poses Little Threat.....	55
	2. An Ultimately Ineffective Approach.....	56
V.	The Benefits and Limitations of Applying the Refined FinCEN Standard .....	58
	A. Applying the Refined FinCEN Standard to Currency Exchanges.....	58
	1. Easily Identifiable Currency Exchanges .....	58
	2. Secretive Currency Exchanges.....	59
	B. Applying the Refined FinCEN Standard to Businesses .....	60
	C. Applying the Refined FinCEN Standard to Mixers .....	61
VI.	Conclusion .....	63

## I. INTRODUCTION

Bitcoin<sup>1</sup> is the most popular, decentralized virtual currency in the world.<sup>2</sup> Created by the enigmatic Satoshi Nakamoto in 2009,<sup>3</sup> Bitcoin’s propagation and use has caused heated controversy.<sup>4</sup> Businesses both large and small have begun to accept bitcoins as a

---

<sup>1</sup> In this Article, “Bitcoin” will refer to the entire Bitcoin network or the currency as a whole, while “bitcoin” will refer to the individual currency units.

<sup>2</sup> *Crypto-Currency Market Capitalizations*, COINMARKETCAP, <https://coinmarketcap.com> (last visited Mar. 27, 2014).

<sup>3</sup> See *Frequently Asked Questions*, BITCOIN.ORG, <https://bitcoin.org/en/faq> (last visited Mar. 27, 2014) [hereinafter *Bitcoin FAQ*] (identifying Satoshi Nakamoto under the “Who created Bitcoin?” heading).

<sup>4</sup> See Joe Light, *Should You Invest in Bitcoin?*, WALL ST. J.,

legal form of payment.<sup>5</sup> In addition, Bitcoin currency exchanges, which trade bitcoins for real currency, have quickly arisen because of the currency's growing popularity.<sup>6</sup>

But Bitcoin's evolution has also been marred with criminality. Hundreds of millions of dollars' worth of bitcoins have been stolen from businesses and large Bitcoin currency exchanges.<sup>7</sup> The infamous "Silk Road"—an illegal, online drug market, which the FBI took down in 2013—dealt in this currency.<sup>8</sup> Criminal prosecution has implicated some of the most publicly respected members of the Bitcoin community, such as Charlie Shrem, who was arrested for money laundering in early 2014.<sup>9</sup> The use of bitcoins for illicit purposes not only facilitates criminal activity throughout the world, but also undermines the security of individuals using bitcoins for legitimate purposes, such as users who send remittances to family members abroad.<sup>10</sup>

The Financial Crimes Enforcement Network (FinCEN), a bureau of the U.S. Department of the Treasury, stands at the forefront of Bitcoin regulation.<sup>11</sup> FinCEN was the first federal agency to address convertible virtual-currency regulation, providing legal guidance (the Guidance) that explains how the Bank Secrecy Act (BSA) applies to convertible virtual currencies.<sup>12</sup> For this reason, this Article analyzes and evaluates the Guidance's standards regarding convertible virtual currencies. Additionally, although this Article's conclusions apply categorically to all convertible virtual currencies, this Article focuses solely on Bitcoin because it is the most widely used virtual currency and possesses the most similarities with other convertible virtual currencies generally.<sup>13</sup>

---

<http://online.wsj.com/news/articles/SB10001424052702304607104579212101356897382> (last updated Nov. 23, 2013).

<sup>5</sup> See Ian Kar, *What Companies Accept Bitcoin?*, NASDAQ (Feb. 4, 2014, 10:05 AM), <http://www.nasdaq.com/article/what-companies-accept-bitcoin-cm323438>.

<sup>6</sup> See *Complete List of Bitcoin Exchanges*, PLANET BITCOIN, <http://planetbtc.com/complete-list-of-bitcoin-exchanges/> (last visited Mar. 27, 2014).

<sup>7</sup> See, e.g., Lucian Constantin, *Withdrawal Vulnerabilities Enabled Bitcoin Theft from Flexcoin and Poloniex*, PC WORLD (Mar. 5, 2014, 10:37 AM), <http://www.pcworld.com/article/2104940/withdrawal-vulnerabilities-enabled-bitcoin-theft-from-flexcoin-and-poloniex.html>; Nathaniel Popper & Rachel Abrams, *Apparent Theft at Mt. Gox Shakes Bitcoin World*, N.Y. TIMES (Feb. 25, 2014), <http://www.nytimes.com/2014/02/25/business/apparent-theft-at-mt-gox-shakes-bitcoin-world.html>.

<sup>8</sup> See Tim Hume, *How FBI Caught Ross Ulbricht, Alleged Creator of Criminal Marketplace Silk Road*, CNN, <http://www.cnn.com/2013/10/04/world/americas/silk-road-ross-ulbricht/> (last updated Oct. 5, 2013).

<sup>9</sup> Kyle Russell, *Meet the "Bitcoin Millionaire" Arrested for Allegedly Helping Silk Road Launder \$1 Million*, BUS. INSIDER (Jan. 28, 2014, 11:00 PM), <http://www.businessinsider.com/charlie-shrem-arrested-bitcoin-ceo-2014-1>.

<sup>10</sup> See JERRY BRITO & ANDREA CASTILLO, BITCOIN: A PRIMER FOR POLICYMAKERS 13 (Aug. 19, 2013), available at [http://mercatus.org/sites/default/files/Brito\\_BitcoinPrimer\\_embargoed.pdf](http://mercatus.org/sites/default/files/Brito_BitcoinPrimer_embargoed.pdf).

<sup>11</sup> See *Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies: Hearing on S.D. 342 Before the S. Comm. on Homeland Sec. & Gov't Affairs*, 113th Cong. 6–7 (2013) [hereinafter *FinCEN Hearing*], available at <http://www.hsgac.senate.gov/download/?id=e92d0cf1-9df0-44d9-b25a-d734547c0c30>.

<sup>12</sup> See FIN. CRIMES ENFORCEMENT NETWORK, DEP'T OF THE TREASURY, FIN-2013-G001, APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES 1 (Mar. 18, 2013) [hereinafter THE GUIDANCE], available at [http://fincen.gov/statutes\\_regs/guidance/pdf/FIN-2013-G001.pdf](http://fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf); *History of Anti-Money Laundering Laws*, FIN. CRIMES ENFORCEMENT NETWORK, [http://www.fincen.gov/news\\_room/aml\\_history.html](http://www.fincen.gov/news_room/aml_history.html) (last visited Mar. 27, 2014) [hereinafter *BSA History*] (discussing the Bank Secrecy Act).

<sup>13</sup> See *Crypto-Currency Market Capitalizations*, *supra* note 2; *Digital Currencies in the Datacenter: Altcoins Explained*, LIQUIDWEB (Mar. 12, 2014), <http://www.liquidweb.com/blog/index.php/digital-currencies-in-the-datacenter-altcoins-explained/>.

¶14 This Article proposes a refined regulatory framework that both deters money laundering in Bitcoin—a pervasive problem in the world of decentralized virtual currencies—and allows the recognized benefits of this virtual currency to develop free from innovation-stifling regulation. Among other benefits, Bitcoin increases access to financing in impoverished areas, provides an avenue for low-cost remittances, lowers transaction costs for businesses burdened with high credit-card fees, and perhaps most importantly, creates a global platform for financial and technological innovation to flourish.<sup>14</sup> While authorities recognize these advantages, the potential for criminal abuse nevertheless remains salient. This Article seeks to provide the optimal balance between these often-conflicting interests.

¶15 Part II begins the analysis, discussing what Bitcoin is and how it works. Part III explains the BSA and examines the Guidance. Part IV reviews FinCEN’s Guidance and administrative rulings, and offers an alternative solution that both accords with the current BSA framework and allows Bitcoin to progress. Finally, Part V applies this solution to various types of Bitcoin institutions and assesses the resulting benefits and limitations. As this Article suggests, revising FinCEN’s current regulatory standards<sup>15</sup> not only produces a more effective legal framework to deter money laundering in Bitcoin, but also cultivates the innovative platform’s growth and unrealized value.

## II. HOW BITCOIN WORKS

¶16 At its core, Bitcoin is a peer-to-peer, decentralized network administered by the network’s users,<sup>16</sup> as opposed to a centralized network in which a single individual or group controls the network and issues currency to the users. In a decentralized network, no one owns the network, and thus, no one has absolute control over the applicable currency.<sup>17</sup>

¶17 Understanding how Bitcoin works, and therefore how criminals launder money using the Bitcoin system, requires knowledge of three key concepts. Part II (A) first examines the “double-spending problem,” which Bitcoin was designed to tackle. Part II (B) explains how one conducts a Bitcoin transaction. Finally, Part II (C) delves into the functions of the “miner,” an important figure in Bitcoin, and the mining process that creates bitcoins.

### A. *The Double-Spending Problem*

¶18 The double-spending problem is the biggest obstacle to creating a viable virtual currency. Put simply, an individual double spends when he uses the same unit of currency

---

<sup>14</sup> See BRITO & CASTILLO, *supra* note 10, at 10, 13–16.

<sup>15</sup> See THE GUIDANCE, *supra* note 12, at 2.

<sup>16</sup> *Bitcoin FAQ*, *supra* note 3 (identifying Bitcoin as a decentralized, peer-to-peer network under the “What is Bitcoin?” heading). For more information on how Bitcoin works, the two sources this Article primarily cites to explain Bitcoin, the Bitcoin.org FAQ page and the Michael Nielsen blog post, supplemented with the Bitcoin wiki, are helpful aids to anyone seeking to understand Bitcoin basics. *Id.*; see Michael Nielsen, *How the Bitcoin Protocol Actually Works*, DATA-DRIVEN INTELLIGENCE BLOG (Dec. 6, 2013), <http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/>; BITCOIN WIKI, [https://en.bitcoin.it/wiki/Main\\_Page](https://en.bitcoin.it/wiki/Main_Page).

<sup>17</sup> See *Bitcoin FAQ*, *supra* note 3 (noting that no centralized authority has control over the Bitcoin network under the “What is Bitcoin?” heading).

in multiple transactions. Due to the ease of copying virtual currency, the double-spending problem is especially salient in virtual currency networks. If left unresolved, users can create and trade currency units freely, thus undermining the currency's value. Bitcoin is unique in that it mitigates the double-spending threat without resorting to third-party oversight.<sup>18</sup>

### B. *How a Bitcoin Transaction Occurs*

¶9 Before a user can trade in Bitcoin, the user must download a “Bitcoin Wallet” application, which contains both a “public key” and “private key.”<sup>19</sup> The public key is composed of a series of characters constituting the user's public address,<sup>20</sup> which serves as an identifying mark the user can post on the Internet to engage in trade.<sup>21</sup> On the other hand, only the user knows his private key, which he may use to “sign” transactions.<sup>22</sup> The public key is analogous to a physical home address available in a directory, while the private key is analogous to a unique pen used solely to sign one's contractual agreements.

¶10 The following hypothetical illustrates the specific steps in a Bitcoin transaction. Say that Sally wants to sell a pair of alpaca socks to Bob. First, Sally tells Bob her public address.<sup>23</sup> After Bob decides to buy these socks, he generates a transaction quantifying his bitcoin payment for the alpaca socks, which everyone in Bitcoin can see.<sup>24</sup> He then signs the transaction with his unique private key.<sup>25</sup> Finally, a so-called “Bitcoin miner”—in this case, Moe—verifies the transaction.<sup>26</sup>

¶11 Before verifying the transaction, Moe looks at the “public ledger” to confirm that the transaction does not involve double spending.<sup>27</sup> The public ledger serves as a publically available chronological list of all past transactions in the network.<sup>28</sup> The transaction history of a single bitcoin can be traced in the public ledger by looking at every transaction signature accompanying each trade of the bitcoin.<sup>29</sup> In this manner, a bitcoin can be identified as a single chain of past, distinctive digital signatures recorded in the public ledger with each signature serving as a link in the chain.<sup>30</sup> This chain of past signatures exclusively applies to a single bitcoin because no two bitcoins share the same

---

<sup>18</sup> SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM 1 (2009), available at <https://bitcoin.org/bitcoin.pdf> (discussing the benefits of solving the double-spending problem without resorting to a third party).

<sup>19</sup> Nielsen, *supra* note 16 (discussing the public and private keys under the “Bitcoin” heading).

<sup>20</sup> *Id.*

<sup>21</sup> *See id.*

<sup>22</sup> *Id.*

<sup>23</sup> *See id.*

<sup>24</sup> *See id.*

<sup>25</sup> *See id.* All Bitcoin transactions are irreversible. *Bitcoin FAQ*, *supra* note 3 (noting the irreversibility of Bitcoin transactions under the “Is Bitcoin useful for illegal activities?” heading).

<sup>26</sup> *See Bitcoin FAQ*, *supra* note 3 (discussing the verification process under the “How does Bitcoin mining work?” heading).

<sup>27</sup> *See Nielsen*, *supra* note 16 (noting that miners look to the public ledger when verifying Bitcoin transactions under the “Making everyone collectively the bank” heading).

<sup>28</sup> *Bitcoin FAQ*, *supra* note 3 (noting that the public ledger contains all past transactions under the “How does Bitcoin work?” heading); Nielsen, *supra* note 16 (noting that the transactions are time ordered under the “Proof-of-work” heading).

<sup>29</sup> Nielsen, *supra* note 16 (discussing the traceability of transaction signatures under the “Bitcoin” heading).

<sup>30</sup> *Id.*

transaction history,<sup>31</sup> thus providing the unique identifying feature allowing miners to detect double spending.

¶12 The public-ledger system is critical to Bitcoin’s development because it allows the decentralized network to operate without third-party oversight. This decreases transaction costs, increases Bitcoin liquidity, and provides the necessary safeguards to ensure consumer confidence. For instance, if Bob spends the same bitcoin twice, giving it to Sally for alpaca socks and to Ted for a book, the two transactions are broadcast to the network. Moe will see that both of Bob’s transactions have the same transaction history in the public ledger and recognize the double-spending threat. As a result, Moe will choose to verify only one of the transactions, preventing Bob from double spending.

¶13 The public ledger illustrates that Bitcoin is not an anonymous network but a pseudonymous one. Because every transaction appears in the public ledger, which includes the public addresses of those involved in specific transactions, all bitcoin transactions are traceable.<sup>32</sup> And while a public address cannot be traced directly to a person’s identity,<sup>33</sup> it is linked to an IP address—the unique identifier assigned to devices accessing the Internet.<sup>34</sup> For the unwary, this allows someone to discover a user’s location and personal identity with relative ease. This fear has prompted users to employ anonymizing software, such as “The Onion Router” (Tor),<sup>35</sup> which hides a user’s IP address to grant total anonymity on the Internet.<sup>36</sup>

¶14 Anonymous Bitcoin users utilizing Tor pose one of the biggest challenges for potential Bitcoin regulation and enforcement. Tor allows criminals to purchase bitcoins anonymously with stolen U.S. dollars (USD), which effectively conceals funds from law enforcement and tax authorities. When a money launderer feels it is safe, he can use these bitcoins to either buy goods or exchange them for USD, without ever revealing his IP address. Workable anti-money-laundering laws for Bitcoin, therefore, must either bypass or eliminate anonymity in the network.

### C. *The Function of Miners and the Mining Process*

¶15 Miners play a crucial role in Bitcoin. For this analysis, three specific functions of miners and the mining process are most important. This section explains how miners update the public ledger with recent transactions, how mining introduces new bitcoins into circulation, and how the mining process resolves the double-spending problem.

---

<sup>31</sup> This chain serves as a bitcoin’s serial number. *Id.*

<sup>32</sup> *See id.* (noting that all transactions are traceable to public addresses under the “How anonymous is Bitcoin?” heading).

<sup>33</sup> *Id.*

<sup>34</sup> *See Protect Your Privacy*, BITCOIN.ORG, <https://bitcoin.org/en/protect-your-privacy> (last visited Mar. 27, 2014).

<sup>35</sup> *See Maintaining Anonymity While Using Bitcoins*, DAILY ATTACK (June 16, 2011), <http://thedailyattack.com/2013/06/maintaining-anonymity-while-using-bitcoins/>.

<sup>36</sup> *See* Dune Lawrence, *The Inside Story of Tor: The Best Internet Anonymity Tool the Government Ever Built*, BLOOMBERG BUSINESSWEEK (Jan. 23, 2014), <http://www.businessweek.com/articles/2014-01-23/tor-anonymity-software-vs-dot-the-national-security-agency#p1>; *see also* Jake Rocheleau, *Introduction to Bitcoins and the Tor Network*, HONGKIAT.COM, <http://www.hongkiat.com/blog/introductions-to-bitcoins-tor-network/> (last visited Jan. 12, 2015) (“[W]hen you go to access a website on Tor it’ll pass your request through 3 different computers (called nodes). This level of encryption ensures that no single computer within the proxy chain can determine your physical location and requested content.”).

## 1. Updating the Public Ledger with New Transactions

¶16 Miners verify bitcoin transactions through the mining process.<sup>37</sup> Miners group these transactions into “blocks,” which miners add to the public ledger forming a compilation of recent transactions.<sup>38</sup> This creates an accurate chronology of all bitcoin transactions because every block contains a reference point identifying the immediately preceding block in the public ledger.<sup>39</sup> Thus, alongside Sally and Bob’s transaction for alpaca socks, Moe verifies various other transactions to put into the public ledger collectively as a block.<sup>40</sup>

¶17 Figure 1 illustrates the public ledger’s structure. Think of the squares in the figure as cardboard boxes, each filled with signed paper contracts made between various parties. The boxes on the far right contain the most recent contracts. The boxes on the far left include contracts dating back to the public ledger’s inception. This forms the “block chain.”<sup>41</sup> When Moe decides he has completed the verification process for a group of transactions, his “box” of contracts will be the most recently placed box on the far right of the line. The box to the immediate left of Moe’s box contains contracts previously verified by another miner. One can follow this chain of boxes back to the first box filled with contracts.

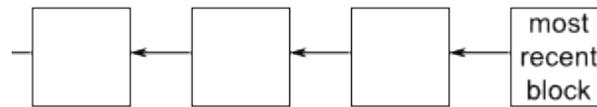


Figure 1<sup>42</sup>

## 2. The Introduction of New Bitcoins into Circulation

¶18 After a miner verifies a block of transactions, new bitcoins enter circulation.<sup>43</sup> Miners receive these new bitcoins as compensation for updating the public ledger with recent transactions.<sup>44</sup> Although the maximum amount of bitcoins in circulation is capped at twenty-one million,<sup>45</sup> the incentive to mine will likely remain after reaching this ceiling because parties are often willing to pay voluntary transaction fees in real currency to

<sup>37</sup> *Bitcoin FAQ*, *supra* note 3 (discussing the mining process under the “What is Bitcoin mining?” heading).

<sup>38</sup> *Id.* (discussing the verification of transactions under the “How does Bitcoin mining work?” heading).

<sup>39</sup> See Nielsen, *supra* note 16 (noting that blocks contain a reference to a past block and a list of transactions under the “Proof-of-work” heading).

<sup>40</sup> See *Bitcoin FAQ*, *supra* note 3 (discussing how transactions must be included in a block to be confirmed under the “How does Bitcoin mining work?” heading).

<sup>41</sup> See Nielsen, *supra* note 16 (noting that blocks contain a reference to a past block and a list of transactions under the “Proof-of-work” heading).

<sup>42</sup> See *id.*

<sup>43</sup> *Bitcoin FAQ*, *supra* note 3 (detailing how bitcoins are created under the “How are bitcoins created?” heading).

<sup>44</sup> See Nielsen, *supra* note 16 (discussing the rationale for awarding bitcoins to miners under the “Proof-of-work” heading).

<sup>45</sup> *Bitcoin FAQ*, *supra* note 3 (identifying the cap under the “How are bitcoins created?” heading).

verify their transactions.<sup>46</sup> And because miners choose which transactions to verify, miners can avoid transactions that do not provide a fee. Therefore, if at some point new-bitcoin compensation no longer provides sufficient incentives for miner verification, voluntary transaction fees will likely become more common.

### 3. Mining and the Prevention of Double Spending

¶19 The Bitcoin-mining system is important because, if easily manipulated, users might exploit the process for double-spending purposes. For example, if verifying a block of transactions required a majority vote of all network users, a double spender could game the system by creating enough public addresses to make up a majority of “users” in the network.<sup>47</sup> The double spender could then use this artificially created majority to vote in favor of a block containing his double-spent transactions.<sup>48</sup> So, if Bob wants to double spend, he would first use the same bitcoins to buy alpaca socks from many sellers. When the time comes to verify the block for these transactions, all of the sellers, and everyone else in the network, will notice that Bob double spent and refuse to verify the block. To overrule this refusal, Bob will create public addresses to form an artificial majority. This would allow Bob to verify transactions where he used the same unit of currency to pay various sellers.

¶20 Bitcoin’s unique structure precludes this type of behavior. To verify a block of transactions in Bitcoin, a miner must solve a complex math problem and generate a “proof of work” to everyone in the network upon completion of the problem.<sup>49</sup> Solving these problems requires computational power and expertise.<sup>50</sup> Unable to circumvent these math problems, miners compete to verify blocks, and the more computing power a miner has, the greater the chance she verifies a block first.<sup>51</sup> In this manner, a miner’s likelihood of verifying a block is proportional to the amount of computing power she wields compared to everyone else in the network.<sup>52</sup> As more miners enter the system, the network automatically increases the difficulty of the math problems, thus requiring a greater amount of computing power to solve a single problem.<sup>53</sup> In this system, a miner (or a group of miners) must control 51% of the computing power in the network to verify double-spent transactions consistently against the will of the remaining 49% of miners.<sup>54</sup>

¶21 Although the Bitcoin network makes double spending more difficult, the system is not bulletproof. Large mining companies have nearly attained 51% of Bitcoin’s

---

<sup>46</sup> Nielsen, *supra* note 16 (identifying the voluntary transaction fee under the “Proof-of-work” heading).

<sup>47</sup> *See id.* (discussing what verification would look like if determined by sheer number of identities). A tech-savvy individual can create various public addresses quickly and easily. *Id.*

<sup>48</sup> *See id.* (discussing what verification would look like if determined by sheer number of identities).

<sup>49</sup> *Bitcoin FAQ*, *supra* note 3 (describing the proof-of-work under the “How does Bitcoin mining work?” heading).

<sup>50</sup> *Id.* (explaining how computers must perform billions of calculations per second to solve these problems).

<sup>51</sup> Nielsen, *supra* note 16 (discussing the competition to verify blocks and the advantage of having more computing power under the “Proof-of-work” heading).

<sup>52</sup> *Id.*

<sup>53</sup> *Bitcoin FAQ*, *supra* note 3 (noting that the difficulty of the proof-of-work increases when more miners enter the system under the “How does Bitcoin mining work?” heading).

<sup>54</sup> *See* Alec Liu, *Bitcoin’s Fatal Flaw Was Nearly Exposed*, MOTHERBOARD (Jan. 10, 2014), <http://motherboard.vice.com/blog/bitcoins-fatal-flaw-was-nearly-exposed>.

computing power several times.<sup>55</sup> Double spending through a “51% attack,” however, has yet to occur, largely due to Bitcoin’s public ledger. Specifically, the public ledger can alert Bitcoin users of an attack, thus allowing users to take preventative measures before the brunt of the attack occurs.<sup>56</sup>

¶22 As a final note on the mining process, competition between miners has spiked over the past few years. This increased competition has spawned the birth of a new industry, with companies developing specialized computers, referred to as “rigs,” to mine bitcoin blocks more efficiently.<sup>57</sup> Consequently, it has become increasingly difficult for miners using average desktop computers to remain competitive.<sup>58</sup> Discussed *infra* Part IV, regulations that impose disclosure requirements on businesses selling mining equipment could help provide adequate safeguards for bitcoin users—thus increasing liquidity, promoting development, and maximizing Bitcoin’s potential value—while deterring money laundering.

### III. THE BANK SECRECY ACT

¶23 Part III first examines the Bank Secrecy Act (BSA) and its potential impact on the development of anti-money-laundering laws in Bitcoin. An analysis follows that further delves into the importance of the BSA in light of FinCEN’s Guidance concerning convertible virtual currencies.<sup>59</sup>

#### A. Explanation

¶24 Fundamentally, the BSA is a compilation of statutory provisions designed to prevent money laundering.<sup>60</sup> Congress enacted the BSA in 1970 to deter people from using banks and other financial institutions for money laundering.<sup>61</sup> The BSA requires financial institutions to disclose the identities of parties to transactions in excess of \$10,000 in Currency Transaction Reports (CTRs).<sup>62</sup> Further, the BSA imposes an affirmative duty on financial institutions to file Suspicious Activity Reports (SARs) for suspected-illegal transactions and implement anti-money-laundering programs.<sup>63</sup> In addition, Congress passed the Money Laundering Control Act of 1986, which makes

---

<sup>55</sup> See *id.* (displaying a graph with the mining power distribution in the Bitcoin network). The same article points out that a single mining company came close to reaching 51% of the network’s mining power, but members of the mining company left in order to bring its computing-power percentage down. *Id.* The “51% attack” problem is a systemic risk of the Bitcoin network. *Id.*

<sup>56</sup> See Daniel Cawrey, *Are 51% Attacks a Real Threat to Bitcoin?*, COINDESK (June 20, 2014), <http://www.coindesk.com/51-attacks-real-threat-bitcoin/>.

<sup>57</sup> Ashlee Vance & Brad Stone, *The Bitcoin-Mining Arms Race Heats Up*, BLOOMBERG BUSINESSWEEK (Jan. 9, 2014), <http://www.businessweek.com/articles/2014-01-09/bitcoin-mining-chips-gear-computing-groups-competition-heats-up#p3>; see *infra* Part IV(C) for a discussion of the burgeoning bitcoin-mining industry.

<sup>58</sup> See Vance & Stone, *supra* note 57.

<sup>59</sup> See THE GUIDANCE, *supra* note 12, at 1.

<sup>60</sup> See *BSA History*, *supra* note 12.

<sup>61</sup> See STEVEN LEVY, FEDERAL MONEY LAUNDERING REGULATION: BANKING, CORPORATE AND SECURITIES COMPLIANCE § 3.01 (2003).

<sup>62</sup> 31 U.S.C. § 5313(a) (2012); 31 C.F.R. § 1010.311 (2011). CTRs are filed with the Treasury Department. *Id.*

<sup>63</sup> 31 U.S.C. § 5318(g)(1), (h) (2012).

money laundering a federal crime,<sup>64</sup> and the USA Patriot Act of 2001, which deems operating an unlicensed money-transmission business a felony.<sup>65</sup> Generally, these anti-money-laundering laws prohibit transactions where parties hide the nature and ownership of ill-gotten proceeds, avoid reporting requirements, or intend to facilitate further crime.<sup>66</sup>

¶25 In 1970, Congress authorized the Secretary of the Treasury to implement the BSA.<sup>67</sup> The Treasury eventually delegated this authority to FinCEN, one of its bureaus.<sup>68</sup> FinCEN is ultimately responsible for issuing, implementing, and administering regulations pursuant to BSA mandate.<sup>69</sup> While FinCEN delegates its examination authority to other agencies, it remains the rulemaking authority for the BSA, often exercising this authority through the issuance of administrative rulings interpreting federal law and regulations.<sup>70</sup>

### B. Importance

¶26 The money-service-business (MSB) federal regulations implicate institutions involved in Bitcoin.<sup>71</sup> An MSB is defined under 31 C.F.R. 1010.100(ff) as “[a] person wherever located doing business, whether or not on a regular basis or as an organized or licensed business concern, wholly or in substantial part within the United States, in one or more of the capacities listed in paragraphs (ff)(1) through (ff)(7) of this section.”<sup>72</sup> The “capacity” of particular importance for Bitcoin is the “money transmitter,” defined as “[a] person that provides money transmission services . . . mean[ing] 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.”<sup>73</sup> Moreover, if an entity qualifies as an MSB, federal regulations also deem that entity a financial institution,<sup>74</sup> thereby mandating the entity to register with FinCEN,<sup>75</sup> file certain reports,<sup>76</sup> keep accurate records,<sup>77</sup> and implement anti-money-laundering programs.<sup>78</sup> Discussed *infra* Part V, the customer identification

<sup>64</sup> 18 U.S.C. §§ 1956(a), 1957(a) (2013).

<sup>65</sup> Andrew Schouten, *Unlicensed Money Transmitting Businesses and Mens Rea Under the USA PATRIOT Act*, 39 MCGEORGE L. REV. 1099, 1100 (2008).

<sup>66</sup> See LEVY, *supra* note 61, § 3.04.

<sup>67</sup> 31 U.S.C. § 5318(a) (2012).

<sup>68</sup> Treas. Order 180-01 (Oct. 21, 2002), available at <http://www.gpo.gov/fdsys/pkg/FR-2002-10-21/pdf/02-26656.pdf>.

<sup>69</sup> *Id.*

<sup>70</sup> 31 C.F.R. § 1010.810(a)-(b) (2011).

<sup>71</sup> See 31 C.F.R. § 1010.312 (2011); 31 C.F.R. § 1022.320(a)(1), (b)(1) (2011); FIN. CRIMES ENFORCEMENT NETWORK, DEP'T OF THE TREASURY, TDF 90-22.56B, SUSPICIOUS ACTIVITY REPORT INSTRUCTIONS 2, available at <http://www.fincen.gov/forms/files/f902256b.pdf> (last visited Jan. 8, 2015) [hereinafter SAR] (explaining SAR identification requirements for money-service-business customers). For instance, Bitcoin currency exchanges are institutions subject to MSB regulation under the BSA. See 31 C.F.R. § 1010.100(ff)(5)(i) (2011).

<sup>72</sup> 31 C.F.R. § 1010.100(ff) (2011).

<sup>73</sup> 31 C.F.R. § 1010.100(ff)(5)(i) (2011).

<sup>74</sup> 31 C.F.R. § 1010.100(t)(3).

<sup>75</sup> 31 U.S.C. § 5330(a)(1) (2012).

<sup>76</sup> 31 C.F.R. § 1010.306 (2011).

<sup>77</sup> See 31 C.F.R. § 1010.410 (2011).

<sup>78</sup> 31 C.F.R. § 1010.310 (2011); 31 C.F.R. §§ 1022.320, 1022.210(a) (2011).

requirements provided via SARs and CTRs are critical to removing anonymity in the Bitcoin network.<sup>79</sup>

¶27 Pursuant to BSA mandate, FinCEN’s broad rulemaking authority makes it one of the few federal agencies with the power to regulate virtual currency, which FinCEN first exercised through an interpretive guidance (the Guidance) in March 2013.<sup>80</sup> The Guidance currently provides the only instruction in determining how regulators intend to handle virtual currency going forward, especially with respect to money laundering.

### C. *FinCEN’s Interpretive Guidance*

¶28 The Guidance defines virtual currency as “a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency.”<sup>81</sup> It further defines convertible virtual currency as a type of virtual currency that “either has an equivalent value in real currency, or acts as a substitute for real currency.”<sup>82</sup> Important for this Article’s analysis, the Guidance categorizes users of convertible virtual currencies,<sup>83</sup> treating some as money transmitters subject to MSB registration, reporting, and recordkeeping requirements.<sup>84</sup> Specifically, FinCEN divides individuals participating in Bitcoin into three buckets: users, exchangers, and administrators.<sup>85</sup> Because the administrator category applies only to centralized virtual currencies, this Article analyzes only the user and exchanger categories.<sup>86</sup>

¶29 The Guidance defines a “user” as someone “who obtains convertible virtual currency and uses it to purchase real or virtual goods or services.”<sup>87</sup> This activity does not fit the BSA’s “money transmission service” definition; thus, users are not subject to MSB

---

<sup>79</sup> See 31 C.F.R. § 1010.312 (2011); SAR, *supra* note 71, at 2.

<sup>80</sup> See Anita Ramasastry, *Bitcoin: If You Can’t Ban It, Should You Regulate It?*, VERDICT (Feb. 25, 2014), <http://verdict.justia.com/2014/02/25/bitcoin-cant-ban-regulate> (identifying FinCEN as the only federal agency to have implemented Bitcoin regulation). The IRS has also issued legal guidance on the use of bitcoins. I.R.S. Notice 14-21, 2014-16 C.B. 938, 938–39 (2014), *available at* <http://www.irs.gov/pub/irs-irbs/irb14-16.pdf>. This notice stipulates that Bitcoin is to be treated as property for tax purposes, and therefore, Bitcoin users must calculate the fair market value, in USD, of bitcoins received. *Id.* Although the need to make such calculations will deter potential users from otherwise adopting the currency, there are at least two facts that help mitigate this concern. First, since all Bitcoin transactions are recorded in the public ledger, all of the information a law-abiding user will need to file taxes will already exist in the public ledger, which makes keeping personal track of transactions less burdensome. *Bitcoin FAQ*, *supra* note 3 (noting that the public ledger contains all past transactions under the “How does Bitcoin work?” heading). Second, the calculation of taxable income could be made easier in the future by the development of computer applications that track an individual or business’s transactions. Jose Pagliery, *New IRS Rules Make Using Bitcoins a Fiasco*, CNN MONEY (Mar. 31, 2014), <http://money.cnn.com/2014/03/31/technology/irs-bitcoin/>.

<sup>81</sup> THE GUIDANCE, *supra* note 12, at 1.

<sup>82</sup> *Id.*

<sup>83</sup> The distinction between virtual and convertible virtual currencies is immaterial for the rest of this Article, as a nonconvertible virtual currency will not be discussed. Thus, this Article refers to convertible virtual currencies as simply “virtual currencies.”

<sup>84</sup> See THE GUIDANCE, *supra* note 12, at 1.

<sup>85</sup> *Id.*

<sup>86</sup> *Id.* at 2.

<sup>87</sup> *Id.*

regulation.<sup>88</sup> In addition, a person who creates units of virtual currency (e.g., a miner) is not an MSB if she uses the virtual currency to buy goods or services.<sup>89</sup>

¶30 The Guidance defines an “exchanger” as “a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency.”<sup>90</sup> If a person’s activities fall within this definition, then accepting, buying, or selling virtual currency, for any reason, subjects that person to FinCEN’s MSB regulations.<sup>91</sup> Thus, exchangers qualify as MSBs unless a BSA exemption applies. For example, if Sally operates a virtual-currency exchange (making her an exchanger), and Bob wants to exchange his bitcoins for USD, Sally immediately becomes a money transmitter when she accepts Bob’s bitcoins.<sup>92</sup>

¶31 Perhaps recognizing the Guidance’s initial ambiguity, FinCEN released two administrative rulings in January 2014 to clarify both its user definition and the BSA’s application to virtual currencies.<sup>93</sup> Although these administrative rulings resolve some of the problems from the Guidance’s initial framework, important uncertainties remain.<sup>94</sup>

#### IV. REFINING FINCEN’S INTERPRETIVE GUIDANCE

¶32 Part IV first establishes this Article’s policy rationale for regulating Bitcoin, which focuses on the detriments of overregulation. A critique follows, questioning FinCEN’s original definition of “user” and its revised version thereof. In an effort to eliminate ambiguity and provide a viable regulatory framework, this Article recommends that FinCEN redefine “user” as “a possessor of a bitcoin that is not an exchanger.”<sup>95</sup> Part IV concludes with an analysis of two arguments advocating an alternative solution, which designates all Bitcoin miners as money transmitters by fiat.

##### A. *Bitcoin Regulation: The Detriment of Overly Burdensome Regulation*

¶33 One approach is to regulate Bitcoin out of existence. Proponents of this argument suggest that Bitcoin primarily provides value to criminals, and therefore should be

---

<sup>88</sup> *Id.*

<sup>89</sup> *Id.* at 5.

<sup>90</sup> *Id.* at 2.

<sup>91</sup> *See id.* at 3.

<sup>92</sup> *See id.*

<sup>93</sup> *See* FIN. CRIMES ENFORCEMENT NETWORK, DEP’T OF THE TREASURY, FIN-2014-R001, APPLICATION OF FINCEN’S REGULATIONS TO VIRTUAL CURRENCY MINING OPERATIONS 3–4 (2014) [hereinafter MINING RULING], available at [http://www.fincen.gov/news\\_room/rp/rulings/pdf/FIN-2014-R001.pdf](http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R001.pdf); FIN. CRIMES ENFORCEMENT NETWORK, DEP’T OF THE TREASURY, FIN-2014-R001, APPLICATION OF FINCEN’S REGULATIONS TO VIRTUAL CURRENCY SOFTWARE DEVELOPMENT AND CERTAIN INVESTMENT ACTIVITY 2–3 (2014) [hereinafter INVESTMENT RULING], available at [http://www.fincen.gov/news\\_room/rp/rulings/pdf/FIN-2014-R002.pdf](http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R002.pdf).

<sup>94</sup> *See, e.g., U.S. Treasury Cautions Bitcoin Businesses on Compliance Duties, Advocate Cites “Chilling Effect,”* REUTERS (Jan. 6, 2014) [hereinafter *Chilling Effect*], <http://blogs.reuters.com/financial-regulatory-forum/2014/01/06/u-s-treasury-cautions-bitcoin-businesses-on-compliance-duties-advocate-cites-chilling-effect/>.

<sup>95</sup> *See* THE GUIDANCE, *supra* note 12, at 1; INVESTMENT RULING, *supra* note 93, at 3–4; MINING RULING, *supra* note 93, at 2–3.

banned to prevent further criminal use.<sup>96</sup> These critics believe that Bitcoin's use provides little, if any, beneficial, noncriminal value, thus justifying its eradication.

¶34 But this stance goes too far. Bitcoin increases access to financing in poor areas, allows for low-cost remittances, decreases transaction costs for businesses burdened with high credit-card fees, and provides avenues for financial innovation, such as micro-transactions.<sup>97</sup> FinCEN has recognized these benefits, stating it does not wish to stifle Bitcoin's potential through regulations making its use prohibitively expensive.<sup>98</sup>

¶35 Additionally, enforcing regulations meant to eliminate Bitcoin is likely impossible. Bitcoin users wishing to remain anonymous can use Tor to avoid having their public addresses linked to their personal identities.<sup>99</sup> Consequently, criminals—rightfully assuming the improbability of detection—can continue to use the network regardless of government action. In fact, this heavy-handed approach will likely eradicate only the legitimate uses of Bitcoin, leaving users conducting clandestine transactions unscathed. Therefore, given the recognized beneficial uses of Bitcoin, regulators should pursue a balanced approach; one that fosters Bitcoin's benefits and deters money laundering, understanding that at a certain point regulation will be ineffective against anonymous users.

¶36 With these policy considerations in mind, the optimal regulatory strategy must target Bitcoin institutions that exchange virtual currency for real currency. Specifically, FinCEN should classify these institutions as “exchangers,” subjecting them to MSB regulations.<sup>100</sup> This deters money laundering without stymieing Bitcoin's potential in two primary ways. First, because of its widespread use, most criminals wish to exchange bitcoins for USD, which makes these financial institutions the focal point of money laundering in Bitcoin.<sup>101</sup> Second, MSB regulations require qualifying institutions to file CTRs and SARs, the former of which allows government agencies to ascertain the identity of any individual who converts bitcoins into at least \$10,000.<sup>102</sup> This relatively unobtrusive solution not only makes it more difficult for criminals to remain anonymous in Bitcoin, but also promotes the development of the virtual currency through transparency and predictability. In sum, because these regulations only target institutions that exchange in real and virtual currency as a business, this approach leaves businesses and individuals exchanging in goods and other services to their own devices.

---

<sup>96</sup> See, e.g., Constantin, *supra* note 7; Popper & Abrams, *supra* note 7.

<sup>97</sup> BRITO & CASTILLO, *supra* note 10, at 10, 13–16.

<sup>98</sup> FinCEN Hearing, *supra* note 11, at 2, 8, 10–11.

<sup>99</sup> Lawrence, *supra* note 36, at 1.

<sup>100</sup> See THE GUIDANCE, *supra* note 12, at 3.

<sup>101</sup> See, e.g., *Top 10 Most-Used Currencies in the World*, CHINA DAILY, [http://www.chinadaily.com.cn/business/2014-03/03/content\\_17316095.htm](http://www.chinadaily.com.cn/business/2014-03/03/content_17316095.htm) (last updated Mar. 3, 2014).

<sup>102</sup> 31 C.F.R. §§ 1010.312, 1022.320(a)(2). MSBs required to report transactions of \$2,000 or more. *Id.*

## B. Redefining FinCEN's "User" Definition

### 1. FinCEN's Clarification

#### (i) Uncertainty Surrounding Who Qualifies as a "User"

¶37 The definition of "user" from FinCEN's initial Guidance creates uncertainty among Bitcoin participants who do not clearly fit the definition. Although FinCEN's administrative rulings have since partially fleshed out the Guidance's ambiguity, discussing the initial confusion helps illustrate the issues that prompted the administrative rulings and highlights the remaining problems despite those rulings.<sup>103</sup>

¶38 FinCEN's initial definition of a "user" was too restrictive and overly vague,<sup>104</sup> omitting myriad individuals who do not "obtain virtual currency to purchase goods or services." For instance, people may use bitcoins for remittances, as gifts of money to friends or family for ordinary activities, or for charitable donations.<sup>105</sup> Some users simply collect them as a hobby. Further, the Guidance's user definition excluded businesses selling goods or services in exchange for bitcoins and entities investing in bitcoins as a currency. And because these groups do not exchange virtual currency for real currency, none qualifies as an "exchanger." These discrepancies raised an important question: If a group does not fall squarely within either definition—that of "user" or "exchanger"—what regulatory obligations apply? Notwithstanding FinCEN's subsequent administrative rulings, this question remains unanswered for various parties.

¶39 The opacity of the Guidance's virtual-currency framework had already created confusion before FinCEN rendered its administrative rulings.<sup>106</sup> In early January 2014, FinCEN exacerbated this apprehension when it mailed letters to Bitcoin businesses alleging they might qualify as money transmitters, thereby mandating compliance with certain federal regulations.<sup>107</sup> FinCEN argued that these letters were merely a form of "industry outreach" meant to alert Bitcoin businesses that certain commercial acts could subject them to federal anti-money-laundering requirements.<sup>108</sup> Regardless of FinCEN's intent, the letters nevertheless had a chilling effect on these businesses, many of which continue to refute their MSB-status.<sup>109</sup>

#### (ii) FinCEN's Administrative Rulings

¶40 In an effort to clear up this uncertainty, FinCEN released two administrative rulings that elaborate on the "user" definition.<sup>110</sup> In response to a software company's inquiry, the first ruling (the Investment Ruling) confronts the issue of whether certain investment activities in virtual currency deem one an MSB under the BSA.<sup>111</sup> FinCEN explained that

---

<sup>103</sup> See INVESTMENT RULING, *supra* note 93, at 3–4; MINING RULING, *supra* note 93, at 2–3.

<sup>104</sup> See THE GUIDANCE, *supra* note 12, at 2.

<sup>105</sup> Those using bitcoins in this way are hereinafter collectively referred to as "money-givers."

<sup>106</sup> See *Chilling Effect*, *supra* note 94.

<sup>107</sup> *Id.*

<sup>108</sup> *Id.*

<sup>109</sup> *Id.*

<sup>110</sup> INVESTMENT RULING, *supra* note 93, at 3–4; MINING RULING, *supra* note 93, at 2–3.

<sup>111</sup> INVESTMENT RULING, *supra* note 93, at 3–4.

in determining whether someone qualifies as an MSB, what matters is “not the mechanism by which [the] person obtains the convertible virtual currency, but what the person uses the convertible virtual currency for, and for whose benefit.”<sup>112</sup> Operating under this revised framework, FinCEN redefined the Guidance’s prior “user” definition to include anyone who uses virtual currency for that user’s sole benefit.<sup>113</sup> Thus, persons who use bitcoins exclusively for their own account (e.g., buying goods, personal investment), and not for the benefit of others (e.g., investing on another’s behalf), qualify as users.<sup>114</sup>

¶41 The Investment Ruling successfully resolves several questions that the Guidance initially left unanswered. It clarifies that Bitcoin investors qualify as users if they benefit from their virtual-currency transactions solely on their own account. In this same vein, FinCEN relied upon its revised user definition to classify the software company—a business selling goods—as a user because it solely benefited from the virtual currency’s use. However, even if the benefit-focused inquiry had deemed the company an MSB, the company nevertheless may have qualified for a BSA exemption that excludes businesses primarily selling goods and services from MSB regulation.<sup>115</sup> In fact, the Investment Ruling suggests that a company selling goods or services will likely avoid MSB regulation in most instances.<sup>116</sup> Finally, Bitcoin enthusiasts—individuals who hold bitcoins as a hobby—fall outside the benefit-focused inquiry entirely because they refrain from actually using the currency, thus negating any potential MSB designation.<sup>117</sup>

¶42 FinCEN’s second administrative ruling (the Mining Ruling) reinforces the validity of the benefit-focused inquiry.<sup>118</sup> FinCEN issued the Mining Ruling in response to a Bitcoin-mining company’s concerns about whether it would be considered an MSB for using bitcoins to purchase goods and services, converting bitcoins into real currency to buy goods and services, or transferring bitcoins to the owner of the company.<sup>119</sup> FinCEN explained that, as long as the company only used mined bitcoins for the company’s own benefit, the company did not qualify as an MSB.<sup>120</sup> In contrast, if the company were to use bitcoins for the benefit of another, it would qualify as a money transmitter. Again, FinCEN looked not to how the party acquired the bitcoins, but rather to who benefited from its use. Similar to the Investment Ruling, the Mining Ruling’s analysis appears to rely almost exclusively upon the bright-line test focusing on the beneficial use of virtual currency.

¶43 Yet it remains unclear how remittance users and money-givers fit FinCEN’s user definition. Unlike Bitcoin enthusiasts who refrain from spending bitcoins, remittance users and money-givers actually use virtual currency, subjecting them to the benefit-focused inquiry. And because both groups use bitcoins to benefit others, neither seemingly qualifies as a user according to FinCEN’s definition. This creates the

---

<sup>112</sup> *Id.* at 3.

<sup>113</sup> THE GUIDANCE, *supra* note 12, at 1; INVESTMENT RULING, *supra* note 93, at 4.

<sup>114</sup> THE GUIDANCE, *supra* note 12, at 1; INVESTMENT RULING, *supra* note 93, at 4.

<sup>115</sup> INVESTMENT RULING, *supra* note 93, at 4 n.10.

<sup>116</sup> *Id.* at 4.

<sup>117</sup> INVESTMENT RULING, *supra* note 93, at 4.

<sup>118</sup> See MINING RULING, *supra* note 93, at 1. FinCEN issued the MINING RULING and the INVESTMENT RULING on the same day. *Id.*

<sup>119</sup> *Id.*

<sup>120</sup> *Id.* at 3.

possibility of a third nebulous category of Bitcoin participants who qualify neither as users nor as exchangers.

## 2. Continuing Uncertainty

¶44 The remaining confusion regarding money-givers and remittance users ultimately exists because of the Investment Ruling’s unclear definition of “user” within the context of the BSA’s money-transmitter regime, which makes no mention of the “for one’s own benefit” definition.<sup>121</sup> The incongruity between FinCEN’s virtual-currency framework and the BSA creates the possibility of a third category of Bitcoin participants that fall into a regulatory grey area.

¶45 One could argue, however, that FinCEN’s application of the BSA to virtual currency does in fact align with the BSA’s money-transmitter regime and fully accounts for this undefined category. This argument is predicated upon the assumption that three categories of persons, aside from administrators, exist in Bitcoin: users, exchangers, and users not using bitcoins for their own benefit. Under this interpretation, FinCEN would deem parties in the last category money transmitters; however, the BSA would accommodate these persons because anyone falling into this third category qualifies for an exemption.<sup>122</sup> For example, money-givers and remittance users<sup>123</sup> likely qualify for the exemption that excludes from MSB regulation natural persons engaging in money-transmission services not-for-profit on an infrequent basis.<sup>124</sup> If this interpretation were correct, determining how to treat members of this third category becomes less problematic. Because FinCEN consistently refers to the BSA’s money-transmitter regime as the rationale behind both the Guidance and its administrative rulings, this argument appears seemingly valid.<sup>125</sup>

¶46 Yet uncertainty remains. Regardless of the former interpretation’s apparent soundness, one could argue that a second interpretation, classifying members of the undefined category as money transmitters subject to MSB regulation, is nevertheless possible—perhaps, even likely. This alternative interpretation requires that only two categories exist: users and exchangers. Under this interpretation, FinCEN would consider an individual using bitcoins not for his sole benefit a money transmitter; however, unlike the first interpretation, no pertinent BSA exemption would apply.

¶47 These interpretations diverge on FinCEN’s possible treatment of the BSA’s money-transmitter exemptions. The first interpretation assumes that FinCEN intends for the BSA exemptions to apply to virtual currencies the same way the exemptions apply to other currencies. The second interpretation, accounting for the implication that an individual using bitcoins for the benefit of another qualifies as a money transmitter,<sup>126</sup> assumes that

<sup>121</sup> *Id.*; see 31 C.F.R. § 1010.100(ff)(5).

<sup>122</sup> See, e.g., 31 C.F.R. § 1010.100(ff)(8)(iii).

<sup>123</sup> A money-remittance facilitator is an example of someone who would not fall under the natural-person exemption. While this person would be facilitating money-remittances on a not-for-profit basis, he may be doing so on a not-infrequent basis. *Id.*

<sup>124</sup> 31 C.F.R. § 1010.100(ff)(8)(iii).

<sup>125</sup> See THE GUIDANCE, *supra* note 12, at 1–3; INVESTMENT RULING, *supra* note 93, at 3–4; MINING RULING, *supra* note 93, at 1–3.

<sup>126</sup> See MINING RULING, *supra* note 93, at 3; INVESTMENT RULING, *supra* note 93, at 4.

FinCEN does not intend for the BSA exemptions to apply equally to all virtual-currency users.

¶48 In fact, when understood together, FinCEN’s administrative rulings and Guidance likely support the second interpretation. Specifically, FinCEN’s analysis suggests that the BSA exemptions apply solely to exchangers. The Guidance identifies the BSA’s business exemption exclusively for exchangers, which exempts from MSB regulation a company that accepts and transmits funds essential only to the sale of goods or services, and never mentions the natural-persons limitation for users.<sup>127</sup> Without more, one could argue that this exclusion was inadvertent, resulting perhaps from the Guidance’s original user definition that categorically barred users from MSB designation regardless of exemptions.<sup>128</sup> But FinCEN abandons this all-encompassing user category in the administrative rulings, instead redefining a user as a person who uses virtual currency to purchase goods or services for the user’s sole benefit. Although given the opportunity, FinCEN’s administrative rulings continue to identify only the BSA’s business exemption, neglecting any discussion of potential BSA exemptions applicable to users.<sup>129</sup> Given this consistent omission, FinCEN may not have intended for any BSA exemptions to apply for users.<sup>130</sup> While one would expect FinCEN to apply these exemptions in light of its revised “user” definition, it failed to provide a critical explanation of this potential applicability for unknown reasons.

¶49 Instead, the administrative rulings provide support for the second interpretation. Both rulings repeatedly emphasize that only a person using bitcoins for his sole benefit avoids MSB designation, thus implying that using bitcoins for the benefit of another subjects a person to MSB regulation.<sup>131</sup> If FinCEN were to adopt this second interpretation, remittance users and money-givers would qualify as money transmitters subject to MSB regulation.

¶50 In sum, the administrative rulings pinpoint the conflict between FinCEN’s user definition and the BSA’s money-transmitter regime, and specifically, the lack of clarity for when BSA exemptions might apply. For instance, a money-giver likely falls under the BSA exemption for natural persons transmitting money not-for-profit.<sup>132</sup> Simultaneously, however, the money-giver is not using bitcoins for his own benefit, thus making him an

---

<sup>127</sup> THE GUIDANCE, *supra* note 12, at 2 n.9 (referring only to 31 C.F.R. § 1010.100 (ff)(1–7), excluding 31 C.F.R. § 1010.100 (ff)(8), which provides for the BSA’s natural-persons exemption). The BSA business exemption excludes a person who “[a]ccepts and transmits funds only integral to the sale of goods or the provision of services, other than money transmission services, by the person who is accepting and transmitting the funds.” 31 C.F.R. § 1010.100 (ff)(5)(ii)(F).

<sup>128</sup> See INVESTMENT RULING, *supra* note 93, at 4 n.10.

<sup>129</sup> See THE GUIDANCE, *supra* note 12, at 1. One could argue that FinCEN did not intend the BSA exemptions to apply to users because it asserted in THE GUIDANCE that users were categorically not money transmitters, and thus there was no need to mention the BSA exemptions. *Id.* In the two administrative rulings, however, FinCEN abandons this categorical exemption, and instead qualifies that a user who obtains virtual currency and buys goods with it (for his own benefit) is not an MSB (one can understand this third nebulous category of persons as being users who are protected). See MINING RULING, *supra* note 93, at 2; INVESTMENT RULING, *supra* note 93, at 3; THE GUIDANCE, *supra* note 12, at 1. Moreover, FinCEN, in both of its administrative rulings, does not assert that all of the BSA exemptions apply to users, as it continues to do for exchangers. INVESTMENT RULING, *supra* note 93, at 3; MINING RULING, *supra* note 93, at 2.

<sup>130</sup> See 31 C.F.R. § 1010.100(ff)(8)(iii).

<sup>131</sup> See MINING RULING, *supra* note 93, at 3; INVESTMENT RULING, *supra* note 93, at 4.

<sup>132</sup> 31 C.F.R. § 1010.100(ff)(8)(iii).

MSB under FinCEN's definition. Notwithstanding the merits of either argument, it is the uncertainty that vexes Bitcoin users. Until FinCEN explicitly adopts an unambiguous interpretation, many money-givers and remittance users will opt to use Bitcoin anonymously or avoid it entirely, not wanting to trigger MSB regulation.

### 3. FinCEN's Definition of User Should Be Replaced

¶51 FinCEN should modify its "user" definition. As it stands, the definition is too ambiguous under the first interpretation and too restrictive under the second interpretation.<sup>133</sup> Substantively, the first interpretation comports with a viable regulatory framework. But ambiguity breeds doubt. In turn, this doubt allows alternative interpretations to abound. And while the second interpretation provides the necessary clarity, it subjects remittance users and money-givers to costly BSA regulation, quashing a legitimate use of Bitcoin without producing any concomitant benefits. Deeming money-givers to be money-transmitters equates to requiring parents to register with FinCEN if they wish to give their children cash to go shopping. Under either interpretation's current state, Bitcoin's potential unrealized value for certain users is likely to remain exactly that—unrealized.

¶52 MSB compliance requires time, money, and expertise, which affect those with the fewest resources disproportionately. Thus, the second interpretation's regulatory burden would likely harm remittance users and money-givers more so than anyone else, penalizing one of the most beneficial noncriminal uses of Bitcoin.<sup>134</sup> Moreover, even for those capable of shouldering the additional expense, compliance nevertheless increases transaction costs, decreases Bitcoin liquidity, and ultimately hinders the development of a virtual currency with recognized benefits.

¶53 If the first interpretation wins the day, however, many of these adverse policy consequences disappear. Specifically, under the first interpretation, the BSA natural-persons exemption applies to both money-givers and remittance users operating on a not-for-profit and infrequent basis, thus negating the detriments of costly regulation for these legitimate bitcoin users.<sup>135</sup> In the end, the first interpretation's only limitation comes down to whether it is the correct interpretation in the eyes of the pertinent regulators, which is unclear. FinCEN has only exacerbated this lack of clarity. This Article's proposed solution ameliorates this confusion.

### 4. Redefining FinCEN's Definition of User

¶54 Redefining the Guidance's "user" definition as "a possessor of a bitcoin that is neither an exchanger nor an administrator" provides the optimal solution. Further, clarifying that federal regulators do not consider persons acting in their capacities as users to be money transmitters likewise mitigates any trepidation. In tandem, both

---

<sup>133</sup> Recall that the second interpretation finds persons who do not fall within the exchanger and user categories as money transmitters while the first interpretation does not.

<sup>134</sup> See *Suspicious Activity and Currency Transaction Reports: Balancing Law Enforcement Utility and Regulatory Requirements: Hearing Before the Subcomm. on Oversight and Investigations of the H. Comm. on Fin. Servs.*, 110th Cong. 84 (2007) [hereinafter *Suspicious Activity Hearing*] (statement of Steve Bartlett, Fin. Servs. Roundtable).

<sup>135</sup> See 31 C.F.R. § 1010.100(ff)(8)(iii).

simplify and clarify how persons using bitcoins are to be treated. The term “user” thus becomes a catchall category for every person holding a bitcoin that is not an exchanger. In turn, the exchanger category becomes the only group subject to MSB regulation. Simply stated, if a person is not an exchanger, then that person is not a money transmitter. This solution provides Bitcoin users certainty as to their applicable regulatory status.

¶55 This solution also aligns with the existing BSA money-transmitter regulatory regime. The definitions of exchanger and money transmitter are very similar, both focusing on a person exchanging currency for currency.<sup>136</sup> Moreover, the exchanger definition and the BSA’s money-transmitter definition are analogous in that both were drafted in an effort to achieve the same anti-money-laundering goals, the primary difference being that the former applies to virtual currencies. Finally, redefining the “exchanger” definition as someone in the business of exchanging currency “from one person to another person or location” provides consistency and further clarity. In sum, these revisions provide an intelligible, bright-line test for determining MSB-status, aligning FinCEN’s virtual-currency framework with the BSA’s regulatory regime.

### C. *Alternative Solution: Treating All Miners as Money Transmitters*

¶56 In contrast to this refined-standard approach, one could argue that simply designating all miners as money transmitters by fiat is more effective. Proponents of this approach likely identify a number of potential benefits, specifically its prophylactic nature meant to prevent widespread money laundering in Bitcoin. This section argues that this over-inclusive designation would be both ineffective in combating money laundering and deleterious to beneficial innovation. Regulating Bitcoin requires a scalpel, not a cudgel.

#### 1. Mining as a Money-Laundering Technique Poses Little Threat

¶57 First, one might argue that although the mining process does not inherently implicate money-laundering concerns, lucrative transaction fees for miners willing to verify fraudulent transactions might incentivize criminal behavior.<sup>137</sup> Thus, because of this potentially adverse incentive, authorities should designate miners as money transmitters subject to MSB regulation. This scenario is illustrated best via hypothetical.

¶58 Money laundering vis-à-vis the mining process occurs when a criminal miner—in this case, Mike—and two other criminals, Charles and David, stage a transaction. Charles and David first enter into an ordinary transaction, where Charles gives David one bitcoin. Then, Charles and David give Mike a specific amount of bitcoins in transaction fees. However, Charles and David purchased these bitcoins with “dirty money,” or money acquired through criminal means, which must be laundered to avoid detection. Mike verifies the transaction along with other bitcoin transactions made between noncriminal parties who similarly provide Mike transaction fees but with “clean money,” or money untainted by criminal activity. Finally, Mike returns to Charles and David the original

<sup>136</sup> See THE GUIDANCE, *supra* note 12, at 2; 31 C.F.R. § 1010.100(ff)(5)(i).

<sup>137</sup> See *Bitcoin FAQ*, *supra* note 3 (discussing transaction fees under the “How does Bitcoin mining work?” heading).

amount in clean bitcoins received from the noncriminal parties, thus allowing Charles and David to spend their criminal proceeds without fear of detection.

¶159 But does designating all miners as money transmitters prevent this kind of money laundering? Most likely, it does not. In fact, a valid counterargument to the designation by fiat approach is that such a declaration is superfluous. In the above hypothetical, Mike's actions qualify him as an exchanger because he is exchanging virtual currency for the same kind of currency—dirty bitcoins for clean bitcoins—and is doing so as a business. Further, all the parties are knowingly attempting to hide income gained from unlawful activity, which the BSA explicitly forbids.<sup>138</sup> Therefore, notwithstanding the miner's original non-MSB status, the miner's actions nevertheless qualify him as an exchanger subject to MSB regulation. In the end, all parties are guilty of money laundering, based not on their status, but on their knowingly fraudulent actions.

¶160 Moreover, the realistic unlikelihood of successfully laundering money in this manner diminishes the actual threat posed. Importantly, a criminal wishing to launder money cannot select a co-conspirator miner to verify the fraudulent transaction.<sup>139</sup> Instead, various miners compete to verify the transaction.<sup>140</sup> Criminal miners must therefore outperform other miners to verify the criminal transaction; otherwise, the criminal miner is unable to receive the transaction fees provided by his co-conspirators. These fees, which stem from criminal proceeds, thus end up in the hands of an unknown miner, effectively vanquishing a criminal's ability to benefit from his ill-gotten gains. The low probability of a criminal miner outperforming other miners for a single transaction sufficiently deters such activity, especially in light of increased competition from sophisticated mining companies.

¶161 Yet notwithstanding these claims, the argument remains that the designation by fiat approach nevertheless provides some ancillary benefits, however slight. For instance, this over-inclusive designation would likely increase transparency throughout the Bitcoin network by subjecting more actors to the requisite BSA reporting requirements. In turn, this increased systemic transparency would make it more difficult for nefarious activity to flourish in Bitcoin, regardless of whether such improper conduct involves money laundering. Thus, this prophylactic approach focuses not on the ultimate goal of preventing money laundering in Bitcoin, but rather on the simplicity of streamlining Bitcoin regulation. One must therefore determine whether the ancillary benefits of this streamlined regulation outweigh the potential value of a narrower and more complex approach tailored specifically to money-laundering prevention. Keeping in mind the myriad recognized benefits of Bitcoin, the appeal of regulatory simplicity must be tempered with an honest evaluation of the likely costs imposed.

## 2. An Ultimately Ineffective Approach

¶162 From a purely regulatory standpoint, at first blush, treating all miners as money transmitters appears to diminish the specter of money laundering in Bitcoin substantially. For instance, if miners were subject to the BSA recording requirements, miners would

---

<sup>138</sup> See 18 U.S.C. § 1956(a)(1)(B)(i) (2012).

<sup>139</sup> *Bitcoin FAQ*, *supra* note 3 (discussing how Bitcoin mining is a competitive business under the “How does Bitcoin mining work?” heading).

<sup>140</sup> See *id.*

have to ascertain the identities of customers—the parties to the transactions miners verify—and disclose those identities upon government request or statutory mandate.<sup>141</sup> Compliance with the reporting requirements would thus eliminate anonymity in the network because miners must verify all transactions.

¶163 The miner-verification process is critical. As noted previously, Bitcoin mitigates the threat of double spending through miner verification.<sup>142</sup> Without verification, determining instances of double spending in the network becomes impossible, causing confidence in the system to quickly collapse. And because of the necessity of miner verification, designating miners as money transmitters would require all bitcoin users to divulge identifying information to transact in bitcoins. From this, law enforcement could identify suspicious transactions and ascertain the personal identities from the public addresses involved in these transactions. Therefore, on its face, categorically designating miners as MSBs provides a panacea to the money-laundering problem. This method, however, not only overregulates Bitcoin, but also inevitably fails.

¶164 This regulatory approach disrupts Bitcoin’s decentralized ecosystem, imposing high barriers to entry for miners. Complying with MSB regulation is costly,<sup>143</sup> perhaps prohibitively so for miners operating alone, which thus entrenches only those wealthy enough to afford the increased costs.<sup>144</sup> Given the need for the bitcoin-verification process, this solution will likely force miners to centralize, further increasing large mining companies’ share of the bitcoin-verification market. In turn, less competition imposes fewer market constraints, increasing the cost of miner verification, or worse, encouraging an oligopoly to develop between the largest mining companies in an effort to fix prices. Large transaction fees, once voluntary, will become mandatory and commonplace. In the end, these expensive transactions fees will deter many users, thus reducing the liquidity of Bitcoin and hindering the currency’s development.

¶165 In the current system, miner competition perpetuates the decentralized nature of the network and its attendant benefits. For instance, miners can prevent an oligopoly from forming by undercutting the larger mining companies’ transaction-fee requirements. This is possible because the current cost of mining includes only the cost of a computer and any expenses stemming from the computing power (electricity costs) necessary to mine proficiently.<sup>145</sup> Although users cannot choose which miners verify their transactions, users are ultimately responsible for setting transaction-fee amounts. Thus, if a large mining company deems a transaction fee insufficient, it will likely refuse to compete for this transaction, thereby leaving the proceeds to other miners more willing to pursue less profitable endeavors.<sup>146</sup> Moreover, these passed-over transactions incentivize miners employed by large mining companies to start their own mining ventures. This increases the number of potential verifiers, creating a more competitive market for verification

---

<sup>141</sup> 31 C.F.R. § 1010.312; SAR, *supra* note 71, at 2.

<sup>142</sup> See NAKAMOTO, *supra* note 18, at 1.

<sup>143</sup> See *Suspicious Activity Hearing*, *supra* note 134.

<sup>144</sup> See *cf.* TANYA D. MARSH & JOSEPH W. NORMAN, REFORMING THE REGULATION OF COMMUNITY BANKS AFTER DODD-FRANK 2 (2013) (“A \$165 million bank is less able to absorb regulatory burden than a \$2 trillion bank. By imposing unnecessary regulations on smaller institutions, we are awarding the larger banks a further competitive advantage.”).

<sup>145</sup> Vance & Stone, *supra* note 57.

<sup>146</sup> See *Bitcoin FAQ*, *supra* note 3 (noting that miners choose which transactions to verify, thus negating a user’s ability to influence the selection of miners).

fees. In sum, voluntary transaction fees and low overhead facilitate competition, which both increases liquidity and prompts the network's growth.

¶166 Finally, notwithstanding these prior arguments, the biggest obstacle for this over-inclusive approach remains—anonymity. Miners, like users, can always use Tor to remain anonymous.<sup>147</sup> Consequently, noncompliant miners may still mine on their own, or in anonymous groups, but more discreetly. As discussed *supra* Part IV(A), because of the challenges posed by anonymity, a heavy-handed regulatory approach likely affects only those parties willing to submit to regulation, which clearly excludes money launderers. While authorities might eventually find a way to eliminate this anonymity, as both the law and technology currently stands, sophisticated parties wishing to conceal their identities are able to do so with relative ease.<sup>148</sup>

## V. THE BENEFITS AND LIMITATIONS OF APPLYING THE REFINED FINCEN STANDARD

¶167 So far, this Article has primarily focused on revising the FinCEN standards in the abstract. Part V turns to the concrete results that likely derive from the proposed refined standard's application to particular bitcoin-using institutions. This application illustrates the refined standard's benefits—detering money laundering and fostering Bitcoin's benefits—and highlights the inherent limitations to Bitcoin regulation. This section first applies the refined standard to the largest and most easily identifiable entities in Bitcoin. A similar analysis follows, but applies the refined standard to Bitcoin's smaller and more secretive entities. Generally, the smaller and more secretive the entity, the more difficult it is to enforce the refined definition because these entities most easily remain anonymous. This Article concludes that Bitcoin currency exchanges provide the optimal target for anti-money-laundering laws, followed closely by other easily identifiable businesses.

### A. *Applying the Refined FinCEN Standard to Currency Exchanges*

#### 1. Easily Identifiable Currency Exchanges

¶168 Bitcoin currency exchanges, such as BitStamp, CoinCafe, and Coinbase, are easily identifiable institutions with readily detectable headquarters.<sup>149</sup> Further, these currency exchanges clearly qualify as exchangers under both the Guidance and this Article's

---

<sup>147</sup> Lawrence, *supra* note 36, at 1.

<sup>148</sup> Although labeling all miners as money transmitters is misguided, indirectly regulating miners might be a viable solution. See Vance & Stone, *supra* note 57. Businesses selling “mining rigs,” or computers designed specifically to mine bitcoins, provide a means of achieving this indirect regulatory approach. See *id.* FinCEN could construct a licensing scheme where purchasers of these rigs would be required to provide identifying information to the government upon purchase, thereby enabling the government to track the purchaser's activity in the public ledger. This solution would not only give the government more data to detect money laundering, but also would avoid over-regulating Bitcoin. These miners would only have to provide identifying information, and would not have to comply with any other costly regulation. Although this solution will likely cause certain miners to customize their rigs to remain unidentified, it would nevertheless help identify miners engaging in unlicensed money transmission and money laundering.

<sup>149</sup> *About Us*, BITSTAMP, [https://www.bitstamp.net/about\\_us/](https://www.bitstamp.net/about_us/) (last visited Mar. 29, 2014); *Contact Us*, COIN CAFÉ, <https://coincafe.com/contactus.php> (last visited Oct. 29, 2014); *About Coinbase*, COINBASE, <https://coinbase.com/about> (last visited Mar. 29, 2014).

refined standard thereof. All of these currency exchanges are in the business of exchanging bitcoins for other currency, and therefore, are subject to MSB regulation.<sup>150</sup>

¶169 Regulating virtual-currency exchanges deters money laundering in myriad ways. First, these exchanges must reveal the identity of customers engaging in certain transactions pursuant to the BSA's reporting requirements.<sup>151</sup> Normally, currency exchanges can easily provide identifying information stored in "online wallets," which create and store all of their customers' public and private keys.<sup>152</sup> Some currency exchanges even require identifying information from a customer before providing him with these keys,<sup>153</sup> thus granting the government access to the identity of anyone who receives \$10,000 or more through these Bitcoin exchanges.<sup>154</sup> Because currency exchanges are the gatekeepers to real currency, customer identification requirements make it much more difficult for a money launderer to get his money out of Bitcoin. This consequence is especially salient for U.S. regulators because most criminals attempting to launder money wish to convert bitcoins to USD due to its widespread use.<sup>155</sup>

¶170 But at first blush, this threshold requirement appears rife for circumvention. For instance, it seems criminals could easily bypass the \$10,000 requirement by engaging in multiple transactions individually below the limit, but that surpass the \$10,000 threshold as a whole.<sup>156</sup> This tactic, defined and criminalized as "structuring," exists in real-currency markets and creates sometimes-insurmountable obstacles for law enforcement.<sup>157</sup> But the Bitcoin network actually mitigates these difficulties. In fact, law enforcement likely prefers when money launderers attempt to "structure" bitcoin transactions because the public ledger allows one to track not only transactions made through the specific currency exchange, but also all of a user's previous transactions in the network, thus permitting authorities to identify repeat offenders more readily.

## 2. Secretive Currency Exchanges

¶171 For large and easily identifiable exchanges, the refined FinCEN standard's enforcement benefits are clear. However, enforcement becomes more difficult for currency exchanges that intentionally obscure user identities. For example, an individual might run an exchange using several public addresses from different Bitcoin wallets to make pinpointing a single identity for these addresses incredibly difficult, especially if she uses Tor to conceal her IP address.

¶172 But anonymity also imposes costs on the currency-exchange owner. For instance, this opacity might prompt reputational concerns for potential customers. After all, many users—legitimate or not—might balk at transferring currency to an untraceable, and

---

<sup>150</sup> See THE GUIDANCE, *supra* note 12, at 2.

<sup>151</sup> See 31 C.F.R. § 1010.312 (2011); SAR, *supra* note 71, at 2.

<sup>152</sup> *How to Store Your Bitcoins*, COINDESK, <http://www.coindesk.com/information/how-to-store-your-bitcoins/> (last updated July 22, 2014); Philip Raymond, *Bitcoin Wallets: How to Protect Your Digital Currency*, NAKED SECURITY (Jan. 23, 2014), <http://nakedsecurity.sophos.com/2014/01/23/bitcoin-wallets-how-to-protect-your-digital-currency/>.

<sup>153</sup> See Raymond, *supra* note 152; see also *How to Buy Bitcoin*, COINBASE, <https://coinbase.com/buy-bitcoin> (last visited Mar. 29, 2014) (requiring customers to add a bank account).

<sup>154</sup> 31 C.F.R. § 1010.312 (2011).

<sup>155</sup> See *Top 10 Most-Used Currencies in the World*, *supra* note 101.

<sup>156</sup> See *id.*

<sup>157</sup> 31 C.F.R. §§ 1010.100(xx), 1010.314(c) (2011).

therefore unaccountable, entity. Moreover, anonymity conceals the currency-exchange owner not only from law enforcement, but also from Bitcoin users, which limits options for building and maintaining a customer base. Perhaps, she could alert her customers through Internet forums which public addresses she will use to exchange bitcoins for real currency, allowing her to evade detection by creating new public addresses frequently. On the other hand, she could risk consistently using one easily identifiable public address, or a set of thereof, for customers to locate her, relying solely on Tor's effectiveness to elude the authorities. Either way, law enforcement would be able to determine the total amount of bitcoins the public addresses receive by tracing transaction histories, but would be unable to ascertain the currency-exchange owner's identity, or group of identities, because of Tor.<sup>158</sup>

¶73 While this anonymity problem poses challenges for law enforcement in the near term, money laundering in Bitcoin usually bleeds outside of the virtual network eventually. If the owner converts her bitcoins into USD at another Bitcoin currency exchange—which is the most likely scenario—the exchange will require her to provide identifying information for transactions pursuant to CTR and SAR requirements,<sup>159</sup> thus leaving a trail outside of Bitcoin for law enforcement to follow. In the end, money laundering in Bitcoin requires real currency from individuals operating outside the network. Similar to any other criminal attempting to avoid detection, at a certain point, the currency-exchange owner must launder her money in a more traditional fashion, which raises the same red flags typically associated with cash-based money laundering.<sup>160</sup>

#### B. *Applying the Refined FinCEN Standard to Businesses*

¶74 If a business exchanges bitcoins for real or other virtual currency as its primary means of garnering a profit, both the Guidance and the refined FinCEN standard readily deem the business an exchanger.<sup>161</sup> On the other hand, if the business primarily sells goods or services, neither exchanger definition likely fits because the company is not predominantly exchanging currency as a business. But this question becomes more difficult for investment companies, specifically whether certain money-transmission activities are integral to their investment services. Footnote 10 in the Investment Ruling addresses this scenario, noting that investment companies that transmit money could qualify for the BSA's business exemption if the company's money-transmitting services are not integral to its business.<sup>162</sup> On this point, the refined standard differs from the Investment Ruling only in that the non-integral money-transmission services need not be for the company's sole benefit.

¶75 Importantly, the refined standard does not preclude the regulation of non-money-transmitting Bitcoin businesses. In fact, a dual approach regulating both Bitcoin-focused enterprises and virtual-currency exchanges would potentially create synergies providing an optimal balance between competing interests. For instance, FinCEN could adopt New

---

<sup>158</sup> See Nielsen, *supra* note 16 (noting that all transactions are traceable to public addresses under the "How anonymous is Bitcoin?" heading).

<sup>159</sup> See 31 C.F.R. § 1010.312 (2011); SAR, *supra* note 71, at 2.

<sup>160</sup> See 18 U.S.C. § 1960(a) (2012).

<sup>161</sup> See THE GUIDANCE, *supra* note 12, at 2.

<sup>162</sup> INVESTMENT RULING, *supra* note 93, at 4 n.10.

York’s proposed idea to issue “Bitlicenses” to businesses utilizing virtual currency.<sup>163</sup> Combined with the refined standard’s regulation of currency exchanges, this scheme would create an effective money-laundering-prevention system by focusing solely on customer identification requirements. Under this arrangement, businesses would be required to identify their customers and conduct business only with public addresses from a Bitcoin currency-exchange wallet. Before completing a transaction, a business would have to confirm the customer’s identity by asking the exchange to verify that the public address matches the identifying information.

¶76 This licensing scheme, though, would be vulnerable to abuse in that a criminal posing as a business could request identifying information from a virtual-currency exchange to determine the identity of a target for a fraud or theft. Coupled with the fact that the public ledger reveals the amount of bitcoins a user possesses, thieves would be able to determine the wealthiest targets, further increasing the incentive for criminal behavior.<sup>164</sup> Therefore, exchanges would likely have to develop safeguards to ensure disclosure only to legitimate businesses. The easiest way to accomplish this would be if FinCEN assigned a unique code to Bitlicense-holding businesses that currency exchanges could verify with FinCEN upon a request for information.

¶77 Of course, regulators should evaluate and reassess this system to avoid overregulating the network, taking into account the costs of security, the net loss of privacy and its effect on user interest in Bitcoin, and the ease of implementation and its attendant costs. If regulators were to deem these concerns negligible and adopt this licensing scheme, incentives to launder money through Bitcoin would diminish significantly because every FinCEN-verified business the launderer transacts with would have his identifying information. Many criminals would thus likely opt for the more traditional route of laundering money through cash-based transactions.

### C. *Applying the Refined FinCEN Standard to Mixers*

¶78 “Mixers” are secretive organizations that typify the most salient impediments for the effective administration of anti-money-laundering laws in Bitcoin. A mixer is an entity that attempts to obscure a customer’s transaction history on the public ledger for a fee, providing an easy way to launder money undetected. Further, a mixer requires many users to subscribe to its services for it to be effective, creating a complex scheme to rid the trail of dirty money.<sup>165</sup> For example, if a bitcoin thief—in this case, Thad—robbed a Bitcoin currency exchange of 100 bitcoins, few people would accept these bitcoins because the public ledger clearly indicates them as stolen. Mixers help solve Thad’s problem. In order to make these bitcoins clean, and thus spendable, Thad transfers his dirty bitcoins to a public address owned by the mixer.<sup>166</sup> The mixer records how many bitcoins it owes Thad,<sup>167</sup> and proceeds to mix the dirty bitcoins with clean bitcoins from

---

<sup>163</sup> Cameron Fuller, *Bit Licenses: How Will New York Regulate Bitcoins?*, INT’L BUS. TIMES (Jan. 30, 2014), <http://www.ibtimes.com/bit-licenses-how-will-new-york-regulate-bitcoins-1552078>.

<sup>164</sup> See Nielsen, *supra* note 16 (noting that every transaction in Bitcoin is publicly viewable under the “How Anonymous is Bitcoin?” heading).

<sup>165</sup> See Adrienne Jeffries, *How to Steal Bitcoin in Three Easy Steps*, THE VERGE (Dec. 19, 2013, 1:10 PM), <http://www.theverge.com/2013/12/19/5183356/how-to-steal-bitcoin-in-three-easy-steps>.

<sup>166</sup> See *id.*

<sup>167</sup> See *id.*

other users belonging to its service, obscuring the dirty bitcoins' transaction histories.<sup>168</sup> The mixer then gives bitcoins to a newly created public address for Thad from the mixer's clean public address, which was unrelated to the mixing process.<sup>169</sup> Lastly, the mixer collects payment for its services and refills its bitcoin reserves by gradually collecting the laundered bitcoins from the public addresses that participated in the mixing process.<sup>170</sup>

¶179 Both the Guidance's exchanger definition and the refined exchanger definition include mixers because mixers are businesses exchanging virtual currency for other virtual currency.<sup>171</sup> Thus, a mixer's failure to register with FinCEN makes it an unlicensed MSB, which is subject to fine or imprisonment.<sup>172</sup> Unfortunately, several factors make enforcing any mixer-focused regulations infeasible. For instance, it is incredibly difficult to track a bitcoin after a mixer has comingled the currency because the once-identifiable bitcoin becomes unrelated to its transaction history.<sup>173</sup> And unsurprisingly, many mixers use Tor, which makes tracking the mixing-service owner challenging as well.<sup>174</sup> Moreover, a mixer operator may also clean his bitcoins through his service, converting bitcoins into real currency, thus receiving the benefit of his proceeds without ever revealing his identity or ownership status. A statement by Bitcoin Fog, a mixing service, illustrates the confidence many mixers exude in remaining untraceable: "[W]e can say with high certainty that not only will we not cooperate with any authorities, the authorities will not actually be able to show up at our doorstep, because finding a [T]or doorstep has proven difficult."<sup>175</sup> Combined with the use of Tor, the fact that mixers only handle bitcoins in their virtual operations makes enforcement near impossible because a mixer's conduct starts and ends online, never exiting the Bitcoin network.

¶180 Nevertheless, one might argue that law enforcement will inevitably discover a way to ascertain the identities of mixer owners using Tor. After all, law enforcement caught Ross Ulbricht, the leader of Silk Road, who used Tor.<sup>176</sup> Simply put, if the authorities can detain and prosecute the mastermind behind the most notorious, illegal bitcoin market, then law enforcement should be capable of discovering a less-sophisticated mixer owner's identity. Silk Road's downfall, however, is not a good measuring stick to gauge the difficulty of uncovering a mixer's identity. Ulbricht made numerous mistakes that most prudent individuals would avoid. For example, he used the same username across drug-user forums to advertise Silk Road and then, using this same username, posted a link to his email account—containing his full name—on a Bitcoin forum to solicit IT

---

<sup>168</sup> See *id.*

<sup>169</sup> See *id.*

<sup>170</sup> See *id.*

<sup>171</sup> THE GUIDANCE, *supra* note 12, at 2; see *supra* Part IV(B).

<sup>172</sup> 18 U.S.C. § 1960(a) (2012).

<sup>173</sup> See Andy Greenberg, *Follow the Bitcoins: How We Got Busted Buying Drugs on Silk Road's Black Market*, FORBES (Sept. 5, 2013, 10:36 AM), <http://www.forbes.com/sites/andygreenberg/2013/09/05/follow-the-bitcoins-how-we-got-busted-buying-drugs-on-silk-roads-black-market/>.

<sup>174</sup> See, e.g., *Accessing Bitcoin Fog*, BITCOIN FOG, <http://www.bitcoinfog.com/> (last visited Mar. 30, 2014); BITCOIN BLENDER, <https://bitcoinblender.wordpress.com/> (last visited Mar. 30, 2014) (noting that the service uses Tor).

<sup>175</sup> *Accessing Bitcoin Fog*, *supra* note 174.

<sup>176</sup> See Hume, *supra* note 8.

professionals.<sup>177</sup> Whether these mistakes resulted from sheer ignorance or unrepentant hubris is unknown; regardless, this brazen conduct is unlikely to be repeated by others. If law enforcement were to use the same methods to find Bitcoin mixers as it used for Silk Road, it would be relying solely on the hope that mixers will make similarly injudicious mistakes.

¶81 This is not to say that Tor users will forever remain beyond the reach of law enforcement. Various parties are developing sophisticated methods for tracking bitcoin transactions, and it is always possible that a government agency will devise an innovative enforcement strategy in the near future.<sup>178</sup> However, these hopeful solutions highlight the difficulty anonymity poses for regulating Bitcoin. The law, as it currently stands, is relatively powerless in its application to these highly secretive organizations. The difficulty of enforcing these laws should therefore prompt policymakers to focus less on these secretive organizations and more on Bitcoin currency exchanges and businesses, which are easier to regulate. This would minimize the benefits of using secretive organizations, at least until enforcement methods become more effective.

## VI. CONCLUSION

¶82 Bitcoin is an emerging technology with many potential beneficial uses.<sup>179</sup> As FinCEN has recognized, these benefits should be cultivated.<sup>180</sup> At the same time, however, FinCEN also acknowledged the potential use of Bitcoin for money laundering and thus the need for regulation.<sup>181</sup> FinCEN's Guidance seemingly attempts to balance these competing interests.<sup>182</sup> As of now, though, this balance appears inadequate.

¶83 FinCEN's Guidance and two administrative rulings present a framework that purports to apply the existing BSA money-transmitter regime. Yet this framework creates needless uncertainty as to who will be treated as an MSB, contradicting FinCEN's assertions that regulations should not stifle Bitcoin's beneficial uses.<sup>183</sup> The aim of this Article's proposed solution—the refined FinCEN standard—is to make FinCEN's Guidance and administrative rulings more closely conform to the existing BSA framework. The revised exchanger definition, which this Article argues should be the only FinCEN category that includes money transmitters, closely resembles the BSA's money-transmitter definition, and thus should be understood as merely an extension of this definition to virtual currency.<sup>184</sup> The revised user and exchanger definitions work together to resolve the existing framework's ambiguity, focusing the inquiry solely on whether a person is an exchanger.

¶84 The refined standard's benefits and limitations are apparent when applied to real-world Bitcoin entities. It is most effective when applied to easily identifiable currency exchanges, where the government can track customer identities through SARs and

---

<sup>177</sup> *Id.*

<sup>178</sup> Joshua Brustein, *Bitcoin May Not Be So Anonymous, After All*, BLOOMBERG BUSINESSWEEK (Aug. 27, 2013), <http://www.businessweek.com/articles/2013-08-27/bitcoin-may-not-be-so-anonymous-after-all>.

<sup>179</sup> See BRITO & CASTILLO, *supra* note 10, at 10, 13–16.

<sup>180</sup> See *FinCEN Hearing*, *supra* note 11, at 2.

<sup>181</sup> *Id.*

<sup>182</sup> See THE GUIDANCE, *supra* note 12, at 1.

<sup>183</sup> *FinCEN Hearing*, *supra* note 11, at 2.

<sup>184</sup> See 31 C.F.R. § 1010.100(ff)(5)(i).

CTRs.<sup>185</sup> The refined standard also effectively applies to easily identifiable businesses that engage in money transmitting. And to the extent these businesses do not fall under the exchanger definition, developing a licensing scheme to combat money laundering might well suffice. However, enforcing the refined standard becomes more problematic for secretive organizations, like mixers, which operate solely within the Bitcoin network and rely on Tor—all in an effort to conceal identities.<sup>186</sup> These organizations will likely continue to exist, at least as long as the Bitcoin network remains, and although the law can deem their activities illegal as unlicensed MSBs, enforcement will continue to be difficult.<sup>187</sup>

¶185 As a result, the refined standard encourages a gatekeeper approach to combat money laundering in Bitcoin, where the gatekeepers between real and virtual currency are the primary subjects of anti-money-laundering regulations. These gatekeepers are the Bitcoin institutions—primarily currency exchanges—that convert bitcoins into real currency. Insofar as these businesses are subject to money-transmission laws under the refined standard, money launderers who want to exchange bitcoins for real currency will be subject to the scrutiny of these institutions. And because most offenders wish to convert bitcoins into real currency,<sup>188</sup> specifically USD, the refined standard should provide an effective anti-money-laundering mechanism for U.S. regulators. Finally, if Bitcoin use becomes more widespread, solutions similar to the licensing scheme suggested *supra* Part V could help further deter money laundering.<sup>189</sup>

¶186 Bitcoin provides myriad benefits, many of which are yet unknown. But it is unclear whether Bitcoin's future will allow for this value to be realized. It could be a large speculative bubble,<sup>190</sup> its current volatility may never cease,<sup>191</sup> or deflation may ruin its viability as a currency.<sup>192</sup> Although these problems should not be taken lightly, Bitcoin's continued persistence in spite of these issues indicates its resiliency. Proper regulation must be implemented to harness this potential. In addition, alternative, decentralized virtual currencies similar to Bitcoin<sup>193</sup> have appeared since Bitcoin's inception.<sup>194</sup> Given the potential benefits of Bitcoin and these virtual currencies, it is not farfetched to think that at least one of these currencies will develop into something truly profound.<sup>195</sup>

---

<sup>185</sup> See 31 C.F.R. § 1010.312; SAR, *supra* note 71, at 2.

<sup>186</sup> Jeffries, *supra* note 165.

<sup>187</sup> See 18 U.S.C. § 1960(a) (2012).

<sup>188</sup> See Kashmir Hill, *21 Things I Learned About Bitcoin from Living on It for a Week*, FORBES (May 9, 2013, 1:54 PM), <http://www.forbes.com/sites/kashmirhill/2013/05/09/25-things-i-learned-about-bitcoin-from-living-on-it-for-a-week/>.

<sup>189</sup> See *supra* Part V(B).

<sup>190</sup> See Jesse Colombo, *Bitcoin May Be Following this Classic Bubble Stages Chart*, FORBES (Dec. 19, 2013, 12:09 PM), <http://www.forbes.com/sites/jessecolombo/2013/12/19/bitcoin-may-be-following-this-classic-bubble-stages-chart/>.

<sup>191</sup> See Toph Tucker, *Bitcoin's Volatility Problem: Why Today's Selloff Won't Be the Last*, BLOOMBERG BUSINESSWEEK (Dec. 5, 2013), <http://www.businessweek.com/articles/2013-12-05/bitcoins-volatility-problem-why-todays-sell-off-wont-be-the-last>.

<sup>192</sup> See Mathew Yglesias, *Bitcoin Will Spiral Up and Down Forever*, SLATE (Apr. 10, 2013, 2:39 PM), [http://www.slate.com/blogs/moneybox/2013/04/10/bitcoin\\_s\\_deflation\\_problem.html](http://www.slate.com/blogs/moneybox/2013/04/10/bitcoin_s_deflation_problem.html).

<sup>193</sup> See *Digital Currencies in the Data Center: Altcoins Explained*, *supra* note 13.

<sup>194</sup> *Crypto-Currency Market Capitalizations*, *supra* note 2.

<sup>195</sup> Although this Article specifically focuses on Bitcoin, the regulatory framework FinCEN promulgated in THE GUIDANCE was intended for all virtual currencies, and thus so too are this Article's proposed refinements. THE GUIDANCE, *supra* note 12, at 1.