

# Legitimizing Cryptocurrencies

## Making the Virtual Economy Work for the United States

Samuel | Dunham



*Brief No. 6.3*

# The Project on International Peace and Security

---

Launched in 2008, the Project on International Peace and Security (PIPS) is an undergraduate think tank based at the College of William and Mary. PIPS represents an innovative approach to undergraduate education that highlights the value of applied liberal arts training to producing the next generation of foreign policy analysts, leaders, and engaged citizens.

PIPS is premised on two core beliefs: (1) rigorous policy-relevant research is a core component of a student's education; and (2) when guided by faculty and members of the foreign policy community, undergraduates can make meaningful contributions to policy debates; their creativity and energy are untapped resources. To this end, PIPS each year selects six research fellows and six research interns. Research fellows identify emerging international security challenges and develop original policy papers. Research interns support the work of the fellows and learn the craft of conducting policy research and writing briefs.

For more on PIPS, visit [www.wm.edu/pips](http://www.wm.edu/pips).

Amy Oakes, Ph.D.

Dennis A. Smith, Ph.D.

Directors

The Project on International Peace and Security © 2014  
All rights reserved.

Please direct inquiries to:

The Project on International Peace and Security (PIPS)  
Institute for the Theory and Practice of International Relations  
The College of William and Mary  
427 Scotland Street  
Williamsburg, Virginia 23185  
tele. 757.221.1441  
fax. 757.221.4650  
pips@wm.edu

Electronic copies of this report are available at [www.wm.edu/pips](http://www.wm.edu/pips)

# Legitimizing Cryptocurrencies

## Making the Virtual Economy Work for the United States

APRIL 2014

Samuel Dunham

# Legitimizing Cryptocurrencies

## Making the Virtual Economy Work for the United States

*Cryptocurrencies, such as Bitcoin, are online currencies not sanctioned or produced by any state entity. These currencies provide a level of anonymity and easy transferability that facilitates money laundering, drug trafficking, and financial crime. Left unregulated, cryptocurrencies constitute a new challenge to states' control over the transfer of illegal funds and foreign exchange markets. To address this challenge, the United States should introduce a new federal-level license for businesses that trade cryptocurrencies for real currencies, which would both encourage the creation of these businesses within the United States and allow for greater government oversight of cryptocurrency transactions.*

### **Introduction**

In 2008, an anonymous figure named Satoshi Nakamoto published a paper outlining a new type of currency called Bitcoin. This new currency, called a cryptocurrency, would exist online, be free from government regulation, have a hard cap on supply, and be freely available to anyone with an internet connection. In 2009, Satoshi Nakamoto mined the first bitcoin.<sup>1</sup>

Bitcoin has since exploded in popularity, becoming the currency of choice for a vast hidden online network of terrorists, drug dealers, and internet pornographers. Criminals and terrorists use cryptocurrencies to launder and transfer money. Drug users and dealers also conduct trades in cryptocurrency to hide illicit purchases. As these new currencies grow in popularity—and value—there is greater potential for them to disrupt the stability of international currency markets.

With proper regulation, however, cryptocurrencies could be a positive economic development. Because of their accessibility and easy transferability, these currencies can reach people underserved by traditional financial markets. Cryptocurrencies also offer potential benefits to the banking industry and could provide transparent records of document and property ownership. This white paper first describes the differences between cryptocurrencies and real currencies. The paper then explains why these differences make unregulated cryptocurrencies threatening. Finally, the paper recommends creating clear standards for online exchanges of cryptocurrency, while also encouraging online entrepreneurs to establish these exchanges in the United States.

## Cryptocurrencies: Virtual, Decentralized, and Semi-anonymous

*What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.*

—Satoshi Nakamoto, Inventor of Bitcoin, 2008

Cryptocurrencies are a “virtual currency,” an online currency not backed by any government. Cryptocurrency users trade coins without any central oversight, while potentially hiding their identity.

- *Virtual currencies.* Virtual currencies exist online and, unlike real currencies, are not backed by states.<sup>2</sup> Some virtual currencies exist within video games, such as Second Life’s Linden Dollars or World of Warcraft’s Gold.<sup>3</sup> Others, such as E-gold and Liberty Reserve, were backed by organizations that tie their value to a limited number of real-world goods.<sup>4</sup> Cryptocurrencies are not backed by any real-world goods or institutions and instead exist only as data on a computer network. They have value because users of the cryptocurrency trust the network to prevent counterfeiting.<sup>5</sup>

Most virtual currencies can be easily transferred anywhere on the globe with an internet connection. For example, E-gold users lived in hundreds of different countries, and only 200,000 of the millions of Liberty Reserve users lived in the United States.<sup>6</sup> Users can also exchange virtual currency for real currency through online intermediaries, such as the websites BitStamp and the now-defunct Mt. Gox.<sup>7</sup> The federal government has monitored and shut down some virtual currency networks because the degree of anonymity and mobility offered by many virtual currencies makes them useful for money laundering and illicit transfers of currency.<sup>8</sup>

- *Decentralized.* No government or non-governmental institution facilitates or maintains cryptocurrency networks. Cryptocurrencies run on peer-to-peer networks, on which users, or “peers,” share files among themselves—from music and movies to records of cryptocurrency transactions. If one peer disconnects from the internet, users can still download files from the other peers on the network.<sup>9</sup> This capability makes peer-to-peer networks harder to shut down than the more traditional client-server networks, in which many users, or “clients,” download files from one central database, or the “server.”<sup>10</sup>

Peer-to-peer networks allow cryptocurrency users to manage their currency without a centralized state or non-state institution to back the currency. Every user on the network has a special program called a “wallet,” which helps them use the cryptocurrency network.<sup>11</sup> Every user also has a file called a “block chain” that contains a record of every transaction made on the network.<sup>12</sup> Users can volunteer to check the accuracy of this shared record in a process called “mining.” When users mine cryptocurrencies, they devote some of their computer’s processing power to verifying the accuracy of the record stored

in the block chain. The network automatically creates new cryptocurrencies to reward miners.<sup>13</sup>

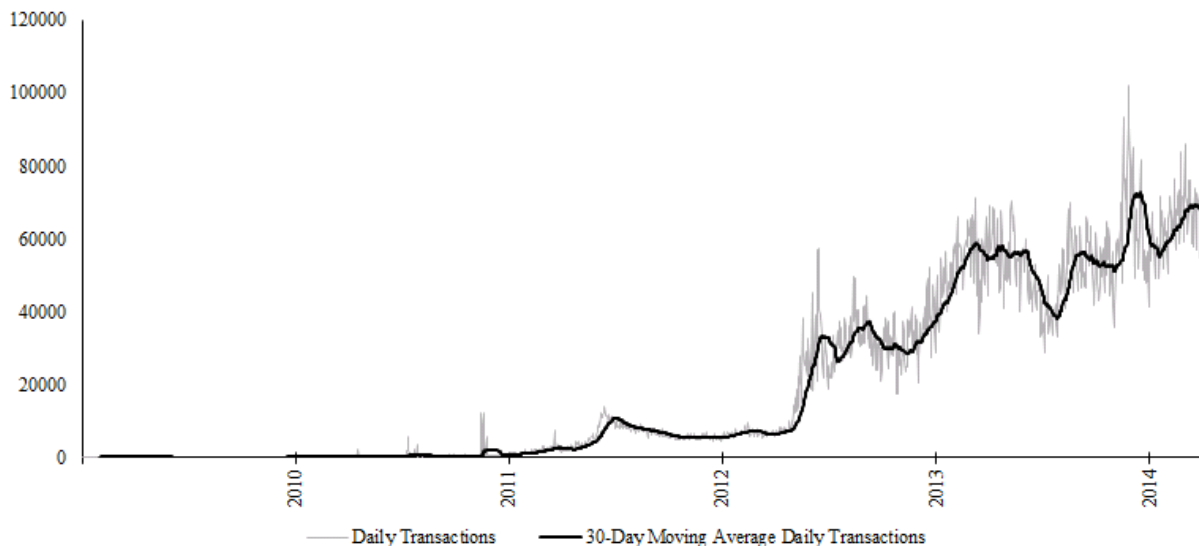
- *Semi-anonymous.* Cryptocurrency networks provide a degree of anonymity because they do not require users to submit their real names. Users identify themselves with “keys” unique to their wallets. These keys are two special strings of numbers stored in the wallet file that help the user encode and decode encrypted information about trades they make on the cryptocurrency network.<sup>14</sup>

The partial anonymity granted by keys is deceptive and is termed “pseudonymity” by cryptocurrency users. Users on the network are not truly anonymous, because cryptocurrency trades are still marked by one of the user’s keys.<sup>15</sup> Real identities can be linked to this key by U.S. law enforcement without the use of additional tools. Users must employ tools like the Tor Network, an online identity-hiding service, in order to conceal their identities.<sup>16</sup> Users can also utilize cryptocurrency tumblers, services that swap coins between many wallets to hide the source of the coin.<sup>17</sup>

- *A growing challenge.* The popularity of cryptocurrencies has grown rapidly since the creation of Bitcoin in 2009. The average market capitalization of Bitcoin in 2011 was \$41 million (US) and an average of around 5,000 transactions were performed on the network daily.<sup>18</sup> As of April 1, 2014, Bitcoin’s market capitalization had climbed to \$6 billion (US) with about 68,000 daily transactions performed on the network.<sup>19</sup> Around 12.5 million bitcoins currently circulate online, with more mined every day.<sup>20</sup>

Bitcoin only represents the beginning of the cryptocurrency phenomenon. Programmers and entrepreneurs already have launched other cryptocurrencies based on the Bitcoin model. Litecoin, Peercoin, Dogecoin, Auroracoin and Namecoin are the most popular of these “altcoins.” The listed altcoins each individually have market capitalizations of over \$10 million (US).<sup>21</sup> A total of around 83 types of altcoins are currently in circulation.<sup>22</sup>

Figure 1: Daily Transactions on the Bitcoin Network



The virtual, decentralized, and semi-anonymous nature of cryptocurrencies provides an opportunity for criminals and a challenge to regulators. Regulators have difficulty eradicating cryptocurrencies because they run on peer-to-peer networks. The pseudonymity offered by cryptocurrency networks, coupled with additional anonymity-hiding tools, such as Tor, makes it difficult for regulators to track trades made on the network. Regulators also cannot guarantee cryptocurrency transactions or cryptocurrency assets or enact monetary policy for cryptocurrency markets.

## Threats from Cryptocurrencies

*Commercial child pornography, sexual exploitation, sex trafficking and other criminal enterprises are increasingly moving to a new unregulated, unbanked digital economy... Child pornography producers are using Tor hidden services for the creation and dissemination of child pornography—and Bitcoin for payment.*

—Ernie Allen, International Centre for Missing and Exploited Children, 2013

Illicit cryptocurrency users couple cryptocurrencies with internet anonymity tools, like the Tor Network, to transfer funds with little government oversight. Real currency can be converted into cryptocurrency at an unregulated exchange, moved and spent semi-anonymously, and then transferred back into real currency. The secrecy of these transactions facilitates entire illicit economies for drugs, weapons, and human beings. The inability of the United States to control the flow of cryptocurrencies also creates risks for financial disruption for both cryptocurrency users and financial markets as a whole.

### *Cryptocurrency and Illicit Transactions*

The pseudonymity and decentralization of cryptocurrencies make them attractive tools for covertly transferring funds to terrorist and insurgent groups. Online marketplaces dealing in illicit goods and services, like drugs and prostitution, also often use cryptocurrencies as payment mechanisms.

- *Terrorist funding.* Cryptocurrencies have utility similar to that of *hawala* networks to terrorist financiers. *Hawala* networks allow expatriates living in the United States to deposit money for another person living outside the country to a local *hawala* broker without ever needing to use a traditional bank.<sup>23</sup> *Hawala* networks were investigated and regulated by the Financial Crimes Enforcement Network after the terrorist attacks on September 11, 2001, when they discovered that terrorist financiers used the *hawala* network to covertly move money out of the United States.<sup>24</sup>

Cryptocurrency networks are also decentralized, difficult to monitor, and nearly impossible to shut down.<sup>25</sup> Jeremy Allaire, CEO of the cryptocurrency-focused company Circle Internet Financial, admits that “terrorists will seek to employ digital currency if it



remains unregulated.”<sup>26</sup> Experts in both the computer science and criminal justice fields agree that the potential exists for cryptocurrencies to fund a terrorist attack.<sup>27</sup>

- *Sales of illicit goods.* Online retail sites use cryptocurrencies, such as Bitcoin, to facilitate illicit trading because of the degree of anonymity they provide.<sup>28</sup> Sites such as Silk Road, the Sheep Marketplace, and Black Market Reloaded offer online marketplaces, similar to Amazon or Ebay, through which users can buy and sell drugs using cryptocurrencies for exchange.<sup>29</sup> These sites are difficult for law enforcement to combat. For example, despite being shut down and having its Bitcoin assets confiscated by the FBI in 2013, Silk Road reopened later the same year.<sup>30</sup> It is estimated that around 18 percent of current U.S. drug users have purchased illegal drugs on Silk Road.<sup>31</sup>
- *Facilitation of human trafficking.* Cryptocurrencies could promote the exploitation and trade of human beings. Though evidence for human trafficking using cryptocurrencies remains somewhat anecdotal, anonymous law enforcement officials suggest that cryptocurrencies like Bitcoin, used in conjunction with the Tor network, not only allow for trade in child pornography, but also actively encourage it.<sup>32</sup>

### *Cryptocurrency and Financial Disruption*

Cryptocurrency use presents risk to both individual users and national economies. Lack of regulation and consumer protection create dangers for the cryptocurrency user. As cryptocurrencies grow in value relative to real currencies, the possibility for online currency to disrupt real currencies also grows.

- *No consumer protection.* Lack of centralized oversight puts cryptocurrency users at risk. Stolen or lost wallets still have unclear legal status in relation to real currency. Also, unlike exchanges between banks, cryptocurrency trades do not pass through heavily regulated central intermediaries called clearing houses.<sup>33</sup> Clearing houses can monitor and reverse trades connected with fraud or theft, but cryptocurrency transactions are direct and irreversible. The lack of an agency like the Federal Deposit Insurance Corporation for cryptocurrencies further decreases consumer safety in cryptocurrency networks.<sup>34</sup>
- *Preclusion of monetary policy.* The decentralization of cryptocurrency networks prevents the implementation of monetary policy to counter the frequent fluctuations in the value of cryptocurrencies.<sup>35</sup> After China proposed strictly regulating the Bitcoin network in December 2013, for instance, the value of a bitcoin dropped by nearly half, from around \$1,200 (US) to around \$600 (US).<sup>36</sup> No central authority exists to stabilize these fluctuations, because the total amount of cryptocurrency available to be mined is predetermined at the creation of the network and new cryptocurrencies are automatically granted to miners by the network.<sup>37</sup> Furthermore, the Federal Reserve has determined that it does not have the legal authority to regulate cryptocurrency networks.<sup>38</sup>

- *Destabilization of real currencies.* Cryptocurrencies could be used to undermine both financial regulation and the value of real currencies. Argentina has already had difficulty regulating flows of pesos out of the country after they are converted into bitcoins.<sup>39</sup> Potential also exists for a coordinated speculative attack on a real currency using cryptocurrencies. Actors could use cryptocurrencies to rapidly devalue a real currency by repeatedly betting against the value of a currency and pumping large amounts of the real currency into the market at once.<sup>40</sup> Central banks defend their currencies from an attack by selling reserves of the attacking currency. However, most states would be unable to defend against an attack by a cryptocurrency, as few states hold large reserves of cryptocurrencies.

The lack of effective regulation for cryptocurrencies and cryptocurrency exchanges endangers U.S. security interests by facilitating terrorism, drug trading, and human trafficking. They also endanger their users as well as undermine attempts to regulate financial markets. Without effective regulation of currencies and exchanges, the United States cannot counter these threats.

## **Benefits of Cryptocurrencies**

With effective regulation, cryptocurrencies could offer major benefits to the economy. Cryptocurrencies can provide a secure, low-cost method of transferring and storing value for legitimate users. Their online nature makes them accessible to people who might otherwise not use banks or feel overly regulated. Cryptocurrencies can also be used to represent ownership of real properties or ideas, making them useful in managing deeds, contracts, and patents.

- *Simplification of banking transactions.* Cryptocurrencies could provide an accurate, fast, and easily used method of transferring and tracking value to facilitate online transactions. Traditional centralized clearing houses can take hours, or even days, to complete many funds transfers. Banks could use a decentralized cryptocurrency system similar to Bitcoin in order to directly settle their accounts.<sup>41</sup> This new system could even use clearing houses designed around cryptocurrencies to further monitor and secure transactions to counter risks associated with irreversible transactions.<sup>42</sup> These clearing-house functions could be cheaper, faster, and more secure than traditional clearing-house networks.
- *Potential for record-keeping functions.* “Colored coins” could revolutionize recordkeeping of stock ownership, patents, and even ownership of material goods. A colored cryptocoin contains information tying it to some other property, and transferring ownership of the coin irrevocably transfers the property’s ownership as well. This property could be a stock, a patent, or even a physical object, like a car.<sup>43</sup> A complete, reliable history of the property’s ownership exists in the cryptocurrency’s block chain tied to a particular colored coin.

Users already take advantage of colored coins, and improving cryptocurrency regulation could encourage widespread adoption of this technology. Special wallet programs are

available for download that can color existing bitcoins.<sup>44</sup> Software developers have begun the creation of networks, such as Mastercoin, which are designed to exist alongside Bitcoin and allow for the creation of colored coins.<sup>45</sup> Other developers have started making new networks, separate from other major cryptocurrencies, designed specifically for colored coin use.<sup>46</sup>

- *Aid the unbanked and oppressed.* Cryptocurrencies can help people or communities underserved by traditional money services by providing low-cost, secure alternatives. Bitcoin entrepreneurs hope to provide the 68 percent of Filipinos who remain unbanked with a cheap, easily accessed alternative to bank accounts or credit cards.<sup>47</sup> Properly regulated cryptocurrencies could also help workers send remittances. Around 7 percent of the remittance market are transaction fees. Cryptocurrencies could provide a secure, low-cost tool for workers to transmit money to families abroad.<sup>48</sup>

Cryptocurrencies can also aid users in countries with restrictive capital controls. States like Venezuela, for instance, impose strict regulation on currency exchange and capital flows. Venezuelans also sometimes worry about the price of their currency and its ability to store value in the long term. Users can harness cryptocurrencies to subvert these regulations and securely store and transfer value.<sup>49</sup>

Cryptocurrencies can both improve access to the economy as well as make the economy more secure. Without a regulatory structure designed to harness these new opportunities, however, the United States risks losing these potential benefits.

## **An Inadequate Response to Cryptocurrencies**

U.S. regulators try to apply existing financial regulation to cryptocurrencies, despite the legal and functional differences between these currencies and real currencies. Existing regulations are often unclear and contradictory. The Department of the Treasury, Internal Revenue Service (IRS), and specific state governments all claim some authority over cryptocurrency networks and exchanges.<sup>50</sup> Other government institutions, such as the Federal Reserve, claim no authority over cryptocurrencies.<sup>51</sup>

- *Application of existing law to cryptocurrency exchanges.* Current financial law does not apply clearly to cryptocurrency exchanges, despite the Department of the Treasury's claim of authority over these exchanges through directives published by the Financial Crimes Enforcement Network (FinCEN). FinCEN directives classify cryptocurrency exchanges as a of money services businesses called a money transmitter.<sup>52</sup> Money services businesses (MSBs) include companies that transfer, exchange, or otherwise deal with real currency, but do not include banks or stock trading companies.<sup>53</sup> FinCEN requires that businesses with this status register with FinCEN itself.<sup>54</sup> Money transmitters are then subject to reporting requirements under the Bank Secrecy Act (BSA).<sup>55</sup> Money transmitters must also register independently with each state in order to operate within that state.<sup>56</sup>

Current legal requirements, such as licensing requirements unique to each state, incur high startup costs for potential cryptocurrency exchanges in the United States.<sup>57</sup> MSBs must apply for licenses in 48 states, as well as Washington, D.C. and Puerto Rico. Combined initial licensing fees cost roughly \$64,000 (US), and combined annual fees cost around \$36,000 (US).<sup>58</sup> FinCEN also remains unclear about the exact information it requires from MSBs dealing in cryptocurrencies.<sup>59</sup> BSA reporting requirements also do not adequately regulate cryptocurrency exchanges, as they do not clearly address the ability of cryptocurrency users to remain anonymous while conducting transactions.<sup>60</sup>

- *Classification of cryptocurrency.* The IRS classifies cryptocurrencies as property, not currency.<sup>61</sup> Although the IRS recognizes that cryptocurrencies can be used as payments for other goods and services, they do not recognize them as money for tax purposes. Cryptocurrency users, therefore, must pay capital gains tax on transactions made with cryptocurrencies.<sup>62</sup> These taxes apply both when exchanging cryptocurrencies for real currency and when exchanging cryptocurrencies for any other good with an established value in real currency.<sup>63</sup>

Existing legal precedent, however, does not directly outline legal response to cryptocurrency theft or fraud. While certain laws may indirectly apply to cryptocurrencies, no law currently exists that is tailored to address the threats posed by cryptocurrencies. The applicability of these laws depends on the judgment of the relevant regulatory bodies.

- *Unclear regulatory future.* Though existing laws may apply to some aspects of cryptocurrency-related crime, the lack of law tailored to cryptocurrencies, as well as the lack of clear response from regulatory agencies, makes it difficult for consumers to understand exactly how cryptocurrencies are treated under the law. Cryptocurrency exchanges remain unsure of how best to implement anti-money laundering programs, despite their best efforts to fully comply with FinCEN regulation.<sup>64</sup> This uncertainty has a chilling effect on potential users and exchanges; as of February 2014, none of the five largest cryptocurrency exchanges by trading volume were based in the United States.<sup>65</sup>

Obtaining licenses to trade in cryptocurrencies is complicated and costly, while the actual licensing process does not address the specific dangers of cryptocurrency networks. Inconsistent and unclear regulation drives exchanges outside of U.S. borders and into countries like Slovenia and Japan, impeding American monitoring of these exchanges.

## **Diverse Models for Regulation**

Other states have already taken steps to adapt to cryptocurrencies, giving policymakers a number of policy options from which to choose. These proposals range from ignoring these networks to banning cryptocurrency use entirely.

- *No regulation.* Government regulators have the option of simply ignoring the use and trade of cryptocurrencies. Some states still are unsure about how to treat cryptocurrencies under the law, while others do not have either the resources or political will to develop clear cryptocurrency regulation. Some states, like France and New Zealand, have warned consumers of the dangers of using cryptocurrencies but have declined to regulate them directly.<sup>66</sup> U.S. regulators could also refuse to regulate cryptocurrencies and allow law enforcement to use unregulated cryptocurrency networks to identify potential terrorists and criminals.
- *Apply existing domestic regulation.* Policymakers can allow the use and trade of cryptocurrencies but regulate that use with existing law, depending on the legal classification of cryptocurrencies themselves. Since September 2011, Germany’s central bank and the German Federal Financial Supervisory Authority have considered Bitcoin a Unit of Account and a legitimate financial instrument.<sup>67</sup> Germany taxes Bitcoin because it considers it a Unit of Account.<sup>68</sup> This classification regulates Bitcoin under a legal framework similar to that used to regulate and tax holdings of foreign currencies.<sup>69</sup> Sweden has also proposed cryptocurrency regulation, but has yet to decide whether to classify cryptocurrencies as goods or a means of payment.<sup>70</sup> Because these countries have at least partially legitimized cryptocurrencies, their regulatory agencies have the authority to regulate and restrict cryptocurrency trading services.
- *Create new domestic regulation.* Countries could also create new legislation that directly applies to the use and sale of cryptocurrencies. This option requires that countries draft and pass legislation that identifies online currencies and allows for their regulation. For instance, Brazil passed Law No. 12865 in October 2013, giving the Brazilian Central Bank and the National Monetary Council the authority to regulate “electronic currencies” such as Bitcoin.<sup>71</sup> Some cryptocurrency experts believe this law is friendly to cryptocurrency users, because it integrates them into the real economy.<sup>72</sup>
- *Develop international regulation.* The European Union, for instance, could standardize cryptocurrency regulation across member countries. The EU has unclear regulation regarding the use and transfer of cryptocurrencies. No piece of regulation passed by the European Union specifically regulates virtual currencies.<sup>73</sup> The European Union does regulate “electronic money,” but cryptocurrencies do not fully meet the criteria of an electronic money.<sup>74</sup> Other EU directives could apply to cryptocurrency exchanges. Unlike the United States, the European Union has a single standard for money transmitters. This standard applies to all EU member states, which opens the possibility of regulating cryptocurrencies within an international framework.<sup>75</sup>

The International Monetary Fund could also propose guidelines on trading and regulating cryptocurrencies.<sup>76</sup> The IMF could amend its Articles of Agreement to allow states to classify cryptocurrencies as “separate currencies” that are not the legal tender of the state, but still fall within its jurisdiction.<sup>77</sup> It could also amend the membership requirements of the IMF to allow cryptocurrency networks “quasi-membership,” bringing the network itself under the aegis of IMF authority.<sup>78</sup>

- *Criminalize exchanges or currencies.* China experimented with preventing exchange of cryptocurrencies into real currencies. In December 2013, China proposed banning financial intermediaries from helping online cryptocurrency exchanges convert Bitcoin into real currency.<sup>79</sup> China’s original regulation did not criminalize the ownership, exchange, or creation of cryptocurrency itself. Instead, it cut off cryptocurrency networks from financial markets.

Russia bans the use, purchase, and possession of cryptocurrencies. This method of regulation directly targets the users of cryptocurrencies. Russia may prosecute individual buyers or users of Bitcoin under laws that ban the issuing of “money surrogates.”<sup>80</sup> This regulation differs from China’s in that it not only criminalizes trading cryptocurrencies for real currency, but also criminalizes the actions of the individual cryptocurrency user.

The United States is not the first country to consider cryptocurrency regulation. However, a fully comprehensive and effective method of regulation has not yet been developed.

## **A New Idea: Preemption and Regulation**

*Consumer protection makes sense. I think where bitcoins are exchanged for national currencies, it certainly makes sense that whoever controls those national currencies might want to regulate that.*

—Gavin Andresen, Chief Scientist, Bitcoin Foundation

By monitoring the flow of real currency in and out of cryptocurrency networks through carefully regulated exchanges, policymakers can discourage and prosecute illicit uses of these networks. The U.S. government, therefore, should create a special license called a cryptocurrency transmitter license. This license would be necessary for businesses to exchange cryptocurrency for real currency or another virtual currency. Licenses for cryptocurrency transmitters would be granted only at the federal level through FinCEN and would preempt other state-level authorization for money services businesses to trade cryptocurrencies. The United States could then use anti-money laundering laws to prevent businesses trading cryptocurrency for real currency without a cryptocurrency transmitter license.

- *Clarity and specificity.* Future regulation must directly address the emergent challenge of cryptocurrencies. FinCEN licensing should require all businesses with cryptocurrency transmitter licenses to record and regularly report their users’ names, e-mail addresses, IP addresses, and transaction amounts for each transaction made through the exchange. Many U.S. exchanges already volunteer similar information to regulatory bodies.<sup>81</sup> Legally requiring the reporting of this information would only clarify and institutionalize an already-occurring practice. It would also greatly aid law enforcement officials in tracking criminals using exchanges. FinCEN should also streamline and clarify the application process specifically for cryptocurrency transmitter licenses to ensure that applications ask relevant information of potential transmitters.

- *Universal applicability.* Cryptocurrency licensing and regulation should lower costs for cryptocurrency exchange entrepreneurs by requiring licensing only at the federal level. Cryptocurrency transmitter licenses should be granted by FinCEN, and preempt state-level licenses for other money services businesses. The federal government's preemption of license granting would lower costs for entrepreneurs wishing to start a cryptocurrency exchange. If states resist preemption, the federal government instead could develop uniform application and reporting requirements for all states, similar to the uniformity of money transmitter regulation in the European Union.

Federal regulation of cryptocurrency exchanges would encourage greater consumer confidence in the security and reputability of these exchanges. The size or reputation of these exchanges often does not serve as a good indicator of their true reputability; Mt. Gox, once the largest cryptocurrency exchange in the world, abruptly ceased operations in early January 2014 after losing around \$400 million (US) worth of cryptocurrencies and delayed notifying their customers.<sup>82</sup> Direct federal oversight of exchanges would allow regulators to impose security standards on exchanges and require exchanges to notify customers in the event of a security breach.

The United States must become a secure, welcoming location in which to base cryptocurrency exchanges. Encouraging the establishment of cryptocurrency exchanges within the United States grants it more control over the virtual economy and will position it as a major player in the possible development of future international regulation. By carefully monitoring these exchanges, U.S. regulators can ensure that the money that flows into the virtual economy will be used for beneficial purposes.

## Potential Objections

Several objections could be raised about the proposed recommendation. For example, the proposal could be considered too lax regarding what some may view as a grave threat to U.S. security. The proposal could also overreach, either opening the door for abuse of regulation by other types of businesses, or de-incentivizing entrepreneurs with stringent reporting requirements.

- *Too lenient.* Cryptocurrencies might pose too great a risk to law enforcement and financial regulators to be legal in the United States. The United States could adopt a policy similar to that proposed by China and ban cryptocurrency exchanges. The United States could also legislate against cryptocurrencies themselves by criminalizing cryptocurrency use and production.

Banning cryptocurrencies would not eliminate their risks; in fact, it would only surrender a potentially useful new technology to criminals, terrorists, and drug dealers. In addition, completely banning cryptocurrencies would be nearly impossible, because they run on peer-to-peer networks. Law enforcement has had trouble shutting down these networks in the past. Other peer-to-peer networks, such as the illegal file-sharing network, The Pirate

Bay, have been notoriously difficult for law enforcement to suppress.<sup>83</sup> Banning cryptocurrencies would be at best ineffective and at worst harmful.

- *Preemption opens the door for other businesses to reduce their own regulatory burdens.* Banks and money services businesses could use the introduction of cryptocurrency exchanges as a “foot in the door” to drastically reduce their own reporting requirements. These companies could lobby for their own exemption from state-by-state licensing for non-cryptocurrency related activities.

For this reason, both regulators and legislators need to tailor legislation and enforcement specifically to cryptocurrencies and cryptocurrency exchanges. Preemption only applies to a license to deal in cryptocurrency and does not override other requirements related to traditional banking and money transmitting businesses. Regulators must also make sure to only justify preemption for cryptocurrency exchanges, because they are both an emerging business model and a type of business that needs efficient licensing and regulation.

- *Domestic regulation will not stop cryptocurrency misuse.* Cryptocurrency crime is an international problem and could require international regulation. The United States should ignore domestic regulation and focus on developing agreements with other governments concerned about cryptocurrency crime.

The international nature of cryptocurrency crime actually highlights the need for the United States to become a leader in developing and implementing effective, specific, and welcoming regulation for cryptocurrency exchanges. International regulation may be inevitable, and the United States risks forfeiting its ability to shape possible future cryptocurrency regulation if it has not developed effective domestic regulation of its own. By positioning itself as an innovator in cryptocurrency law, the United States can attract cryptocurrency businesses to U.S. shores, while influencing laws made around the globe.

## **Conclusion**

Cryptocurrencies are fundamentally different from both real currencies and other virtual currencies. Cryptocurrency networks run independently from any government or non-government institution. Decentralization and a degree of anonymity creates opportunities for hackers and thieves to cheat cryptocurrency networks. This decentralization makes banning or directly regulating cryptocurrency networks unfeasible.

Cryptocurrencies must therefore be regulated by monitoring all points at which cryptocurrencies can be exchanged for real currency. The current regulatory structure surrounding currency markets, however, cannot effectively monitor exchanges. Although cryptocurrency exchanges have some of the qualities of a money transmitter, they have vulnerabilities that other money services businesses do not have.



A new federal-level license to run a cryptocurrency exchange would both increase cryptocurrency market security and encourage domestic investment. Trades between cryptocurrency and real currency could be closely monitored by a central organization to prevent money laundering, capital control evasion, and deals in illicit goods. Providing ease of access to U.S. markets by simplifying the licensing process for cryptocurrency exchanges would also incentivize entrepreneurs to establish cryptocurrency exchanges within U.S. borders.

---

<sup>1</sup> “Who Is Satoshi Nakamoto, Mysterious Bitcoin Founder?” Kelleher, John, accessed April 4, 2014, <http://www.investopedia.com/articles/general/032614/who-satoshi-nakamoto-mysteriousbitcoin-founder.asp>.

<sup>2</sup> Calvery, Jennifer. Statement to the Senate, Committee on Homeland Security and Homeland Affairs. *Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies*, Hearing, November 18, 2013. Available at: [http://www.fincen.gov/news\\_room/testimony/pdf/20131118.pdf](http://www.fincen.gov/news_room/testimony/pdf/20131118.pdf). Accessed: 4/4/14.

<sup>3</sup> Bombace, Michael, “Blazing Trails: A New Way Forward for Virtual Currencies and Money Laundering.” *Journal of Virtual Worlds Research*, 6, no. 3 (2013): 1-10.

<sup>4</sup> “A Revolution in Money.” Sorkin, Andrew, accessed April 4, 2014, <http://dealbook.nytimes.com/2014/04/01/a-revolution-in-money/>.

<sup>5</sup> Prevention of counterfeiting and double-spending is an important feature of any currency. The U.S. government is the only entity that has the authority to print U.S. dollars. The U.S. Department of the Treasury designs printed money, for instance, to be very difficult to counterfeit. Cryptocurrencies do not rely on a central authority, like the Department of the Treasury, to create new coins or prevent their counterfeiting. Instead, transactions are verified with public-key encryption. “Designing U.S. Currency to Prevent Counterfeiting.” The Partnership for Public Service, accessed April 10, 2014, [http://www.washingtonpost.com/politics/federal\\_government/designing-us-currency-to-prevent-counterfeiting/2014/01/07/2885c3ae-77a1-11e3-b1c5-739e63e9c9a7\\_story.html](http://www.washingtonpost.com/politics/federal_government/designing-us-currency-to-prevent-counterfeiting/2014/01/07/2885c3ae-77a1-11e3-b1c5-739e63e9c9a7_story.html).

<sup>6</sup> “Bullion and Bandits: The Improbable Rise and Fall of E-Gold,” Kim Zetter, last modified June 9, 2009, <http://www.wired.com/2009/06/e-gold/>. And Santora, Marc, William Rashbaum, and Nicole Perlroth, “Online Currency Exchange Accused of Laundering \$6 Billion.” *The New York Times*, May 28, 2013, accessed March 31, 2014, [http://www.nytimes.com/2013/05/29/nyregion/liberty-reserve-operators-accused-of-money-laundering.html?pagewanted=all&\\_r=1&\\_](http://www.nytimes.com/2013/05/29/nyregion/liberty-reserve-operators-accused-of-money-laundering.html?pagewanted=all&_r=1&_).

<sup>7</sup> “Mt. Gox Says It Found Missing Bitcoin Worth about \$116 Million.” Abrams, Rachel, accessed April 7, 2014, [http://dealbook.nytimes.com/2014/03/21/mt-gox-says-it-has-found-200000-bitcoins-worth-about-114-million/?\\_php=true&\\_type=blogs&\\_r=0](http://dealbook.nytimes.com/2014/03/21/mt-gox-says-it-has-found-200000-bitcoins-worth-about-114-million/?_php=true&_type=blogs&_r=0).

<sup>8</sup> Nakamoto, Satoshi, “Bitcoin: A Peer-to-Peer Electronic Cash System.” *bitcoin.org*, <https://bitcoin.org/bitcoin.pdf>.

<sup>9</sup> Upreti, Naveen, “Exploring the World of Collaborative Sharing over the Internet through the Use of a Peer-to-Peer Network Protocol.” *International Journal of Innovative Research in Computer Science & Technology*, 1, no. 1 (2013): 21.

<sup>10</sup> Upreti, Naveen, “Exploring the World of Collaborative Sharing over the Internet through the Use of a Peer-to-Peer Network Protocol.” *International Journal of Innovative Research in Computer Science & Technology*, 1, no. 1 (2013): 22.

<sup>11</sup> Dinesh C. Verma, *Legitimate Applications of Peer-to-Peer Networks* (Hoboken, NJ: John Wiley and Sons, Inc., 2004).

<sup>12</sup> Ralf Steinmetz and Klaus Wehrle, *Peer-to-Peer Systems and Applications* (Germany: Springer, 1973).

<sup>13</sup> Miers, Ian, Garman, Christina, Green, Matthew, and Rubin, Aviel, “ZeroCoin: Anonymous Distributed E-Cash from Bitcoin.” *Security and Privacy* (2013): 397-411.

<sup>14</sup> A user’s keys are paired—the private key “locks” data by encrypting it in a way that only the paired public key can decrypt, and vice versa. A public key is known to everyone on the network and functions like an address to which other users can send cryptocurrencies. Private keys are intentionally kept secret. When a user wishes to transfer a cryptocurrency, she tells the network that she wishes to transfer funds to another user, identified by a public key. She then “signs” the transfer recorded in the block chain by encrypting information with her own private key. Any other user can later check the validity of her transfer with the public key paired to the private key with which she signed the transaction. Jerry Brito and Andrea Castillo, *Bitcoin: A Primer for Policymakers* (Arlington, VA: Mercatus Center, 2013), 30.

---

<sup>15</sup> Dinesh C. Verma, *Legitimate Applications of Peer-to-Peer Networks* (Hoboken, NJ: John Wiley and Sons, Inc., 2004).

<sup>16</sup> The Tor Network is an internet anonymity tool developed by MIT and the U.S. Naval Research Laboratory. Tor hides the origin of web traffic by directing the traffic through many computers in such a way that makes it impossible to identify the source of the data. Like cryptocurrencies, Tor has the potential for both legitimate and illegitimate use. Though criminals use the service to hide their identities, reporters and activists use it to escape persecution from oppressive governments, and the U.S. military uses it to secure communications. Dinesh C. Verma, *Legitimate Applications of Peer-to-Peer Networks* (Hoboken, NJ: John Wiley and Sons, Inc., 2004) and “Granting Anonymity.” Heffernan, Virginia, accessed April 10, 2014, <http://www.nytimes.com/2010/12/19/magazine/19FOB-Medium-t.html?pagewanted=all>

<sup>17</sup> Litke, Pat, and Stewart, Joe, “Enterprise Best Practices for Cryptocurrency Adoptions.” *Dell SecureWorks*, (2014): 1-12.

<sup>18</sup> “Blockchain,” last modified April 7, 2014, <https://blockchain.info/>.

<sup>19</sup> “Crypto-currencies statistics,” last modified April 7, 2014, <http://bitinfocharts.com/>.

<sup>20</sup> “Crypto-currencies statistics,” last modified April 7, 2014, <http://bitinfocharts.com/>.

<sup>21</sup> “Crypto-currencies statistics,” last modified April 7, 2014, <http://bitinfocharts.com/>.

<sup>22</sup> “The rise of cryptocurrencies.” Powell, Jacob, accessed April 7, 2014, <http://www.aljazeera.com/indepth/features/2014/01/rise-cryptocurrencies-201413012034867124.html>.

<sup>23</sup> “Africa–Denmark: New Commission For Africa.” *Africa Research Bulletin: Political, Social and Cultural Series* 45, no. 3 (2008): 17780.

<sup>24</sup> Perkel, Walter, “Money Laundering and Terrorism: Informal Value Transfer Systems.” *American Criminal Law Review* 41 (2004): 183-186.

<sup>25</sup> Irwin, Angela, Slay, Jill, Choo, Kim-Kwang, and Lui, Lin, “Money laundering and terrorism financing in virtual environments: a feasibility study.” *Journal of Money Laundering Control* 17 (2014): 50-75.

<sup>26</sup> Allaire, Jeremy. Statement to the Senate, Committee on Homeland Security and Homeland Affairs. *Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies*, Hearing, November 18, 2013. Available at: <http://www.hsgac.senate.gov/hearings/beyond-silk-road-potential-risks-threats-and-promises-of-virtual-currencies>. Accessed: 4/7/14.

<sup>27</sup> Griffin, Gordon, “Virtual Currencies in the Crosshairs.” *Criminal Justice* 28, no. 3 (2013): 62.

<sup>28</sup> Van Hout, Marie Claire. “Silk Road,’ the virtual drug marketplace: A single case study of user experiences.” *International Journal of Drug Policy* 24 no. 5 (2013): 385-391.

<sup>29</sup> “Two Guys on Reddit are Chasing a Thief who has \$220 Million in Bitcoins.” Edwards, Jim, accessed April 7, 2014, <http://www.businessinsider.com/220-million-sheep-marketplace-bitcoin-theft-chase-2013-12> and “Silk Road replacement Black Market Reloaded briefly closed.” Hern, Alex, accessed April 7, 2014, <http://www.theguardian.com/technology/2013/oct/18/silk-road-black-market-reloaded-closed>.

<sup>30</sup> “Manhattan U.S. Attorney Announces Seizure of Additional \$28 Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of “Silk Road” Website.” Federal Bureau of Investigation, accessed April 4, 2014, <http://www.fbi.gov/newyork/press-releases/2013/manhattan-u.s.-attorney-announces-seizure-of-additional-28-million-worth-of-bitcoins-belonging-to-ross-william-ulbricht-alleged-owner-and-operator-of-silk-road-website>.

<sup>31</sup> “Estimated 18 percent of U.S. drug users bought from Silk Road, says study.” Johnston, Casey, accessed April 4, 2014, <http://arstechnica.com/business/2013/12/an-estimated-18-percent-of-americans-used-drugs-from-silk-road-says-study/>.

<sup>32</sup> Allen, Ernie. Statement to the Senate, Committee on Homeland Security and Homeland Affairs. *Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies*, Hearing, November 18, 2013. Available at: <http://www.hsgac.senate.gov/hearings/beyond-silk-road-potential-risks-threats-and-promises-of-virtual-currencies>. Accessed: 4/7/14.

<sup>33</sup> “Automated Clearinghouse Services.” Board of Governors of the Federal Reserve System, accessed April 4, 2014, [http://www.federalreserve.gov/paymentsystems/fedach\\_about.htm](http://www.federalreserve.gov/paymentsystems/fedach_about.htm).

<sup>34</sup> “Why Bitcoin Matters for Bankers.” Hachstein, Marc, accessed April 4, 2014, [http://www.americanbanker.com/magazine/124\\_02/why-bitcoin-matters-for-bankers-1065590-1.html](http://www.americanbanker.com/magazine/124_02/why-bitcoin-matters-for-bankers-1065590-1.html).

<sup>35</sup> “Bitcoin Volatility: The 4 perspectives.” Albrecht, Radoslav, accessed April 4, 2014, <http://bitcoinmagazine.com/6543/bitcoin-volatility-analysis/>.

- 
- <sup>36</sup> “The bitcoin crash of 2013: Don’t you feel silly now?.” Hiltzik, Michael, accessed April 4, 2014, <http://www.latimes.com/business/hiltzik/la-fi-mh-the-bitcoin-crash-20131207,0,7011276.story#axzz2npwthsj7>.
- <sup>37</sup> Grinberg, Reuben. “Bitcoin: an innovative alternative digital currency.” (2012).  
For example, the Bitcoin network is capped to produce 21 million bitcoins over roughly 20 years.
- <sup>38</sup> “Janet Yellen: Federal Reserve has no authority to regulate Bitcoin.” Rushe, Dominic, accessed April 4, 2014, <http://www.theguardian.com/business/2014/feb/27/janet-yellen-federal-reserve-no-authority-regulate-bitcoin>.
- <sup>39</sup> Lee, Timothy. “Five Surprising Facts About Bitcoin.” *Washington Post*, August 21, 2013.
- <sup>40</sup> Plassaras, Nicholas. “Regulating Digital Currencies: Bringing Bitcoin Within the Reach of the IMF.” *Chicago Journal of International Law* 14: 377-407.
- <sup>41</sup> “Bitcoin Isn’t the Future of Money, But It Could Be the Future of Moving Money Around.” Roose, Kevin, accessed April 7, 2014, <http://nymag.com/daily/intelligencer/2013/11/how-bitcoin-can-mainstream-in-one-easy-step.html>.
- <sup>42</sup> “Why Bitcoin Won’t Die.” Camhi, Jonathan, accessed April 7, 2014, <http://www.banktech.com/payments-cards/why-bitcoin-wont-die/240166504>.
- <sup>43</sup> “Hidden Flipside.” *The Economist*, accessed April 4, 2014, <http://www.economist.com/news/finance-and-economics/21599054-how-crypto-currency-could-become-internet-money-hidden-flipside>, and “Why Bitcoin Matters for Bankers.” Hachstein, Marc, accessed April 4, 2014, [http://www.americanbanker.com/magazine/124\\_02/why-bitcoin-matters-for-bankers-1065590-1.html](http://www.americanbanker.com/magazine/124_02/why-bitcoin-matters-for-bankers-1065590-1.html).
- <sup>44</sup> “Irish Company Unveils World’s First Colored Coins Web Wallet.” Andrews, S.T., accessed April 4, 2014, <http://bitcoinmagazine.com/11580/coinprismrelease/>.
- <sup>45</sup> “Bitcoin 2.0 Shows Technology Evolving Beyond Use as Money.” Kharif, Olga, accessed April 4, 2014, <http://www.bloomberg.com/news/2014-03-28/bitcoin-2-0-shows-technology-evolving-beyond-use-as-money.html>.
- <sup>46</sup> “Ethereum Launches ‘Cryptocurrency 2.0’ Network.” Hajdarbegovic, Nermin, accessed April 4, 2014, <http://www.coindesk.com/ethererum-launches-cryptocurrency-2-0-network/>.
- <sup>47</sup> “Ron Hose: Bitcoin is great for all the ‘unbanked’ people in the Philippines.” Magdirila, Phoebe, accessed April 4, 2014, <http://www.techinasia.com/ron-hose-bitcoin-great-unbanked-people-philippines/>.
- <sup>48</sup> Shapiro, Adam, “The Way Forward for Digital Currencies.” *Promontory* (2013): 3.
- <sup>49</sup> “‘Micky Malka’ on How Bitcoin Can Help the World’s Unbanked.” Kirby, Carrie, accessed April 4, 2014, <http://www.coindesk.com/micky-malka-bitcoin-can-help-worlds-unbanked/>.
- <sup>50</sup> *Order Pursuant to New York Banking Law* §§ 2-b, 24, 32, 102-a, and 4001-b and *Financial Services Law* §§ 301(c) and 302(a).
- <sup>51</sup> “Federal Reserve Chair Janet Yellen: Fed Has No Authority to Regulate Bitcoin.” Wilhelm, Alex, accessed April 4, 2014, <http://techcrunch.com/2014/02/27/federal-reserve-chair-janet-yellen-fed-has-no-authority-to-regulate-bitcoin/>.
- <sup>52</sup> *Code of Federal Law* § 1010.100 and Financial Crimes Enforcement Network, January 30, 2014.
- <sup>53</sup> “Definition: Money Services Businesses.” Financial Crimes Enforcement Network, accessed April 4, 2014, [http://www.fincen.gov/financial\\_institutions/msb/definitions/msb.html](http://www.fincen.gov/financial_institutions/msb/definitions/msb.html).
- <sup>54</sup> “Definition: Money Services Businesses.” Financial Crimes Enforcement Network, accessed April 4, 2014, [http://www.fincen.gov/financial\\_institutions/msb/definitions/msb.html](http://www.fincen.gov/financial_institutions/msb/definitions/msb.html).
- <sup>55</sup> “Definition: Money Services Businesses.” Financial Crimes Enforcement Network, accessed April 4, 2014, [http://www.fincen.gov/financial\\_institutions/msb/definitions/msb.html](http://www.fincen.gov/financial_institutions/msb/definitions/msb.html).
- <sup>56</sup> Jerry Brito and Andrea Castillo, *Bitcoin: A Primer for Policymakers* (Arlington, VA: Mercatus Center, 2013), 30.
- <sup>57</sup> Jerry Brito and Andrea Castillo, *Bitcoin: A Primer for Policymakers* (Arlington, VA: Mercatus Center, 2013), 41.
- <sup>58</sup> Thomas Brown and Paul Hastings, “State Resources.” *National Money Transmitters Association* (2013), accessed April 8, 2014, [http://abnk.assembly.ca.gov/sites/abnk.assembly.ca.gov/files/50%20State%20Survey%20-%20MTL%20Licensing%20Requirements\(72986803\\_4\).pdf](http://abnk.assembly.ca.gov/sites/abnk.assembly.ca.gov/files/50%20State%20Survey%20-%20MTL%20Licensing%20Requirements(72986803_4).pdf).
- <sup>59</sup> “Op-ed: The legality of virtual currency.” Baroff, Judd, accessed April 4, 2014, <http://arstechnica.com/tech-policy/2014/03/op-ed-the-legality-of-virtual-currency/>.
- <sup>60</sup> “Definition: Money Services Businesses.” Financial Crimes Enforcement Network, accessed April 4, 2014, [http://www.fincen.gov/financial\\_institutions/msb/definitions/msb.html](http://www.fincen.gov/financial_institutions/msb/definitions/msb.html).
- <sup>61</sup> Internal Revenue Service Notice 2014-21.
- <sup>62</sup> “I.R.S. Takes a Position on Bitcoin: It’s Property.” Abrams, Rachel, accessed April 4, 2014, [http://dealbook.nytimes.com/2014/03/25/i-r-s-says-bitcoin-should-be-considered-property-not-currency/?\\_php=true&\\_type=blogs&\\_php=true&\\_type=blogs&\\_r=1](http://dealbook.nytimes.com/2014/03/25/i-r-s-says-bitcoin-should-be-considered-property-not-currency/?_php=true&_type=blogs&_php=true&_type=blogs&_r=1).

- 
- <sup>63</sup> “New IRS Bitcoin Rules Pose a Problem Only an Army of Startups Can Solve.” McMillan, Robert, accessed April 4, 2014, <http://www.wired.com/2014/03/irs-bitcoin/>.
- <sup>64</sup> “Op-ed: The legality of virtual currency.” Baroff, Judd, accessed April 4, 2014, <http://arstechnica.com/tech-policy/2014/03/op-ed-the-legality-of-virtual-currency/>.
- <sup>65</sup> “None of the 5 biggest Bitcoin exchanges are in the United States.” del Castillo, Michael, accessed April 7, 2014, <http://upstart.bizjournals.com/money/loot/2014/02/12/5-biggest-bitcoin-exchanges.html>.
- <sup>66</sup> *Regulation of Bitcoin in Selected Jurisdictions*, (2014), Law Library of Congress.
- <sup>67</sup> Krohn-Grimberghe, Artus, and Sorge, Christoph. “Practical Aspects of the Bitcoin System.” *Computers and Society* (2013): doi: arXiv:1308.6760 [cs.CY].
- <sup>68</sup> Arthur, Charles. “Bitcoin now ‘unit of account’ in Germany.” *The Guardian*, August 20, 2013.
- <sup>69</sup> Federal Financial Supervisory Authority, 2013, [http://www.bafin.de/EN/Service/Footer/LegalInformation/TermsAndConditions/termsandconditions\\_node.html](http://www.bafin.de/EN/Service/Footer/LegalInformation/TermsAndConditions/termsandconditions_node.html).
- <sup>70</sup> Krohn-Grimberghe, Artus, and Sorge, Christoph. “Practical Aspects of the Bitcoin System.” *Computers and Society* (2013): doi: arXiv:1308.6760 [cs.CY]. and “Bitcoin Turns into Art as Sweden Rejects Creative Currency.” Ek, Veronica, and Carlstrom, Johan, accessed April 4, 2014, <http://www.bloomberg.com/news/2014-01-21/bitcoin-becomes-art-as-swedish-taxman-rejects-creative-currency.html>.
- <sup>71</sup> *Regulation of Bitcoin in Selected Jurisdictions*, (2014), Law Library of Congress.
- <sup>72</sup> Bitcoin Around the World: How Virtual Currencies are Treated in 40 Different Countries.” Fuller, Cameron, accessed April 4, 2014, <http://www.ibtimes.com/bitcoin-around-world-how-virtual-currencies-are-treated-40-different-countries-1553532>.
- <sup>73</sup> *Virtual Currency Schemes*, (2012), 45.
- <sup>74</sup> *Virtual Currency Schemes*, (2012), 43.
- <sup>75</sup> “Why Bitcoin Matters for Bankers.” Hachstein, Marc, accessed April 4, 2014, [http://www.americanbanker.com/magazine/124\\_02/why-bitcoin-matters-for-bankers-1065590-1.html](http://www.americanbanker.com/magazine/124_02/why-bitcoin-matters-for-bankers-1065590-1.html).
- <sup>76</sup> Plassaras, Nicholas. “Regulating Digital Currencies: Bringing Bitcoin Within the Reach of the IMF.” *Chicago Journal of International Law* 14: 377-407.
- <sup>77</sup> Plassaras, Nicholas. “Regulating Digital Currencies: Bringing Bitcoin Within the Reach of the IMF.” *Chicago Journal of International Law* 14: 377-407.
- <sup>78</sup> Plassaras, Nicholas. “Regulating Digital Currencies: Bringing Bitcoin Within the Reach of the IMF.” *Chicago Journal of International Law* 14: 377-407.
- <sup>79</sup> “China Bans Payment Companies from Clearing Bitcoin, News Says.” Bloomberg News, accessed April 4, 2014, <http://www.bloomberg.com/news/2013-12-17/china-bans-payment-companies-from-clearing-bitcoin-news-says.html>.
- <sup>80</sup> “Russia Backs Bitcoin Curbs as Central Bank Snubs Sberbank Plan.” Corcoran, Jason, and Kuznetsov, Vladimir, accessed April 4, 2014, <http://www.businessweek.com/news/2014-01-27/russia-backs-bitcoin-curbs-as-central-bank-snubs-sberbank-plan>.
- <sup>81</sup> Op-ed: The legality of virtual currency.” Baroff, Judd, accessed April 4, 2014, <http://arstechnica.com/tech-policy/2014/03/op-ed-the-legality-of-virtual-currency/>.
- <sup>82</sup> “Judge Orders MtGox CEO to U.S. for questions on failed bitcoin exchange.” Hals, Tom, accessed April 7, 2014, <http://www.reuters.com/article/2014/04/01/us-bitcoin-mtgox-karpeles-idUSBREA3021920140401>.
- <sup>83</sup> “The Pirate Bay to Fly ‘Server Drones’ to Avoid Law Enforcement.” Koebler, Jason, accessed April 7, 2014, <http://www.usnews.com/news/articles/2012/03/19/the-pirate-bay-to-fly-server-drones-to-avoid-law-enforcement>.