REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
04-05-2018	Writing Awards Submission	Jan-May 2018

4. TITLE AND SUBTITLE
Regulating Bitcoin to Protect Our National Interests

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Ostrom, Tracy J.

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Writing & Teaching Excellence Center
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT Distribution A: Approved for public release; distribution unlimited.

13. SUPPLEMENTARY NOTES: A paper submitted to the faculty of the NWC in partial satisfaction of the requirements of the curriculum. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy

14. ABSTRACT

Violent Extremist Organizations (VEOs) need financial networks to conduct their operations and achieve their goals. Seeking a new way to build and maintain their financial networks, VEOs have turned to the Internes and virtual currencies to finance their operations The U.S. must mitigate the misuse of cryptocurrencies by regulating their use under traditional financial laws, and in a further step, dedicate national assets to mine cyber currencies in order to disrupt VEO funding and prevent adversarial nation-states from maneuvering around sanctions.

15. SUBJECT TERMS
virtual currencies, cyber currencies, cryptocurrencies, Bitcoin, mining, Violent Extremist Organizations, regulation

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Director, Writing Center
U	UU	U	N/A	31	19b. TELEPHONE NUMBER *(Include area code)* 401-841-6499

Reset

Regulating Bitcoin to Protect Our National Interests

Tracy Ostrom

United States Naval War College

Submitted: 12 February 2018

4,258 Words

Introduction

Terrorists need money to function. It is estimated the September 11, 2001 terrorist attack cost between $400,000-$500,000.[1] After this first ever-terrorist attack on United States (U.S.) soil, President George W. Bush began the Global War on Terrorism. Years later, in 2013, President Obama shifted the Global War on Terrorism to target specific terror networks such as al-Qaida.[2] This specific targeting allows U.S. Counterterrorism agencies to pursue funding sources as a means to dismantle terrorist networks. Since 2014, Violent Extremist Organizations (VEOs) have touted the anonymous transfer of funds through Bitcoin and called for sympathizers around the world to fund a global jihadist campaign using Bitcoin.[3,4] Senator Mike Crapo (R-ID), Chairman of the U.S. Senate Banking Committee, noticing a lack of legislation in virtual currencies, convened his committee on 6 February 2018. In addition to virtual currencies funding terrorism, Senator Crapo expressed concerns that Venezuela and Russia are creating their own cyber currencies to avoid U.S. sanctions.[5] In this vein, the U.S. must mitigate the misuse of cryptocurrencies by regulating their use under traditional financial laws, and in a further step, dedicate national assets to mine cyber currencies in order to disrupt VEO funding and prevent adversarial nation-states from maneuvering around sanctions.

Hesitation surrounding what to do with cryptocurrencies and how to regulate them is concurrent with the urgency of identifying and reducing terrorist funding. The U.S. Senate introduced S 1241 in early 2017 but didn't hold committee meetings

[1] (Temple-Raston 2014)
[2] (Shinkman 2013)
[3] (Irwin and Milad 2016)
[4] (Wile 2014)
[5] (Congressional Hearing 2018)

discussing the regulation of cyber currencies until 28 Nov 2017.[6] The U.S. House of Representatives introduced HR 4373 on 13 Nov 2017.[7] Both bills attempt to modernize current Anti-Money Laundering laws and Counter Terrorist Financing (AML/CTF) rules by amending the basic definition of 'financial institutions' and 'financial account' to include cyber currencies.[8,9] These bills, however, do not go far enough to control or mitigate the risk of cyber currencies. These bills should include a means to monitor and maintain "mining" operations of cryptocurrencies.

In addition to the introductions of these companion bills, the U.S. Senate Banking Committee recently held a hearing debating the use of virtual currencies. On 6 February 2018, testimonies by Mr. J. Christopher Giancarlo (Chairman of the Commodity Futures Trading Commission) and Mr. Jay Clayton (Chairman of Securities and Exchange Commission) seemed skeptical about the longevity of these new currencies. Understandably, they did not want to invest countless hours determining standards and enforcement rules for a "fad" currency.[10] However, Senator Mark Warner (D-VA), the Vice Chair of the Senate Intelligence Committee, countered this assertion by predicting that Bitcoin and other virtual currencies are going to be around for some time and they are going to be huge.[11] Chairman Crapo, who asked these agencies to put their heads together to recommend future legislation, echoed this sentiment about virtual currencies.[12] Due to the anonymity of Bitcoin and its frequent use for illegal activities, providing funding to VEOs and adversarial nation states, mining is best kept within the NSA. The NSA, in conjunction with CYBERCOM, is the only U.S. agency that has the

[6] (Congress.Gov 2017)
[7] (Congress.Gov 2017)
[8] (Congress.Gov 2017)
[9] (Congress.Gov 2017)
[10] (Congressional Hearing 2018)
[11] (Congressional Hearing 2018)
[12] (Congressional Hearing 2018)

required computing power. The U.S. needs not only to regulate Bitcoin but must shift a portion of its computing power to mining Bitcoin. Therefore, to protect U.S. national interests, Congress must pass legislation that both regulates cyber currencies and prevents manipulation of the markets by VEOs and nation states, thus avoiding U.S. sanctions.

Bitcoin Used for Illicit Activities

Criminal or VEOs need financial networks to conduct their operations and achieve their goals.[13] Historically these financial networks used a combination of smuggling drugs and cash, money laundering, bank transfers, membership fees, human trafficking[14] or cybercrime.[15] If these financial networks are cut off or extremely limited, VEOs ability to conduct operations will diminish. Governmental law enforcement agencies trace criminal and terrorist activity through finances. In fact, the goal of the International Financial Action Task Force (FATF) is to "reduce the potential for abuse of financial systems and financial crimes".[16] In 2001, in response to the World Trade Center attack, the FATF enacted strict AML/CTF laws. These laws required financial transactions to be registered and provided a way for law enforcement agencies to follow the money trail of VEOs. This regulation effectively and severely restricted the use of the conventional banking systems to VEOs.[17, 18]

Seeking a new way to build and maintain their financial networks, VEO's are looking to the Internet to finance their operations. Digital currencies (also called cyber currency, cryptocurrency, or virtual currencies) have provided these means.[19] Tracking conversations of jihadists within Internet chat rooms revealed terrorists considered the

[13] (Irwin and Milad 2016)
[14] (Durmaz 2007)
[15] (Nardo 2006)
[16] (Jackson 2017, p.1)
[17] (FATF-GAFI 1999)
[18] (FATF-GATI 2015)
[19] (Brantly 2014)

use of cyber currencies as a method of financing operations.[20] In 2015, an American teenager pleaded guilty to teaching ISIS members how to set up Bitcoin wallets and conduct Bitcoin transactions.[21, 22] Deutsche Welle claims to have uncovered Bitcoin wallets belonging to ISIS members that had $23 million in transactions over a one month period.[23, 24] There is evidence that terrorists have successfully funded terrorist attacks with Bitcoin. Ghost Security Group, a computer hacktivist and anti-terrorist group, investigated both the 2015 shopping mall terrorist bombing in Jakarta, Indonesia[25] and the 2015 coordinated terror attacks in France. Analysis of these separate attacks led them to separate Bitcoin wallets. The French terrorists Bitcoin wallet contained $3 million.[26]

The number of cryptocurrencies and cyber markets change daily. According to Crypto-Currency Market Capitalizations, on 13 January 2018, 1,426 crypto currency and 7,908 markets were in existence.[27] One day later, there were 1429 cryptocurrencies and 7876 markets.[28] Several of the more well-known cyber currencies are Bitcoin, Dodgecoin, Peercoin, Erthereum, Ripple, Litecoin, and Dash (Darkcoin). Bitcoin can only be obtained from buying or mining. Bitcoin is the world's first decentralized currency created by Satoshi Nakamoto in 2007.[29] As outlined in his 31 October 2008 white paper titled *Bitcoin: A Peer-to-Peer Electronic Cash System*, Bitcoin uses peer-to-peer (P2P) blockchain technology that is decentralized.[30] Bitcoin's P2P blockchain technology allows for anonymity in transactions. Anonymity is possible because IP

[20] (Brantly 2014)
[21] (Irwin and Milad 2016)
[22] (Edwards 2015)
[23] (Irwin and Milad 2016)
[24] (Sanders 2015)
[25] (Pick 2015)
[26] (Sameeh 2015)
[27] (CoinMarketCap 2018)
[28] (CoinMarketCap 2018)
[29] (BitcoinWebHosting.net 2014)
[30] (Nakamoto 2008)

addresses may be spoofed by a virtual private network (VPN) or by use of the Tor Network.[31, 32] Therefore, cyber currencies allow any person with a computer or smart phone to anonymously exchange payments for goods and services outside of traditional financial regulations and regulated banking networks. These payments could be for lattes or pizza, but, more often, these anonymous cyber payments are for illicit activities, such as drugs, weapons or explosives. Obviously, anonymity is a key aspect for illegally funding VEOs. Therefore, regulation through existing banking laws is one way to stop and expose illicit fund transfers.

Anonymous, conventional transactions were targeted by FATF after the 2001 U.S. terrorist attack.[33] This crackdown extended to the seizure of numerous Bitcoins from black market websites such as the Silk Road.[34] One of the Silk Road's appeals was the anonymity of transactions. The downfall of the Silk Road in October 2013 was due to charges of money laundering, drug trafficking, and other black market activities.[35, 36] During this 2013 raid the FBI seized anywhere from 144,341 to upward of 174,000 Bitcoins, or 1.5% of the Bitcoin market.[37, 38] To date, the FBI has performed over 725 Bitcoin transactions[39] making the U.S. Government well versed as a Bitcoin operator. The FBI auctioned the seized Bitcoins for cash.

---

[31] (Cocco, Pinna and Marchesi 2017)
[32] (Tor Project 2018) Tor, short for 'The Onion Router", is a free software enabling anonymous communication. The Tor network routes Internet traffic through numerous worldwide volunteer overlay sights, or virtual tunnels, rather than making a direct connection. These virtual tunnels provide the anonymous communication, as a direct and easily traceable connection is not established.
[33] (FATF-GATI 2015)
[34] (D. Leger 2014) The "Silk Road" was a dark web Internet site using Tor for anonymity. The Silk Road was an illegal, blackmarket commerce website similar to eBay or Amazon that specialized in illegal drugs, fake passports, pornography, etc. but founded on the Dark Web. Like all websites listed on the Dark Web, IP addresses were untracable. The Silk Road was one of the first applications using anonymous cyber currencies.
[35] (Greenberg 2013)
[36] (Frizell 2015)The FBI started investigating the Silk Road in early 2012 and invested thousands of man-hours until it was shut down in October 2013.
[37] (Greenberg 2013)
[38] (Blockchain Luxemborg S.A.R.L. 2018)
[39] (Blockchain Luxemborg S.A.R.L. 2018)

The U.S. Government shut down the Silk Road, but failed to recognize the importance of regulating Bitcoin. Examples include the January 2014, shut down of Robert Faeilla's *BTCKing* and Charlie Shrem's *BitInstant.com* Bitcoin exchanges for "money laundering, operating an unlicensed money transmitting business and violating the Bank Secrecy Act by failure to file reports of suspicious activity to the federal government."[40] These same governmental agencies neglected to go after the source of funds for these illegal operations. Instead, they are prosecuting cyber currency exchange operators rather than recognizing cyber currency as a legitimate form of payment. Thus, following this methodology, the only way to stop funding VEOs is to remove the anonymity of cyber currencies. Therefore, S 1241, and its companion bill HR 4373, were drafted to specifically target cyber currencies in 2017. These are important steps towards the regulation of cyber currencies, but, in my opinion, do not go far enough. The U.S. must take a leading role in maintaining the integrity of the blockchain in order to further investigate the use of cyber currency transitions for nefarious operations.

Regulation or Ban

As time passes, cryptocurrencies are gaining popularity not only with VEOs but also with rogue nation states. Reluctance to regulate was explained during the 6 February 2018 congressional testimony where Mr. Clayton and Mr. Giancarlo described that virtual currencies do not fall neatly into any one financial category.[41] Virtual currencies can be used as a medium of exchange such as a currency, they can be used to store value like an asset, which means they can be considered a commodity, and finally, they can be sold as an investment with market variation. Therefore, they can also be considered a

[40] (Leger 2014, p. 1)
[41] (Congressional Hearing 2018)

security.[42] To further complicate matters, the Internal Revenue Service (IRS) currently categorizes cyber currencies solely as property.[43]

The U.S. should immediately define cyber currencies as a currency. The Online Markets Protection Act of 2014 (HR 5892) was a move towards doing so. Though written in 2014, it has been stuck in committee since its introduction in 2015.[44] Passage of this bill will force cyber currency exchanges to comply with existing banking regulations such as the mandatory collection of Know Your Customer (KYC) Reporting information. This information includes personable identifiable information such as social security number, proof of residence, and passport number, which will negate the P2P blockchain technology anonymity[45] and allow law enforcement agencies to trace transactions. The Online Markets Protection Act will require the IRS to clarify Bitcoin as a currency, therefore mandating the required collection of KYC data.[46, 47] Some U.S. cyber currency exchanges are gathering customer information, not because of required regulation, but instead for fear of money laundering charges and becoming the next to fall like *BTCKing* and *BitInstant.com*. Much debate exists about defining virtual currencies as a currency or commodity due to its wild, inconsistent fluctuations.[48] In my opinion, as Bitcoin and the age of virtual currencies mature, these will stabilize; thus they should be categorized and regulated as a currency.

The 2015 FATF Guidelines recommend "[e]ach country should assess the registration and license system with respect to the exchangers of virtual currencies and

---

[42] (Congressional Hearing 2018)
[43] (Ficcaglia 2017)
[44] (Congress.Gov 2015)
[45] (Ficcaglia 2017)
[46] (Zuberi 2017)
[47] Under the IRS definition of property, Bitcoin or a similar cyber currency, may be purchased by a trust or L.L.C. and can be held anonymously by an individual, trust, guild or mob.
[48] (Friedman 2017)

fiat currency, as well as regulation of [AML/CTF], such as customer identification, notification of suspicious transactions and preservation of records."[49] Many countries have already taken a firm stand on cyber currencies. Some countries have chosen to regulate them, while others are choosing to ban cyber currencies altogether. Both of these methodologies meet the goal of cutting off funding to VEOs. The U.S. is behind in this endeavor and needs to take swift action to maintain its national interests.

Japan is the only advanced economy to fully regulate cyber currencies.[50] Japan's regulation reduces the anonymity of transactions by forcing Japanese cyber currency exchanges to register with the Japanese Financial Services Agency, thereby enforcing compliance with established banking rules and regulations.[51] Unfortunately, this regulation provided limited customer protections to cyber exchange users. Japan's major cyber currency exchange, Coincheck, was hacked and $530 million in cryptocurrencies were stolen in January 2018.[52] Was this hack by VEOs or North Korea? No one knows because no one controls the blockchain.

In addition, Russia has just undergone a 180-degree turn on Bitcoin. President Vladimir Putin condemned Bitcoin and cyber currencies most recently in October 2017. However, Dmitry Marchinev, Putin's Internet ombudsman, plans to have Russia rival China in Bitcoin mining.[53] Despite his October statement, Putin has ordered his government to set up regulation and trade of Bitcoin, Initial Coin Offerings (ICOs), and mining by July 2018.[54] Russia is also creating its own cyber currency called the CryptoRuble. The CryptoRuble will exist outside of the regulated banking system, but

[49] (FATF-GATI 2015, p. 4)
[50] (Chan 2017)
[51] (Dhaka 2016)
[52] (The Associated Press 2018)
[53] (Frankenfield 2017)
[54] (Tuwiner 2017) An ICO is used by startups to bypass the rigorous and regulated capital-raising process required by venture capitalist or banks.

will be backed by the Russian Ruble. By controlling its own CryptoRuble blockchain, Russia will be able to circumvent U.S. and U.N. sanctions.[55] This fashion of cryptocurrency manipulation deeply concerns Senator Crapo as it undermines our national interests.[56]

Lastly, South Korea has finalized its decision on Bitcoin. Like Russia, it has vacillated between regulation and banning. On 11 January 2018, South Korea announced a ban on cyber currency exchanges in the morning, and later that afternoon, clarified with a much softer stance and regulatory approach.[57, 58] As the third largest cyber currency exchange, South Korean uncertainty has caused Bitcoin to lose 12% of its value on 11 January 2018 alone.[59] Ultimately, on 30 January 2018, South Korea "outlawed deposits into anonymous virtual accounts at banks and told lenders to report suspicious traders, including those who deposit or withdraw 10 million won ($9,330) or more a day from cryptocurrency venues."[60] The South Korean governments reason for regulating cryptocurrencies is to protect against money laundering, tax evasion and excessive speculation.

Many countries have chosen to ban cryptocurrencies. Bolivia, Ecuador, Kyrgyzstan, Bangladesh, Nepal, and Morocco are in this category.[61] Indonesia plans to enact a ban in 2018.[62] However, some governments are also creating their own cryptocurrency which may allow them to evade international monetary sanctions.[63, 64]

---

[55] (Jenkinson 2017)
[56] (Congressional Hearing 2018)
[57] (Iyengar 2018)
[58] (Choudhury 2018)
[59] (Choudhury 2018)
[60] (Cho 2018, p. 1)
[61] (Razani 2017)
[62] (Chan 2017)
[63] (Congressional Hearing 2018)
[64] (Mason 2017)

According to an October 2017 article, Ecuador, China, Senegal, Singapore, and Tunisia have created their own cyber currency.[65] Estonia, Japan, Palestine, Russia, Sweden, and Venezuela are looking to create their own digital currency.[66, 67] This will negate the established international banking framework.

If governments set up a new currency, why not individual companies? At first bankers were against cyber currencies. Jamie Dimon, CEO of JP Morgan Chase, skeptical at first, called Bitcoin a "fraud".[68] Mr. Dimon said Bitcoin is "worse than tulip bulbs" and further stated "…governments like to control their money supply." He believed individuals would lose their Bitcoin investments with the anticipated fall in the market. Larry Fink, CEO of BlackRock held a similar cynicism.[69] Some question banker's motives for being anti-Bitcoin, as it can be seen as challenging the banking industry. In fact, Associate Professor Beate Sauer, faculty in the Department of Economics and Law of the Global Economy for the Bundeswehr University, Munich, states that one reason cyber currencies are so popular is "[they are] a protest against authority-driven monetary policy decisions."[70] One could argue that banks, similar to governments, like to control the money supply. With the soaring popularity, ease of use, and profitable Bitcoin money exchanges, bankers are now changing their tune. On 9 January 2018, Mr. Dimon stated that he regrets his comments about Bitcoin, and can see how its ICOs and ledgers are useful to individual corporations.[71] One can predict that with the success of Bitcoin, bankers will support regulation to pull investments back into the traditional banking system.

---

[65] (Mason 2017)
[66] (Mason 2017)
[67] (Dorman 2017)
[68] (Son, Levitt and Louis 2017)
[69] (Samson 2018)
[70] (Sauer 2016, p. 1)
[71] (Samson 2018)

If governments and individual companies are creating cyber currencies so can VEOs. In my opinion, merely forcing cyber currencies to comply with existing banking laws through government regulation does not go far enough. As the world's hegemon, the U.S. must take immediate action to both regulate and mine cyber currencies, as are our adversaries.

Blockchain Technology and Computing Demands of Mining

The U.S. needs to invest in blockchain technology in order to impede VEOs funding sources. (Doing so will have the added advantage of preventing nations like Russia from evading sanctions as suggested in the February 2018 Congressional Hearing on Virtual Currencies).[72] Preventing VEOs access to cryptocurrencies may be achieved either by denying them from buying it, or, by controlling the mining of cryptocurrencies. Denying VEOs ability to "buy" P2P currencies is relatively hard.[73] However, limiting VEOs ability to mine is relatively easy. Nation states need only to mature the blockchain to a level that the hashrate cannot be met by a personal computer. China and Russia have already recognized the importance of investing in this technology.

The computing demands of mining and maintaining cyber currencies are enormous. Bitcoin creator Satoshi Nakamoto allowed only 21 million Bitcoin to be produced.[74] To date, only 16,802,462 Bitcoin have been mined.[75] Bitcoin stores both transactions and Bitcoin creation (mining) on something called a blockchain. The miners maintain the blockchain and the individual users access the blockchain "ledger." Through P2P technology, this blockchain allows all users of Bitcoin to see each and

[72] (Congressional Hearing 2018)
[73] See private movies by use of BitTorrents
[74] (Nakamoto 2008)
[75] (CoinMarketCap 2018)

every transaction.[76] As the number of Bitcoin mined increases, the mathematical algorithm required to produce a Bitcoin becomes more complex.[77] *Graph 1* shows a measure of difficulty with each block added to the chain. This means that the computer processing demand is greater with each mined Bitcoin (see *Graph 2*).[78] Since Bitcoin is the oldest cyber currency, it is further along in the mining process, thus requiring extensive computing power. Individual computing devices are no longer able to mine Bitcoin. Therefore individuals are creating network pools, computing guilds, or consortiums of computers. This level of computing power requires immense amounts of electricity that will further limit who may mine for mature cyber currencies.[79] On 9 February 2018, a group of Russian physicists were arrested for connecting an air gapped, nuclear, supercomputer to the Internet to mine Bitcoin.[80, 81] It is only a matter of time before adversarial nation states such as Russia and China choose to dedicate supercomputers.

China has recognized the importance of mining, and at 76.5%, dominates the Bitcoin mining industry at the close of 2017. [82] Many of the established mining pools have IP addresses in China.[83] *Graph 3* shows the mining consortiums by country of origin in July 2017.[84] In contrast, *Graph 4* shows the mining consortiums origins six months later in January 2018. Notice that China continues to lead in mining, but the entry of Russia since Putin's October declaration on cyber currencies. Finally, notice the

[76] (BitcoinWebHosting.net 2014)
[77] (L. M. Cocco 2016) The "algorithm" cannot be solved logically, therefore, a combination of guesses is required to "add" at transaction onto the blockchain. These guesses are called a "hash "and subsequently are measured by something called the hashrate, which is the number of guesses a computer, makes per second.
[78] (Holthaus 2017)
[79] (Holthaus 2017)
[80] (BBC News 2018)
[81] (Morris 2018)
[82] (Tuwiner 2017)
[83] (Tuwiner 2017)
[84] (Tuwiner 2017)

dismal showing by the U.S. (*Figure 1* shows each mining pool's estimated hashrate distribution and percentages of market shares).[85]

Due to the large computer consortiums and energy consumption required to mine Bitcoin, it is unlikely that VEOs will obtain Bitcoin through mining. VEOs will have a limited electrical supply and no supercomputers. Instead they will need to purchase Bitcoin or steal cyber currencies through hacking. Therefore, governments must begin to regulate Bitcoin, and other cyber currencies, as a means to stop a funding stream for VEOs. One can plainly see that other nation-states have already invested in blockchain technology. Since sanctions have tightened on North Korea, their cyber units have branched out and are conducting attacks on South Korean cryptocurrency exchanges.[86] A recent report by Recorded Future (a venture capital firm funded by the CIA) stated that North Korea is mining Bitcoin to generate wealth for the regime.[87] This report hypothesizes that North Korean could set up mining operations in other countries [China] to gain Internet access. Pricilla Moriuchi, a forensic researcher for Recorded Future, said there is clear evidence that a North Korean leader used Bitcoin to purchase a good or service. North Korea is responsible for Bitcoin exchange hacks on Seoul to the tune of $7 million.[88]

During the Virtual Currencies Senate Hearing, Senator Bob Menendez (D-NJ) asked Mr. Clayton and Mr. Giancarlo about cross-boarder and multinational aspects of Bitcoin. He specifically asked what protections are in place to protect U.S. national interests from countries such as Venezuela and Russia whom are creating there own

[85] (Blockchain Luxembourge S.A.R.L. 2018)
[86] (Pham 2017)
[87] (Chen 2017)
[88] (Chen 2017)

virtual currencies to manipulate and avoid U.S. [U.N.] sanctions.[89] Mr. Giancarlo stated that U.S. financial institutions have not looked into that aspect of virtual currencies.[90] The U.S. Department of Treasury initially raised concerns about this threat in 2014.[91] The time to act is now!

Concerns and Challenges

The biggest challenge, and it's a significant one, is that by declaring Bitcoin a currency, it could undermine the dollar on the global market. How to integrate virtual currencies in the U.S. market dominated the discussion during the 6 February 2018 congressional testimony.[92] However, in a 2016 article, Professor Sauer stated that, "neither the monetary policy making power of national central banks, nor the stability the worldwide financial system is endangered by the use of Bitcoin or any other virtual currency."[93] Financial leaders such as Mr. Dimon (JP Morgan Chase CEO) and Mr. Fink (BlackRock CEO) need to assist regulators with the implementation of cyber currency into the current banking system. This assistance should include the integration of information from the blockchain technology into current KYC and AML reporting requirements.[94] The alternative to doing nothing is to embolden financial interest in foreign countries and VEOs through the creation of their own cyber currency.

Why should the NSA dedicate computers to mining blockchain? Is this really in our national interests? Absolutely! First and most importantly, the NSA, as a miner, will have a copy of the blockchain (ledger) to more quickly analyze individual transactions, thereby the ability to quickly go after VEO's. While successful without a copy of the

[89] (Congressional Hearing 2018)
[90] (Congressional Hearing 2018)
[91] (Chen 2017)
[92] (Congressional Hearing 2018)
[93] (Sauer 2016, p. 129)
[94] (Zuberi 2017)

blockchain ledger, the FBI took two and a half years to ferret out and shut down operations on the dark web's Silk Road, allowing illegal transactions to transpire during this time. If the NSA does become a miner, it has an added benefit that when Bitcoin are mined, the value could be invested or sold to cover the energy costs. Secondly, people use Bitcoin because it is a cryptocurrency that has been holding its value in the markets. However, as the blockchain becomes longer, it takes longer for individual transactions to be processed. These transactions cannot be sped up through using the dark web or other websites. Each IP address is supplying only one block in the entire blockchain. No one enjoys the backed up check-out line in the Navy War College cafeteria because the credit card reader is slow at processing transactions. To avoid this line, people bring cash. Similarly, throwing in the NSA's computing power will allow for faster Bitcoin transactions while the blockchain continues to reach its maturity. By the NSA investing in mining technologies, users will enjoy a better customer experience. This may keep them from jumping to other cyber currencies, and prevent new cyber currencies from being developed. The real concern is what happens once all 21 million of the Bitcoin have been mined? Transaction speeds will drastically increase, making it nearly impossible for the NSA to trace without a copy of the ledger. Furthermore, this will be a mature and 'legitimized' currency despite governments' failure to recognize it as such.

Conclusion

The U.S. has two choices: bury our head in the sand and ban cyber currencies; or aggressively embrace them through regulations and policies accordingly. The biggest pump gets the water out of the aquifer before its neighbors. The U.S. can continue to be reactive in its approach to limiting VEOs ability to fund their activities by leaving things

as a status quo, or, the U.S. could quickly and aggressively enact cyber currency regulation. Japan has embraced this technology and is the only economically developed country to successfully do so. The U.S. not only needs to regulate cyber currency like Japan, but it needs to go further and actively mine. The U.S. can continue to imprison its own citizens for failure to know who is using U.S. based cyber currency exchanges, or the U.S. can lead the world in recognizing, regulation and controlling cyber currencies though effective regulation and dedication of national assets. Merely seizing all cyber currencies traded through an exchange does nothing to stop P2P transfer of funds to people who would harm the United States. Only by removing the anonymity of cryptocurrencies is it possible for the U.S. to find and subsequently, sever funding to VEOs. In addition, the U.S. must manage the blockchain. Through regulation and the dedication of national computing assets, the U.S. will be able to limit VEOs ability to fund terrorists' activities.

Afterward

In the three months since submission of this paper, three major events occurred in the virtual currency world. First, the Japanese exchange Coincheck reimbursed all 260,000 customers who lost money in the January 2018 hack, to the tune of $440 million or eighty percent of the $530 million stolen.[95] While it is still unclear who is responsible for this cyber heist (and likely will never be solved), it is clear that the 2014 Japanese regulation that all cyber exchanges register with the government, provided protections for these customers. Just a month later, Monex Group, a Japanese online broker, bought Coincheck and pledges "to provide [a] secure environment to customers and to grow sustainably as a socially valuable cryptocurrency exchanger."[96] Japan's Financial Services Agency continues to ramp up regulations to ensure exchanges are more secure.[97] Secondly, the U.S. appears more confused than ever on how to classify virtual currencies. Jack Weinstein, Senior United States District Judge, in a New York Federal Court ruled on 6 March 2018 that virtual currencies are a commodity (Case 1:18-cv-00361-JBW-RLM).[98] Meanwhile, the State of North Carolina shut down the mining company, Power Mining Pool (PMP) because, "The Securities Division found that PMP is violating the Securities Act by: a. offering unregistered securities in the form of 'mining pool shares; ' b. offering securities while it is not registered to do so; and c. making material misstatements when offering securities."[99] Meanwhile, Montana has expanded its virtual currency mining operations originating from the State funded grant

[95] (The Japan Times 2018)
[96] (Lewis and Woodhouse 2018)
[97] (The Japan Times 2018)
[98] (United States District Court Eastern District New York 2018)
[99] (Helms 2018)

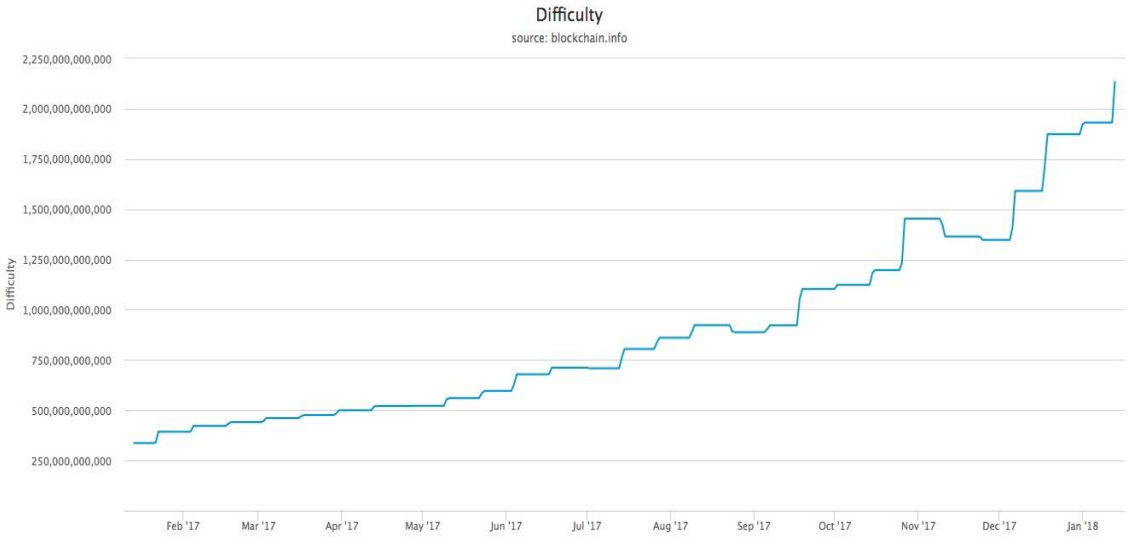
in 2017.[100] Finally, Oki Matsumoto, the CEO of Monex and a Wall Street veteran, predicts virtual currencies will stabilize and become more palatable for regulators as did derivatives the in the 1980's.[101] Time is rapidly diminishing for the U.S. to regulate, mine and own a part of the blockchain ledger for virtual currencies that will assist tracking VEOs through economic means.

[100] (Kelso 2018)
[101] (Rooney 2018)

Graph 1

Difficulty

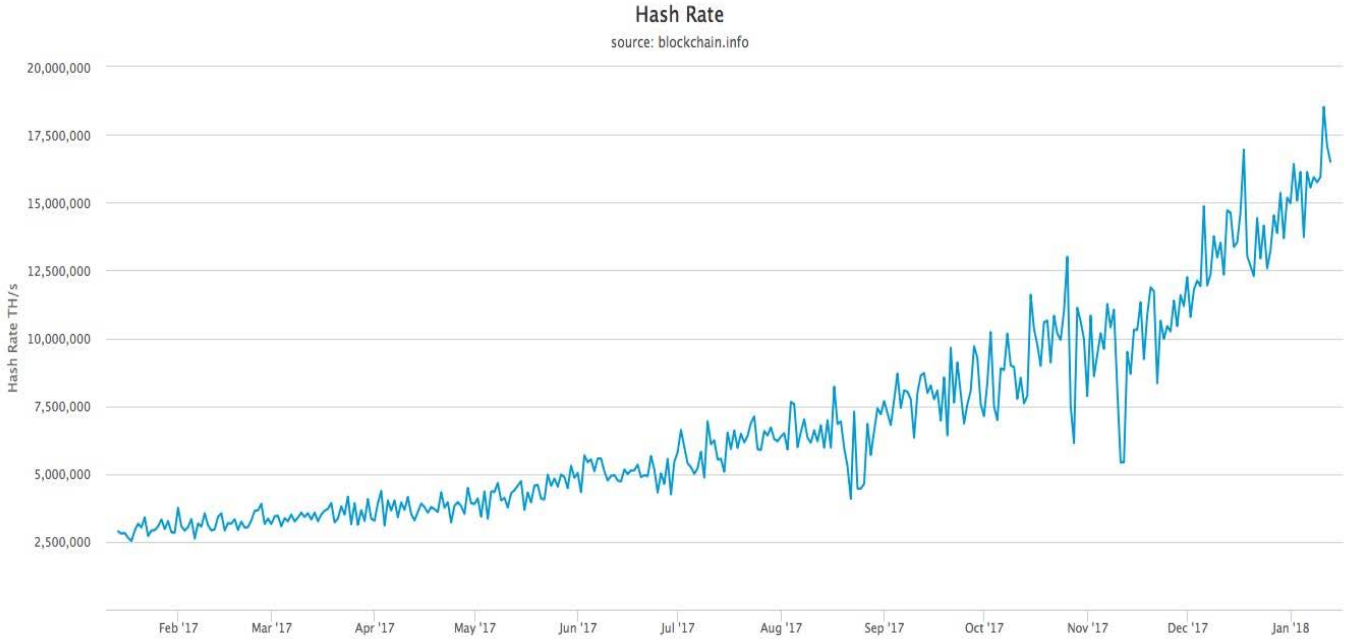
A relative measure of how difficult it is to find a new block. The difficulty is adjusted periodically as a function of how much hashing power has been deployed by the network of miners. (Obtained from Blockchain Luxemborge S.A.R.L on 14 Jan 2018)



Graph 2

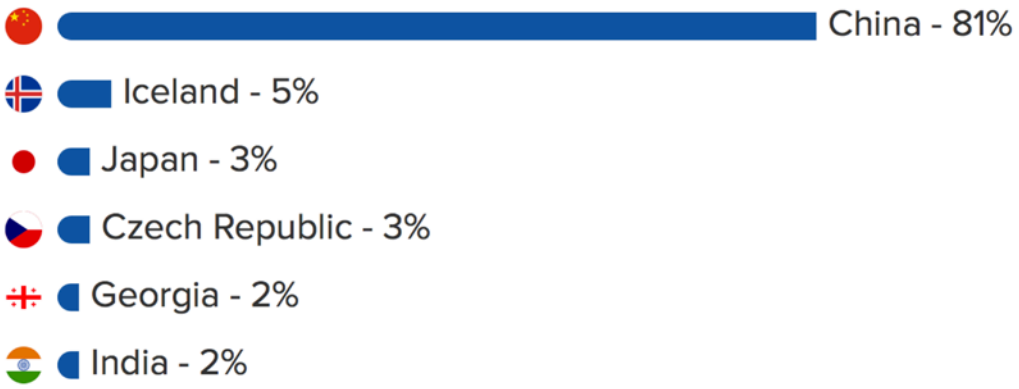
Hash Rate

The estimated number of tera hashes per second (trillions of hashes per second) the Bitcoin network is performing. (Obtained from Blockchain Luxemborge S.A.R.L on 14 Jan 2018)



Graph 3

Graph taken from *Bitcoin Mining Pools* by J. Tuwiner, 13 July 2017



Graph 4

Graph 4 is calculated from Hashrate Distribution Consortium in Figure 1 taken from Blockchain Luxembourg Consortium S.A.R.L website 14 January 2018

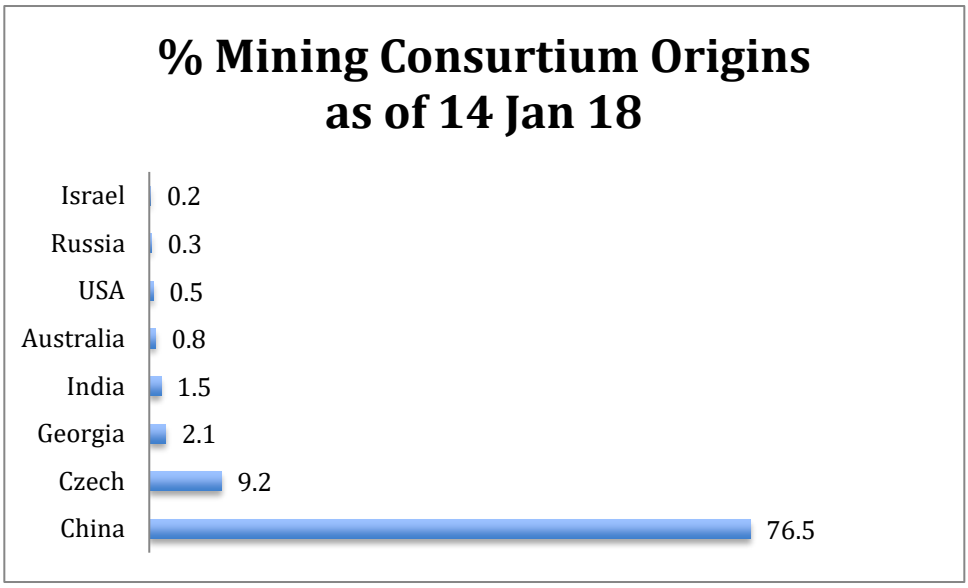
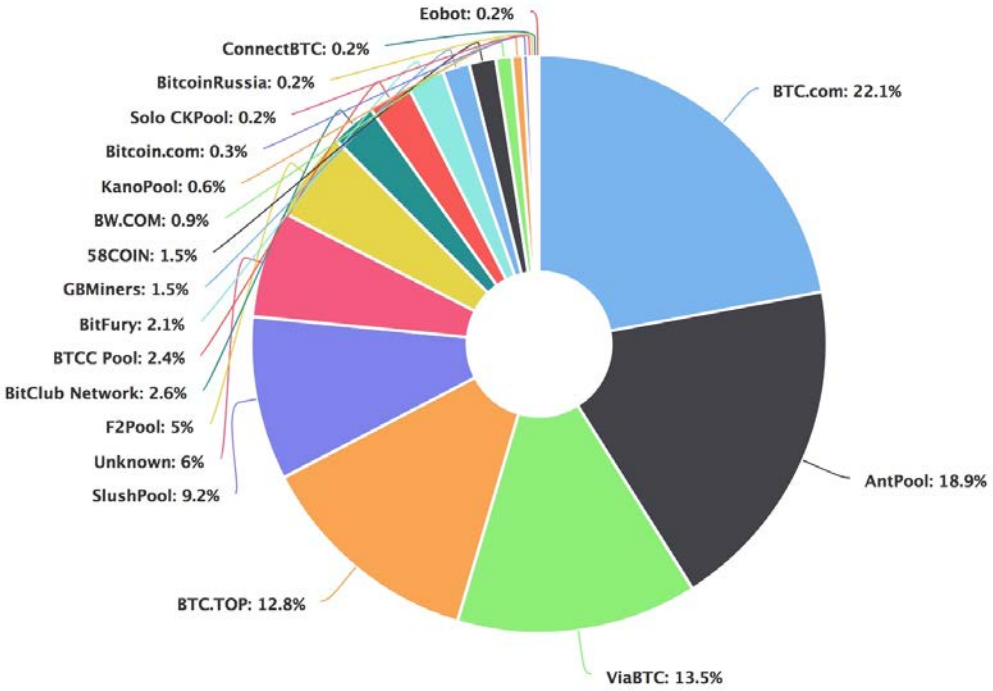


Figure 1

Hashrate Distribution taken from Blockchain Luxembourg S.A.R.L website 14 January 2018. Percentages from this figure were used to calculate *Graph 4.*



References

BBC News. *Russian Nuclear Scientists arrested for 'Bitcoin Mining Plot'.* February 9, 2018. http://www.bbc.com/news/world-europe-43003740 (accessed February 11, 2018).

BitcoinWebHosting.net. *Bitcoin History: The complete history of bitoin.* 2014. http://historyofbitcoin.org (accessed December 22, 2017).

Blockchain Luxemborg S.A.R.L. *DPR seized coins.* January 12, 2018. https://blockchain.info/address/1FfmbHfnpaZjKFvyi1okTjJJusN455paPH?offset=250&filter=6 (accessed January 14, 2018).

Blockchain Luxembourge S.A.R.L. *Hashrate Distribution.* January 14, 2018. https://blockchain.info/pools (accessed January 14, 2018).

Botos, Horia. "Bitcoin Intelligence- Business Intelligence meets Crypto Currency." *CES Working Papers* IX, no. 3 (2017): 488-505.

Brantly, A. "Financing terror bit by bit." *CTC Sentinel* (Combating Terrorism Center at West Point) 7, no. 10 (October 2014): 1-20.

Chan, K. *Asian investors embrace bitcoin, but regulators are wary.* Associated Press International. Hong Kong, December 11, 2017.

Chen, Qin. *Bitcoin 'mining': A new way for North Korea to generate funds for the regime.* September 17, 2017. https://www.cnbc.com/2017/09/13/bitcoin-mining-a-new-way-for-north-korea-to-generate-funds-for-the-regime.html (accessed Febrauary 11, 2018).

Cho, Kyungji. *Why the Cryptocurrency World is Watchign South Korea.* February 4, 2018. https://www.bloomberg.com/news/articles/2018-02-04/why-the-cryptocurrency-world-is-watching-south-korea-quicktake (accessed February 7, 2018).

Choudhury, S. *South Korea is talking down the idea of a cryptocurrency trading ban is imminent.* January 11, 2018. https://www.cnbc.com/2018/01/11/south-korea-cryptocurrency-justice-ministry-softened-stance.html (accessed January 18, 2018).

Cocco, L., Marchesi, M. "Modeling and Simulation of the Economics of Mining in the Bitcoin Market." *Plos One*, October 2016: 1-31.

Cocco, Luisanna, Andrea Pinna, and Michele Marchesi. "Banking on Blockchain: Costs Savinga Thanks to the Blockchain Technology." *Future Internet* 9, no. 25 (June 2017): 1-20.

CoinMarketCap. *Cryptocurrency Market Capitalizations.* January 13, 2018. https://coinmarketcap.com (accessed January 13, 2018).

—. *Cryptocurrency Market Capitalizations.* January 14, 2018. https://coinmarketcap.com/currencies/bitcoin/ (accessed January 14, 2018).

Congress.Gov. *H.R 5892- Online Protection Act of 2014.* January 2, 2015. https://www.congress.gov/bill/113th-congress/house-bill/5892/actions (accessed January 18, 2018).

—. *H.R.4373 - AML and CTF Modernization Act.* November 2017. https://www.congress.gov/bill/115th-congress/house-bill/4373/actions?q=%7B%22search%22%3A%5B%22HR+4373%22%5D%7D&r=1 (accessed December 10, 2017).

—. *S.1241 - Combating Money Laundering, Terrorist Financing, and Counterfeiting Act of 2017.* November 2017. https://www.congress.gov/bill/115th-congress/senate-bill/1241/all-actions?overview=closed#tabs (accessed January 13, 2018).

Congressional Hearing. *Congressional Hearing on Virtual Currencies.* February 6, 2018. https://www.c-span.org/video/?440770-1/jay-clayton-christopher-giancarlo-testify-hearing-virtual-currencies&live (accessed February 6, 2018).

Dhaka. "Japan passes law to regulate virtual currency exchanges." *The Financial Express*, May 2016: 1.

Dorman, M. *Venezuela to introduce cryptocurrency to tackle economc crisis.* December 4, 2017. https://finance.yahoo.com/news/venezuela-introduce-cryptocurrency-tackle-economic-crisis-114125417.html (accessed January 18, 2018).

Durmaz, H. "Understanding and responding to terrorism." *NATO Security through Science Series- E: Human adn Society Dynamics* 19 (2007).

Edelman, A. *rt.com.* December 4, 2017. https://www.infowars.com/u-s-moves-to-criminalize-anonymous-cryptocurrency-ownership/ (accessed December 10, 2017).

Edwards, Julia. *American Teenager Pleads Guilty to Helping Islamic State.* June 11, 2015. https://www.reuters.com/article/us-usa-security-islamicstate/american-teenager-pleads-guilty-to-helping-islamic-state-idUSKBN0OR1V520150611 (accessed February 11, 2018).

FATF-GAFI. *Report on money laundering typologies 1998-1999.* July 2, 1999. http://www.fatf-gafi.org/media/fatf/documents/reports/1998%201999%20ENG.pdf (accessed December 22, 2017).

FATF-GATI. *Guidance for a risk-based approach: Virtual Currencies.* June 26, 2015. http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf (accessed January 13, 2018).

Ficcaglia, Gregory. "Heads or Tails: How Europe Will Become the Global Hub for Bitcoin Businessif the United States Does Not Reexamine its Current Regulation of Virtual Currency." *Suffolk Transnational Law Review* 40, no. 1 (2017): 103-137.

Frankenfield, J. *How Russia plans to rival China in bitcoin mining.* August 11, 2017. https://www.investopedia.com/news/putin-advisor-raise-100-million-bitcoin-mining-venture-russia-china-rival/ (accessed January 14, 2018).

Friedman, George. *Opinion: Why it Matters if Bitcoin is a Currency or a Commodity.* December 2017, 2017. https://www.marketwatch.com/story/why-it-matters-if-bitcoin-is-a-currency-or-a-commodity-2017-12-13 (accessed February 2, 2018).

Frizell, Sam. *How the Feds Nabbed Alleged Silk Road Drug Kingpin 'Dread Pirate Roberts'.* January 21, 2015. http://time.com/3673321/silk-road-dread-pirate-roberts/ (accessed February 8, 2018).

Greenberg, A. *FBI says it's seized $28.5 million in bitcoins from Ross Ulbricht, alleged owner of silk road.* October 25, 2013. https://www.forbes.com/sites/andygreenberg/2013/10/25/fbi-says-its-seized-20-million-in-bitcoins-from-ross-ulbricht-alleged-owner-of-silk-road/ (accessed January 14, 2018).

Haesly II, Kenneth. "How to Solve a Problem Like Venezuela? An Argument for Virtual Currency." *Law and Business Review of the Americas* 22, no. 3 (2016): 261-269.

Helms, Kevin. *U.S. Sate Shuts Down Cryptocurrency Mining Company.* April 26, 2018. https://news.bitcoin.com/us-state-shuts-down-cryptocurrency-mining-company/ (accessed May 3, 2018).

Holthaus, E. *Bitcoin could cost us our clean-energy future.* December 5, 2017. https://grist.org/article/bitcoin-could-cost-us-our-clean-energy-future/ (accessed December 10, 2017).

Huckle, Steve, and Martin White. "Socialism and the Blockchain." *Future Internet* 8, no. 49 (October 2016): 2-15.

Irwin, Angela, and George Milad. "The Use of Crypto-Currencies in Funding Violent Jihad." *Journal of Money Laundering Control* (Emerald Group Publishing Limited) 19, no. 4 (2016): 407-425.

Iyengar, R. *Bitcoin-crazy South Korea may face ban on cryptocurrency trading.* January 11, 2018. http://money.cnn.com/2018/01/11/technology/south-korea-bitcoin-ban-bill-minister/index.html (accessed January 18, 2018).

Jackson, J. "The financial action task force: an overview." Congressional Research Service, 2017.

Jenkinson, G. *Bitcoin will be legal in Russia, mining to be regulated.* December 7, 2017. https://cointelegraph.com/news/bitcoin-will-be-legal-in-russia-mining-to-be-regulated (accessed January 14, 2018).

Kelso, C. Edward. *Montana is Home to New 53 Acre, $75 Million Bitcoin Mining Facility.* February 2, 2018. https://news.bitcoin.com/montana-is-home-to-new-53-acre-75-million-bitcoin-mining-facility/ (accessed May 3, 2018).

Kretzberg, A., interview by T Ostrom. *Personal Conversation* (May 2014).

Leger, D. *Bitcoin dealers charged with money laundering.* January 27, 2014. https://www.usatoday.com/story/tech/2014/01/27/bitcoin-dealers-charged-with-money-laundering/4941313/ (accessed January 18, 2018).

Leger, Donna. *How the FBI brought down cyber-underworld site Silk Road.* May 15, 2014. https://www.usatoday.com/story/news/nation/2013/10/21/fbi-cracks-silk-road/2984921/ (accessed February 8, 2018).

Lewis, Leo, and Alice Woodhouse. *Monex Buys Cryptocurrency Exhange Coincheck for ¥3.6bn.* April 6, 2018. https://www.ft.com/content/9063b3e6-397b-11e8-8eee-e06bde01c544 (accessed May 3, 2018).

Mason, B. *The next cryptocurrency evolution: countries issue their own digital currency.* October 15, 2017. https://finance.yahoo.com/news/next-cryptocurrency-evolution-countries-issue-113110663.html (accessed January 18, 2018).

Morris, Chris. *Russia Arrests Nuclear Scientists Who Used a Supercomputer to Mine Bitcoin.* February 9, 2018. http://fortune.com/2018/02/09/russia-arrests-nuclear-scientists-bitcoin/ (accessed February 11, 2018).

Nakamoto, S. *Bitcoin: A peer-to-peer electronic cash system.* October 31, 2008. https://bitcoin.org/bitcoin.pdf (accessed January 13, 2018).

Nardo, M. "Building synergies between theory and practice: countering financial crime on a systematic approach." *Journal of Financial Crime* 13, no. 3 (2006).

Nauert, H. *ISIS Parks Its Cash in Bitcoin, Experts Say.* November 25, 2015. http://www.foxnews.com/tech/2015/11/25/isis-parks-its-cash-in-bitcoin-experts-say.html (accessed February 11, 2018).

Pham, Sherisse. *North Korea is Trying to Amass a Bitcoin War Chest.* September 12, 2017. http://money.cnn.com/2017/09/12/technology/north-korea-hackers-bitcoin/index.html (accessed February 11, 2018).

Pick, Leon. *Jarkarta "Toilet Bomber" Demanded 100 Bitcoins, Inspired by ISIS.* February 11, 2015. https://www.financemagnates.com/cryptocurrency/news/jakarta-toilet-bomber-demanded-100-bitcoins-inspired-by-isis/ (accessed February 11, 2018).

Price, R. *The 21 companies that control bitcoin.* August 13, 2015. http://www.businessinsider.com/bitcoin-pools-miners-ranked-2015-7/#21-unknown-entity--01-1 (accessed January 14, 2018).

Razani, A. *Counties that have banned cryptocurrency for now.* December 19, 2017. https://coinclarity.com/countries-that-have-banned-cryptocurrency-for-now/ (accessed January 18, 2018).

Rooney, Kate. *Wall Street Veteran and CEO of Japanese Online Broker Says Cryptocurrencies Could Take Off Like Derivatives Did.* May 1, 2018. https://www.marketwatch.com/story/why-it-matters-if-bitcoin-is-a-currency-or-a-commodity-2017-12-13 (accessed May 3, 2018).

Sameeh, T. *ISIL Militants Linked to France Terror Attacks Had a Bitcoin Address with 3 Million Dollars.* November 14, 2015. http://www.newsbtc.com/2015/11/14/isil-militants-linked-to-france-terrorist-attacks-had-a-bitcoin-address-with-3-million-dollars/ (accessed February 11, 2018).

Samson, Adam. *Jamie Dimon: 'I regret" calling bitcoin a fraud.* January 9, 2018. https://www-ft-com.usnwc.idm.oclc.org/content/e04e359a-e9e9-3f8e-8e2f-3f4373e5efb0 (accessed January 18, 2018).

Sanders, L. *Bitcoin: Islamic State's online currency venture.* September 20, 2015. http://www.dw.com/en/bitcoin-islamic-states-online-currency-venture/a-18724856 (accessed February 11, 2018).

Sauer, Beate. "Virtual Currencies, the Money Market, and Monetary Policy." *International Advvances Economic Research* (Springer) 22 (April 2016): 117-130.

Shinkman, P. *Obama: 'Global War on Terror' is over.* May 23, 2013. https://www.usnews.com/news/articles/2013/05/23/obama-global-war-on-terror-is-over (accessed January 14, 2018).

Son, Hugh, Hannah Levitt, and Brian Louis. *Jamie Dimon slams Bitcoin as a 'fraud'.* September 12, 2017. https://www.bloomberg.com/news/articles/2017-09-12/jpmorgan-s-ceo-says-he-d-fire-traders-who-bet-on-fraud-bitcoin (accessed January 14, 2018).

Temple-Raston, Dina. *How Much Does a Terrorist Attack Cost? A Lot Less Than You'd Think.* June 25, 2014. https://www.npr.org/sections/parallels/2014/06/25/325240653/how-much-does-a-terrorist-attack-cost-a-lot-less-than-you-think (accessed February 11, 2018).

The Associated Press. *$530 million lost in hack of Japan cryptocurrency exchange.* January 26, 2018. http://abcnews.go.com/International/wireStory/530-million-lost-hack-japan-cryptocurrency-exchange-52644064 (accessed February 8, 2018).

The Japan Times. *Hacked Japanese Cryptocurrency Exchange Coincheck Refunds Customers.* March 13, 2018. https://www.japantimes.co.jp/news/2018/03/13/business/corporate-

business/hacked-japanese-cryptocurrency-exchange-coincheck-refunds-customers/ (accessed May 3, 2018).

Tor Project. *Tor Overview.* January 2018. https://www.torproject.org/about/overview.html.en (accessed February 7, 2018).

Tuwiner, J. *Bitcoin mining pools.* July 13, 2017. https://www.buybitcoinworldwide.com/mining/pools/ (accessed January 14, 2018).

United States District Court Eastern District New York. "Case 1:18-cv-00361-JBW-RLM." *Commodity Futures Trading Commission.* March 6, 2018. https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoindroporder030618.pdf (accessed May 3, 2018).

Virga, Joy Marie. "International Criminals and their Virtual Currencies: The Need for an International Effort in Regulating Virtual Currencies and Combating Cyber Crime." *Revista de Direito Internacional (Brazilian Journal of International Law)* 12, no. 2 (2015): 511-526.

Wile, Rob. *Supporter of Extremist Group ISIS Explains How Bitcoin Could Be Used to Fund Jihad.* July 8, 2014. https://www.businessinsider.com.au/isis-supporter-outlines-how-to-support-terror-group-with-bitcoin-2014-7 (accessed February 11, 2018).

Zuberi, Madiha. "A Silver ('Chain') Lining: Can Blockchain Technology Succeed in Disrupting the Banking Industry?" *Banking & Financial Services Policy Report* 36, no. 3 (March 2017): 1-4.