ASA

Risk Consultants

Research Note

Money from Nothing: The Socioeconomic Implications of "Cyber-currencies"

By: Justin Brecese

Keywords: virtual currency, digital currency, Bitcoin, risk, economics

Abstract – This research note holistically examines the phenomena of "cyber-currencies" by delineating the primary types currently in circulation, identifying the risks associated with each, and ultimately providing a high-level risk assessment of the overall landscape. While "crypto-currency" such as *Bitcoin* tends to dominate the news, myriad other forms of "cyber" or "digital" currencies exist, each posing their own risks. For this reason, I argue that it is important to establish the differences between these currencies and to understand the scope and implications of each.

Introduction

"Virtual currency" has recently been gaining a notable amount of attention from the media, the federal government, and private investors. But what is it exactly? The U.S. Department of the Treasury Financial Crimes Enforcement Network (FinCEN) states that virtual currency is: "a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction."[1] Even though this type of currency lacks any "legal tender status"—i.e. official government backing—a large draw towards certain versions of cyber-currency is their promise of anonymity in an increasingly surveilled world. Privacy is the primary attribute surrounding much of the more prominent digital currencies, such as *Bitcoin*, lending to their increasing popularity. Specifically, currencies like *Bitcoin* can be understood as "peer-to-peer" systems which, "endeavor to re-establish both privacy and autonomy by avoiding the banking and government middlemen."[2] The key is that these currencies are decentralized, unsupported by any government, anonymous, and entirely immaterial; all attributes which make them

potentially disruptive to economies across the globe, via the risks they bear for citizens, institutions and governments.

These definitions are fairly broad and overarching, however, and a distinction should be made between the different types of "cyber-currencies" in order to garner a holistic understanding of their functionality and implications. As with most relatively new technology-based issues there are many terms floating around the media and public discourse, often used interchangeably—much to the detriment of properly understanding crucial nuances or differences between particular concepts. FinCEN's recent paper briefly describes the differences between several types of virtual currencies, but only does so to describe the basic mechanics of each for regulatory purposes.[3] There are currently at least four terms that tend to be used interchangeably in the discourse on this subject: *virtual currency*, *digital currency*, *crypto-currency* and *electronic money* (or *e-money*). To establish a comprehensive examination of these four separate-but-similar concepts, this research note will use the moniker "cyber-currency" as an umbrella term for all types of currency discussed herein. More specifically, *crypto-currencies* will be examined as a subset of *digital currencies*, which should not be confused with *virtual*

currencies—all three of which differ from *e-money*. It should also be noted that all forms of cyber-currency *are* linked to "real world" economics—some just more overtly than others. This paper will break the issue of cyber-currency down into its components, examining each sub-type with the intent of constructing a "wide angle" view of the issue along with identifying the primary risks involved. Finally, following these delineations and risk identifications will be a high-level risk assessment of the current cyber-economic milieu using the three-step process outlined by the COSO internal controls framework.[4]

Virtual Currency

The term "virtual currency" is linked to virtual economies that develop within (and rely upon) the context of specific virtual environments or worlds, such as those found in massively multi-player online role-playing games (MMORPGs) such as *World of Warcraft*, or simulations like *Second Life*.[5] Virtual currencies are largely restricted to their respective virtual environments, with no *direct* ties to the physical economy. That said, one obvious overlap can be seen in the fact that items and money from virtual worlds do sell for "real world money"—whether going against the policies of game companies and selling virtual items through online commerce websites such as Ebay, or

participating in sanctioned in-game "micro-transactions."[6] One critical distinction between this form of virtual economics and others, however, is the fact that no "real" goods or services are delivered as a result of a virtual economic exchange. Even in instances where actual currency is exchanged for virtual goods or services, the goods or services that are delivered are non-existent outside of their respective virtual context.

So with virtual currency being tethered to virtual worlds, it seems as though there might not really be any significant risks involved. This is a false notion, however. While certainly less risky than other forms of cyber-currency, there are still several issues that arise from these "virtual economies." For one, as with real economies, black markets and crime tends to spring up within bustling virtual economies—and such crime can have effects that reach the "real world" economy. For example, in 2006 there was a large-scale "virtual banking" incident in a game titled *Eve Online* wherein one of the in-game virtual bank executives essentially ripped off thousands of players, selling their bank deposits and collateral on the in-game black market for a real cash payout of $120,000.[7]

It does not take a stretch of the imagination to see the mimesis in activity such as this with the rash of similar real-world corporate scandals in recent years. Other scenarios arise in virtual economies where virtual "crime syndicates" steal from other players within the virtual worlds to ultimately turn a real cash profit from their stolen items and pilfered virtual currency.[8] Another particular incident that hit the media involved a profitable brothel being run within a game called *The Sims*. In this incident, one player was banned from the game because he discovered that the in-game brothel's madam was actually a 17-year-old boy and exposed his identity.[9] This incident not only raised questions of "virtual crime" and selling the in-game virtual currency for real money but also issues of censorship, anonymity online, and the exposure of children to inappropriate scenarios were raised. Two of these issues, censorship and online anonymity, are central to other forms of cyber-currency, the implications of which will be expanded upon later in this research note. Other risks with virtual currency include the potential for addiction and resultant over-spending.[10] Gaming in itself has a tendency to be addicting which, coupled with the engrossing, vicarious living experience provided by MMORPGs and (aptly titled) "life simulators," makes it even easier to

"hook" players. Overall though, virtual currencies and their risks remain somewhat contained due to their largely restricted nature. Other cyber-currencies, conversely, are free of this limitation.

E-currency

As with "virtual currency," the term "digital currency" has a tendency to be loosely used in reference to any form of cyber-currency and/or electronic commerce (*e-commerce*). Perhaps most importantly, a differentiation must be made between the concept of *e-currency* (or *e-money*) and other types of digital currencies since their functionality and risks can vary quite drastically. "E-currency" is defined as "a type of currency in electronic form that is designed especially for paying for goods and services bought on the Internet."[11] Again, this is a very broad definition. The distinguishing factor is that e-money is directly linked to legal tender—i.e. centralized currency that is backed by governments and central banks existing in the physical world. It should essentially be understood as electronic payments or money transfers that are used for purchasing "real" goods online. In a nutshell, e-money is a traceable electronic transfer of legal tender from one person or entity to another, through a regulated third party, typically in exchange for real goods or services. Direct deposits, electronic funds transfers (EFTs), payment

processors, and electronic "wallets" are some examples of e-money systems.

Risks surrounding these forms of electronic payment and e-money are primarily embedded in information security issues. Since this type of currency is directly linked to legal tender, it does not generate quite as many risks as other forms of cyber-currency. Concerns with e-money transactions lie primarily in fraud, identity theft, data breaches, and other cyber-attacks on individuals or financial institutions, which result in loss of availability for the institution(s) or loss of confidentiality for personal financial credentials.[12] Of course fraud, identity theft and theft in general have long been concerns in the "real world" banking and finance sector, which have spread to the "virtual world" of the e-transactions and e-banking as many other crimes have.

Digital Gold

Beyond this type of e-money, other digital currencies have evolved that are not directly tied to legal tender. A relative to the above-described forms of e-money are digital gold currencies (DGCs) such as *e-gold*, *OS-Gold*, and *e-Bullion*—two of which are now defunct. As the name implies, digital gold currencies are based on precious metals (typically gold bullion) and are privately backed as opposed to

nationally-controlled legal tender.[13] DGCs pose more substantial risks to their investors than e-money largely because of their private backing. This means, among other things, a higher risk of volatility in the market. There is also the issue of DGCs functioning as international currencies. Because they are backed by precious metals, rather than national legal tender, they allow for easy trade and transactions across borders without going through "official" channels. This notion generates new risks, as DGCs can easily be used towards nefarious ends such as illicit purchases, money laundering, and funding terrorist groups or other criminal organizations. It does so though the fact that many exchanges only require minimal sign-up credentials, meaning transactions in DGC can not only cross borders easily, but they can do so with relative anonymity.[14] That said, *crypto-currency*, the final type of cyber-currency that will be discussed, has taken this ability much further by basing itself entirely upon anonymity.

Introduction to Crypto-currency

Crypto-currencies emerged following Satoshi Nakamoto's 2008 paper detailing the (then only theoretical) *Bitcoin* protocol.[15] This type of cyber-currency has recently become fairly popular worldwide, garnering widespread media attention and notable investors—such as

the Winklevoss twins of Facebook-related "fame" who own millions of dollars' worth of Bitcoins.[16] What differentiates crypto-currencies from the other forms of cyber-currency discussed thus far is also what makes them far more risky—they are de-centralized, anonymous, and highly volatile as a result.[17] But even with the risks involved, these currencies have been gaining a lot of attention this year. This is likely because the very factors that make it so risky are also what make it attractive—that is, the resistance to any form of censorship or tracking/monitoring of transactions by governments or institutions. In a sense, crypto-currency is "pure" currency; it is the essence of the economic concept. Put simply, because it is decentralized and unregulated by any third party, it can only exist if people accept and circulate it as a medium of exchange and its exchange rate is purely based upon its circulation.

Political Motivation

Because of their foundation in online privacy and anonymity, crypto-currencies are inherently politically charged. This fact alone makes them a more significant threat to existing economic systems and institutions than other forms of privately-backed digital currencies. They carry with them the weight of a specific movement advocating resistance to surveillance and the lack of privacy in the digital age that

dates (at least) as far back as the 1980s when Timothy May began distributing *The Crypto Anarchist Manifesto*. In other words, crypto-currency is absolutely not just another digital currency, it is symbolic of a particular counter-culture and belief system. Indeed, activists which identify themselves as *Crypto Anarchists* and/or *Cypherpunks* are largely responsible for the foundational concepts embodied by crypto-currencies.[18] This anonymity-as-a-lifestyle or political statement is reflected in the very fact that the name "Satoshi Nakamoto," creator of Bitcoin, is a pseudonym. The identity of the original creator is unknown, and there is even uncertainty over whether or not it is one person or multiple. The pseudonym, "Satoshi Nakamoto," is theorized as being a reference to William Gibson's Japanese-inspired cyberpunk culture of the 1980s, meaning there is no evidence that the writer is actually even Japanese.[19] Today, crypto-currencies are relied upon for anonymous transactions across the globe—many of which, of course, are not legal.

The Breadth of Crypto-currencies and Associated Risks

While *Bitcoin* is the most well-known and widely circulated crypto-currency, it is not the only one. Many others exist (roughly 40+), some notable ones being: *Litecoin*, *PPCoin*, and *Namecoin*, which are all either minor variations of, or at least highly inspired by, the *Bitcoin*

protocol developed by Nakamoto.[20] To get an idea of how large crypto-currency has gotten in recent years, there are currently almost 11.25 million Bitcoins in circulation, which by the exchange rate at the time of this writing is roughly 1.386 billion U.S. dollars' worth.[21] With this much already in circulation, and such a volatile exchange rate—spiking to above $260 and falling below $100 within a span of one month—the continually growing amount of crypto-currency being globally circulated demands attention.[22] This form of decentralized currency is risky to both investors and established institutions. Its inherently IT-based nature further interweaves the finance and IT critical infrastructure sectors, exposing both to the risks imposed by a globally-traded ethereal form of digital currency which has zero ties to any third party institutions (public or private).

Along with the economic risks imposed on investors due to market volatility and unreliability, there is a long list of other risks generated by anonymous, decentralized currencies. For instance, with crypto-currencies there is a lack of consumer protection, dispute resolution mechanisms and deposit insurance, leaving consumers fairly vulnerable to losses.[23] Beyond consumer vulnerability, these currencies also allow for circumventing laws and committing crimes such as: tax

evasion, potential violations of securities laws, money laundering, terrorism funding, and the sale and purchase of any type of illegal goods imaginable (as seen on "underground" websites like the infamous *Silk Road*).[24] The fact of the matter is that using these currencies means supporting an "underground economy," so whether or not a consumer using crypto-currency is breaking any laws, he/she is still propagating a system which works to subvert existing government-backed economic systems.

Risk Analysis of Cyber-currencies

Now, with each type of cyber-currency defined and contextualized, the next step is to further assess the risks that have been identified. The table on the following page (Figure 1) outlines the list of risks identified thus far and maps them accordingly to each of the cyber-currency types. It shows the general areas of impact as well as measures of risk on a four-point scale. Measures of risk magnitude were determined based on a correlation of the significance of each risk and their respective likelihood or frequency of occurrence—following the first two steps of the COSO three-step risk assessment process.[25] It must be noted, however, that these are merely approximations based on qualitative research of secondary sources and should therefore not

be taken at face value. The risk magnitude scale for Figure 1 should be interpreted as such:

- **N/A** = That particular risk is not really applicable to that particular cyber-currency; its likelihood or frequency is close to zero
- **Low** = That particular risk would not have a strong impact and/or is unlikely to occur
- **Medium** = That particular risk could have a moderate impact and might occur
- **High** = That particular risk could have a large impact and it is likely to occur

Areas of Highest Impact				Notable Risks	Cyber-Currencies: E-Money	Virtual Currency	Digital Gold	Crypto-Currency
				Market Volatility	Low	High	Medium	High
				Lack of Consumer Protections / Insurance	N/A	Medium	High	High
				Addiction/Over Spending	N/A	Medium	N/A	N/A
				Anonymity	N/A	Medium	High	High
				Data Breaches	Medium	Medium	Medium	Low
				Cyber "Attacks"	Medium	Medium	Medium	Low
				Theft	Medium	High	Medium	Low
				Fraud/Identity Theft	Medium	Medium	High	High
				Unmediated International Trade	N/A	Low	High	High
				Lack of Regulation	Low	Low	High	High
				Black Markets	N/A	High	High	High
				Securities Law Violations	Low	N/A	High	High
				Tax Evasion	Low	Medium	High	High
				Money Laundering	Low	Medium	High	High
				Terrorism Funding	Low	N/A	High	High

Figure 1: (Approximated) Risk Assessment Table for Cyber-Currencies

Regulations (or Lack Thereof)

Currently there is little regulation on most of these currencies and it is difficult to pin them to existing financial laws since they operate independently of government-backed legal tender. Of course, with

crypto-currencies being such a controversial topic, the US Government has not turned a blind eye—even though they do not consider "virtual currencies" such as Bitcoin to be the same as money.[26] FinCEN's recently issued guidelines outline how the various types of cyber-currencies shall be regulated, including the application of "money-laundering rules" to what they call "convertible virtual currency."[27] What distinguishes FinCEN's definition of "convertible virtual currency" from other virtual currencies is that it "has an equivalent value in real currency or [it] acts as a substitute for real currency."[28] One factor of this enforcement worth noting is that it functions alongside the Bank Secrecy Act and only applies to "money transmission service[s]," rather than individual users of convertible virtual currency.[29] This means that cyber-currency exchanges, and financial institutions which conduct business with said exchanges, are the entities susceptible to these rules put forth by FinCEN.

In the wake of these guidelines, government agencies have already made large moves against Bitcoin exchanges. Charges have been brought against Liberty Reserve, a Costa Rican exchange, with accusations of having laundered billions of dollars.[30] The U.S. Treasury Department is also proposing rules to "prohibit regulated financial

institutions from doing business with anyone who processes Liberty Reserve transactions."[31] Similarly, some U.S. accounts of Mt. Gox, the largest of all Bitcoin exchanges, were also frozen, and the Department of Homeland Security has ordered services not to do business with Mt. Gox.[32] Mt. Gox processes roughly 75% of all Bitcoin transactions, so halting their US activity is not insignificant.[33]

Moving Forward

With the future of these crypto-currencies being so uncertain, and the government beginning to take actions towards mitigating some of the risks involved, there are mixed reactions and opinions surrounding what will happen next and what should be done (if anything). The fact that many digital currencies, such as *e-bullion*, have fallen in the past due to illegal activities, aids in the wealth of public speculation that it is only a matter of time until the government takes down the current heavy-hitter—Bitcoin.[34] Others believe the IRS is likely to follow FinCEN and issue tax-reporting rules for Bitcoin users and exchanges.[35] Also, as expected, many existing businesses built on digital currencies are now trying to quickly ensure their compliance with the recent FinCEN rules so as to avoid a similar fate to what Liberty Reserve now faces.[36] All the

while, the debate over whether or not these currencies *should* be regulated still rages on as well.

In the end, if these currencies continue to grow, their associated risks will grow with them. Some of the risks involved may even out, such as their volatility and other consumer-centered risks, but the larger risks to governments and regulated financial institutions will only grow with the popularity of crypto-currencies. The intrinsically political nature of this currency cannot be ignored as it intentionally flies in the face of government-regulated money. Put simply, a decentralized and entirely anonymous currency will always harbor the risk of allowing for serious illegal activities such as tax evasion, black market dealings, money laundering and terrorist funding (to name a few). So regardless of whether one stands for restoring privacy in the electronic age, the risks that must be weighed against our desire for anonymity in transactions are heavy. Unfortunately, with the issue of crypto-currencies we stand on a cusp, upon which there can only be room for either privacy or security, not both. So which one wins in the end? The impossible nature of having to make such a decision is the very reason such currency will never truly flourish.

References

[1] "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies." 2013. *FinCEN*. 2013. <http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html>.

[2] Reitman, Rainey. "Bitcoin - a Step Toward Censorship-Resistant Digital Currency." 2011. *EFF: Electronic Frontier Foundation.* 2013. <https://www.eff.org/deeplinks/2011/01/bitcoin-step-toward-censorship-resistant>.

[3] "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies." 2013.

[4] Moeller, Robert R. *COSO Enterprise Risk Management: Establishing Efective Governance, Risk, ad Compliance Processes*. Hoboken, NJ: John Wiley & Sons, Inc., 2011.

[5] Castronova, Edward. "On Virtual Economies." 2003. *Game Studies.* 2013. <http://www.gamestudies.org/0302/castronova/>.

[6] Halliday, Simon. "The Future of Virtul Economies and MMORPGs." 2012. 2013. <http://www.digitalgameplay.com/the-future-of-virtual-economies-and-mmorpgs/>.
Wright, Lee. "MMORPG Microtransactions: Real Money for Virtual Items." 2009. *Yahoo! Voices.* 2013. <http://voices.yahoo.com/mmorpg-microtransactions-real-money-virtual-items-5022448.html?cat=19>.

[7] Halliday, 2012

[8] Schaefer, Jim. "Sex and the Simulated City: Virtual world raises issues in the real one." 2004. *Detroit Free Press.* 2013. <http://web.archive.org/web/20050716075604/http://www.freep.com/news/mich/sims27_20040127.htm>.

[9] Ibid.

[10] "Virtual Currency." 2013. *Internet Safety Project.* 2013. <http://www.internetsafetyproject.org/wiki/virtual-currency>.

[11] "e-currency." n.d. *Cambridge Dictionaries Online.* 2013. <http://dictionary.cambridge.org/us/dictionary/business-english/e-currency>.

[12] "E-Banking Risks." n.d. *FFIEC IT Examination HandBook InfoBase.* 2013. <http://ithandbook.ffiec.gov/it-booklets/e-banking/e-banking-risks.aspx>.

[13] "Digital Gold Currency – DGC." *Investopedia*. 2013. <http://www.investopedia.com/terms/d/digital-gold-currency-dgc.asp>.

[14] "Regulators worry about digital gold currency's potential as tool for criminal activity." 2008. *International Business Times.* 2013. <http://www.ibtimes.com/regulators-worry-about-digital-gold-currencys-potential-tool-criminal-activity-220989#>.

[15] Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." 2009. *Bitcoin.* 2013. <http://bitcoin.org/bitcoin.pdf>.

[16] Cowley, Stacy. *The Winklevoss twins are Bitcoin bulls*. 2013. 2013. <http://money.cnn.com/2013/05/18/investing/winklevoss-bitcoin/index.html>.

[17] For more information on how this currency works, see: http://www.theblaze.com/stories/2013/04/10/confused-by-digital-currency-this-three-minute-video-has-basics-of-what-you-need-to-know-about-bitcoins/# For information on the Bitcoin mining process, see: http://www.huffingtonpost.com/jesse-seaver/mining-for-digital-gold-n_b_3158988.html

[18] For more information, Tim May's *Crypto Anarchist Manifesto* can be read at: http://activism.net/cypherpunk/crypto-anarchy.html; Eric Hughes' *Cypherpunk's Manifesto* can be read at: http://activism.net/cypherpunk/manifesto.html

[19] Worstall, Tm. "Ted Nelson Says That Bitcoin's Satoshi Nakamoto Is Shinichi Mochizuki." 2013. *Forbes.* 2013. <http://www.forbes.com/sites/timworstall/2013/05/19/ted-nelson-says-that-bitcons-satoshi-nakamoto-is-shinichi-mochizuki/>.

[20] Siluk, Shirley. *What other digital currencies are there?* 2013. 2013. <http://www.coindesk.com/what-other-digital-currencies-are-there/>. xorxor. *List of all cryptocoins*. 2013. 2013. <https://bitcointalk.org/index.php?PHPSESSID=t5q6nm854i2lh24hmak7vff397&topic=134179.0>.

[21] *Total Bitcoins in Circulation*. 2013. 2013. <http://blockchain.info/charts/total-bitcoins>. *Simple Bitcoin Converter*. 2013. 4 June 2013. <http://preev.com/>.

[22] Fowlkes, Michael. *Bitcoin volatility spikes again as Silk Road website crashes*. 2013. 2013. <http://www.marketintelligencecenter.com/articles/276221>.

[23] Duhaime, Christine. *The dangers of bitcoin – the legal risks it poses to consumers and the particular risks it poses in combatting terrorist financing and money laundering*. 2013. 2013. <http://www.duhaimelaw.com/2013/04/21/bitcoin-virtual-currencies-and-the-legal-risks-they-pose-to-consumers-and-the-particular-risks-they-pose-in-combatting-money-laundering-and-terrorist-financing-initiatives/>.

[24] *The Silk Road* is an "underground" black market website which uses the *Tor* network for anonymity. A wide array of goods are sold on the site, with a focus on illegal narcotics and drug paraphernalia. Everything on the site is bought and sold for *Bitcoins*. The website cannot be reached unless the user is operating on a Tor browser. For more information on *The Silk Road*, see: http://gizmodo.com/5805928/the-underground-website-where-you-can-buy-any-drug-imaginable. For more information on the *Tor* project, see: https://www.torproject.org/

[25] Moeller, 2011

[26] Fuchs, Erin. *Why The Feds Aren't Shutting Down Bitcoin — At Least Not Yet*. 2013. 2013. <http://www.businessinsider.com/is-bitcoin-legal-2013-4>.

[27] Lamm, Jim. *Convertible Virtual Currency (Like Bitcoin) is Subject to U.S. Money-Laundering Rules*. 2013. 2013. <http://www.digitalpassing.com/2013/03/22/convertible-virtual-currency-bitcoin-money-laundering-rules/>.

[28] Ibid.

[29] Ibid.

[30] Albergotti, Reed and Jeffrey Sparshott. "U.S. Says Firm Laundered Billions." 2013. *The Wall Street Journal.* 2013. <http://online.wsj.com/article/SB10001424127887323855804578511121238052256.html?mod=business_newsreel>.

[31] Santora, Marc, William K. Rashbaum and Nicole Perlroth. "Online Currency Exchange Accused of Laundering $6 Billion." 2013. *The New York Times.* 2013. <http://www.nytimes.com/2013/05/29/nyregion/liberty-reserve-operators-accused-of-money-laundering.html?_r=0>.

[32] Penenberg, Adam. "US authorities launch their first attack on bitcoin." 2013. *pandodaily.* 2013. <http://pandodaily.com/2013/05/15/us-authorities-launch-their-first-attack-on-bitcoin/>.

[33] Carney, Michael. *Bitcoin is legal, but mainstream adoption will mandate playing by the rules*. 2013. 2013. <http://pandodaily.com/2013/05/17/bitcoin-is-legal-but-mainstream-adoption-will-mandate-playing-by-the-rules/>.

[34] Hernandez, Raul. "Millions to be Repaid to Victims of e-Bullion.com, Feds say." 2013. *VCS.* 2013. <http://blogs.venturacountystar.com/the_court_reporter/2012/08/millions-to-be-repaid-to-victims-of-e-bullioncom-feds-say.html>.

Cohan, Peter. “After Liberty Reserve Shut Down, Is Bitcoin Next?” 2013. *Forbes*. 2013. http://www.forbes.com/sites/petercohan/2013/05/29/after-liberty-reserve-shut-down-is-bitcoin-next/

[35] Wood, Robert W. "IRS Takes A Bite Out Of Bitcoin." 2013. *Forbes.* 2013. <http://www.forbes.com/sites/robertwood/2013/05/02/irs-takes-a-bite-out-of-bitcoin/>.

[36] Flitter, Emily. "Digital currency firms rush to adopt anti-money laundering rules." 2013. *Fox Business.* 2013. <http://www.foxbusiness.com/news/2013/05/31/digital-currency-firms-rush-to-adopt-anti-money-laundering-rules/>.