Virtual Currencies: Safe for Business and Consumers or just for Criminals?
13th European Security Conference & Exhibition
The Hague
April 2, 2014

Erik R. Barnett[1]

There is a significant risk of large-scale criminal use of crypto-currencies because of a lack of universal regulation, a gap in critical industry-based checks against money laundering, a decentralized administration, and the anonymity of internal crypto-currency transactions.

The ongoing use of crypto-currency in the sale of illegal narcotics as well as other illicit goods and to hide transactions that support criminal activity and possibly terrorist financing is being aggressively confronted by criminal investigators. But financial regulators and international law enforcement are being challenged by this emerging technology as they continue efforts to combat transnational serious organized crime and international terrorism.

This paper identifies solutions to prevent virtual currencies from exploitation by transnational criminal or terrorist organizations. Concomitantly, these solutions would also enhance the trust and reliability of crypto-currencies as conduits of online commerce.

1. Introduction

As a subset of virtual currency, crypto-currencies are "defined as Internet peer-to-peer (P2P) [payment systems] having an element of cryptographic security … wherein value is electronically transmitted between parties, *without an intermediary*." [1]. The transfer occurs between individuals outside strictly regulated financial institutions. [2]. However, crypto-currency can ultimately be redeemed for fiat currency through various intermediaries such as an "exchanger."

Perhaps the most commonly known crypto-currency is Bitcoin. Bitcoin has arguably become the "Xerox machine" or "Scotch tape," of virtual currencies in general, and

[1] The author is currently the Attaché to the European Union for U.S. ICE Homeland Security Investigations (HSI), the primary investigative arm of the U.S. Department of Homeland Security. The views expressed are solely those of the author and are not intended to represent the views of any agency of the U.S. government.

crypto-currencies in particular. This paper references Bitcoin only when specifically discussing the network itself and not as a synonym for virtual currencies. [2]

This is done for two reasons. First, it is inappropriate to single out one entity in a discussion about criminal exploitation of an emerging technology.[3]

Further, referencing a singular entity could cause an underestimation of the scope of the potential criminal problem. In March 2013, the Financial Crimes Enforcement Network (FinCEN) noted the existence of nine active crypto-currencies other than Bitcoin and two more in development. Because crypto-currencies are specifically defined as those within a P2P system, this figure necessarily does not include other virtual currency schemes, including those used in online games, some of which are "bidirectional," meaning users can convert their virtual money into traditional, fiat currency.[4]

However, examining Bitcoin and its development helps to understand crypto-currencies. Introduced in 2009 by Satoshi Nakamoto,[5] Bitcoin was described as an "electronic payment system based on cryptographic proof instead of trust . . . ." [5].

Bitcoin's unit of currency is "an electronic coin as a chain of digital signatures." A P2P network verifies transmission from the sender to a recipient, each of who can select a one-time address for the transaction, so that neither is associated with that address beyond the single transaction. The P2P authentication within the virtual financial system creates a public log of the transaction, making it impossible for the owner to twice "spend" the same coin. [6].

In a 2008 white paper, Nakamoto declared the most significant justification for establishing a crypto-graphic currency to be the reduction of costs associated with a trust based model, in which buyer and seller must be wary of fraud and cancelled payments that often require inefficient intervention by a third-party financial institution. Bitcoin transactions are irreversible, so an intermediary to settle disputes is allegedly not needed.

---

[2] As a stylistic matter and consistent with other academic papers on the subject, reference to *Bitcoin* as capitalized is reserved for reference to the payment system, while lower case *bitcoin* is used for the unit of currency.

[3] Law enforcement has so-often witnessed criminal organizations manipulate new technologies or innovations for ill-gotten gain. The United States created a criminal law to specifically deal with the phenomenon of frauds perpetrated over the telephone during this new technology's early expansion. Child sexual abuse material (CSAM) has migrated from physical to online images and videos over the last two decades and most recently live webcam child sex shows sold to pedophiles.

[4] Crypto-currencies are recognized as a subset of virtual currencies and the terms used interchangeably.

[5] Satoshi Nakamoto is generally believed to be a pseudonym for a person or group. *But see* L. McGrath Goodman. The Face Behind Bitcoin. Newsweek. Mar. 6, 2014. mag.newsweek.com/2014/03/14/bitcoin-satoshi-nakamoto.html; accessed on 9 March 2014.

Because the decentralized system relies upon a P2P network, the transactions are perpetually visible to all on the system. However, to preserve the anonymity of the transactors, not all portions of the transaction are visible. [7].[6]

Nakamoto analogized maintaining the anonymity of the transferees, to the ticker tape of stock exchanges in which trades are reported, but not the traders.
This analogy, however, is gravely misleading. Stock exchanges would not include information about the traders on the ticker tape, which serves merely to inform potential investors of the value of the stock itself. However, the underlying stock purchases, including personally identifiable information of the parties, are duly recorded by regulated brokerages and would be made available to relevant authorities upon legally sufficient request.

Regardless of the falsity of the analogy, the growth and desirability of a virtual currency is undeniable, given the expansion of Internet users and their greater sophistication. The 2012 Cisco Visual Networking Index estimates that the number of devices connected to global Internet Protocol networks will be equal to nearly three times the world's population by 2017.

As argued in The Economist, commercial dealings involving traditional international monetary exchanges increase transaction costs, while virtual currency transactions eliminate an inefficient middleman. [8].

The potential societal benefits of virtual currencies include mobile banking systems in developing countries where financial infrastructure may be lacking, decreased transaction costs, and elimination of fees associated with normal bank accounts – all practical benefits for most businesses and consumers. [9].

This paper makes no comment or conclusion about the practicality or security of crypto-currencies. But this is a very legitimate question based upon findings by researchers and open source material. [16] [17].[7] Widely reported has been the alleged suspected theft of $480 million worth of bitcoins from the exchange Mt. Gox, which subsequently filed for bankruptcy protections. [19].

[6] Computer science researchers Sarah Meikeljohn, et. al. argue the transactions are *pseudo-anonymous* and that identities of recipients can be determined using self-initiated transactions and open source material. The researchers acknowledge that "the most motivated users (such as criminals)" can achieve a greater state of anonymity.
[7] In a 2012 intelligence analysis, the FBI assessed with a high-degree of confidence that criminals intending to steal bitcoins can target and exploit third-party Bitcoin services. The FBI cites a series of such events in support of this conclusion.

2. Law Enforcement Deals with Emerging Technology's "Dark Side"

Perhaps foreshadowing future difficulties, on May 14, 2013, U.S. law enforcement seized financial accounts of a subsidiary company of Mt. Gox. [10]. Bitcoins were repeatedly exchanged back and forth into U.S. dollars through the subsidiary company and Mt. Gox.[8] However, neither the subsidiary nor Mt. Gox had registered as a Money Services Business (MSB) as required by law.

While failing to register might seem a mere technical violation, there are obligations for MSBs to implement anti-money laundering measures and file Suspicious Activity Reports (SARS) as well as Cash Transaction Reports (CTRs). These reports are an integral part of a regulatory framework designed to identify money laundering by criminal or terrorist organizations.

On May 28, 2013, federal criminal charges were filed against arguably the world's largest online virtual currency company, Liberty Reserve, and five of its principal employees, for money laundering and operating an unlicensed money transmitting business. Allegedly, Liberty Reserve "deliberately attracted and maintained a customer base of criminals by making financial activity … untraceable and anonymous." [4].[9]

Liberty Reserve facilitated "a broad range of online criminal activity, including credit card fraud, identity theft, investment fraud, computer hacking, child pornography, and narcotics trafficking." Criminal investigators allege that 55 million separate financial transactions illegally laundered over six billion dollars.

Liberty Reserve utilized a digital currency unit known as "LR." Users could open an account with absolutely no proof of identity other than what was typed onto the website. The user then traded LR with other users, with Liberty Reserve taking a one percent fee and another 75 cents per transaction if the account holder wanted to keep his financial transaction private, *even from Liberty Reserve*.

Importantly, to "cash out" LR, account holders were directed to pre-approved exchanges, almost all unlicensed money transmitting businesses with ties to Liberty Reserve. These, of course, did not implement appropriate anti-money laundering measures or report suspicious financial activity to regulators or law enforcement.

The criminal charges against Liberty Reserve and its five principal officers were the culmination of investigative work by law enforcement agencies in 18 countries.

---

[8] While ICE Homeland Security Investigations was the law enforcement agency involved in the seizure of the Mt. Gox accounts, all facts about the seizure are from the affidavit, a public record.

[9] While ICE Homeland Security Investigations was heavily involved in the multi-agency investigation, all discussion about Liberty Reserve is from allegations contained in the indictment, a public record.

Crypto-currencies have been favored by those engaged in cyber crime. In June 2011, the online hacking group LulzSec used Bitcoin and Liberty Reserve, in combination, to launder funds donated by supporters. [11]. According to the FBI, LulzSec used part of these funds to purchase a botnet.[10] French cybersecurity researchers recently proclaimed that Bitcoin "holds a privileged position" as currency among cybercriminals, who "recommend it and praise its reliability." [22].

Criminal charges against the administrator of the Silk Road website are yet another recent example of nefarious use of crypto-currency, with allegations that the site sold illegal narcotics and other illicit services online to anyone in exchange for bitcoins. [3]. As alleged in the public court filing by the U.S. Department of Justice, Silk Road "was used by several thousand drug dealers and other unlawful vendors to distribute hundreds of kilograms of illegal drugs and other illicit goods and services … as well as to launder hundreds of millions of dollars…." The administrator of Silk Road, Ross William Ulbricht, is alleged to have generated sales of illegal narcotics "totaling over 9.5 million Bitcoins and collected commissions from the sales totaling over 600,000 Bitcoins."[11]

Importantly, by Bitcoin's own design, only 21 million coins will ever be produced [6], and by October 2013, when Ulbricht was arrested, only about 11.7 million had been created. [18]. But, due to possible hording, only four million bitcoins may have been in circulation in 2013. [7]. Given these facts and the allegations, it is quite possible that the vast majority of available bitcoins in the world cycled through the hands of narcotics traffickers.

In January 2014, federal agents filed a criminal complaint alleging that Jesse Korff sold a deadly toxin, with the express knowledge it would be used to kill a human being, in exchange for bitcoins after advertising the product on the website Black Market Reloaded.[12]

3. Keeping Virtual Currencies from Becoming Havens for Criminals

All of the above criminal enforcement occurred in less than one calendar year. There are, unfortunately, even more examples of criminal exploitation and use of virtual currencies. Based on this track record, absent changes to the business model and being brought under regulation, the public and law enforcement have good reason to believe criminal use of crytpo-currencies will continue.

---

[10] This is the same hacker group that breached the IT security of Infragard, an FBI-sponsored private-public partnership. A majority of the group was subsequently arrested.
[11] While ICE Homeland Security Investigations was involved in portions of the Silk Road investigation, all discussion about the matter are from allegations contained in court filings or other public records.
[12] While an ICE Homeland Security Investigations agent swore to facts in the criminal complaint against Jesse Korff, all discussion about the matter are from allegations contained in court filings or other public records.

This concern is not confined to one country. The European Central Bank has declared virtual currencies "could represent a challenge for public authorities, given the legal uncertainty surrounding these schemes, as they can be used by criminals, fraudsters and money launderers to perform their illegal activities." [2].

3.1 Institution of Anti-Money Laundering Programs is an Absolute Necessity

Robust anti-money laundering (AML) obligations and strong financial regulatory systems frustrate the ability of criminal and terrorist organizations to finance their activities or launder its proceeds. This has proven to be true with traditional brick and mortar banking institutions, which have reasonably recognized AML responsibilities as enhancing their professional reputations. [12]. There is no rational reason not to apply such provisions to the virtual world.

In February 2012, the Financial Action Task Force (FATF) concluded that money or value transfer services (MVTS), such as virtual currency exchanges, should be licensed and registered. [13] The FATF also recommended that governments ensure MVTS have in place proper AML controls and that all MVTS have agents accessible to authorities.

Because of the anonymity within crypto-currency transactions, only the "cashing out" into fiat currency will allow law enforcement to link funds to a specific individual or account. This makes virtual currency exchanges relevant choke points to observe potential criminal activity and money laundering activities. But they must have AML controls in place and exercise due diligence to be effective.

In March 2013, FinCEN issued guidance that regulated money services businesses (MSBs) include individuals or companies engaged as a business in issuing virtual currency or in the exchange of virtual currency for fiat currency. [13]. However, the largest bitcoin exchange at the time, Mt. Gox not only failed to register, but its subsidiary actually claimed it was not a business engaged in money services. [10]. Registration would be followed by implementation of AML programs, including filing of Suspicious Activity Reports (SARS).

SARS provide critical information to law enforcement about financial activities seemingly not supported by a business or lawful purpose. FinCEN identified only about 70 SARS filed between 2009 and 2013 associated with crypto-currencies. During this same time period, Silk Road and Liberty Reserve were exclusively using crypto-currencies in criminal schemes.

[13] The Financial Action Task Force is widely recognized by law enforcement internationally as an opinion leader in the fight against transnational money laundering.

Importantly, AML measures are not voluntary for financial institutions.[14] They must be undertaken proactively within the virtual currency industry to strengthen the reputation of crypto-currencies as legitimate tools of international commerce, while imposing a minimal burden.[15]

3.2 Universality of Regulation

The regulation by FinCEN and other U.S. entities against virtual currencies may lead to a decampment of such businesses from the United States. [15]. But, as noted by the FATF, there must be a broad international regulatory scheme to control for regionalized regulation. Liberty Reserve already showed the globalization of virtual currencies with significant law enforcement effort expended in 18 countries in order to thwart its criminal activity.

Regulatory action should be harmonized with other countries so crypto-currencies are not faced with possibly contradictory guidelines or gaps in regulatory oversight and so law enforcement has reciprocal money laundering laws internationally.

Innovators within the virtual currency community are publicly recognizing the importance of regulation to preserve the credibility of crypto-currencies as a financial system, particularly in the wake of the collapse of Mt. Gox, once the largest bitcoin exchange. [21].

3.3 End of Anonymity

Tellingly, anonymity of transactions was not noted as a justification for creation of Bitcoin, but was built into the business model. [5]. Nonetheless, as crypto-currencies flourish, this anonymity will continue to attract criminal activity and pose a significant obstacle to law enforcement's ability to "follow the money" in criminal investigations. When appropriate legal process is provided to a financial institution for relevant records, the identities of those transferring funds should be discernible to investigators.

A disturbing trend is entrepreneurial services within crypto-currency communities that "auto-launder" currency units for users. There are vendors that advertise increased anonymity. Crypto-currencies must discourage these vendors by establishing systems where use of those services precludes payment transfers.

---

[14] In a case investigated by ICE Homeland Security Investigations, HSBC agreed to forfeit $1.256 billion to the United States based upon its failure to exercise due diligence and have appropriate AML controls in place. http://www.ice.gov/news/releases/1212/121211newyork.htm; accessed on 19 November 2013.

[15] Sarah Meikeljohn et. al. found that since early 2012, 40% of Bitcoin's transactions were for less than a single bitcoin, worth about $750 on November 19, 2013, and 20% were for a tenth of a bitcoin. SARS and CTR reports normally involve much larger transaction amounts.

Further, crypto-currencies should implement "know your customer" practices that require true identities and residences of account holders. It is desirable to have privacy in financial transactions. But we have already determined as a society to balance privacy with transparency when criminal or terrorist organizations use our financial institutions.

3.4 Centralization of Administration

There must be a self-imposed centralized control within crypto-currencies to ensure integrity of the transactions, to create AML monitoring, and to provide a single point of contact to regulatory and law enforcement authorities.

Bitcoin uses a P2P network to verify transactions, a function normally performed by a centralized authority in other financial institutions, including other virtual currencies. The decentralized administration cannot implement AML efforts, exercise due diligence, or provide relevant records of account holders to law enforcement or regulators.

While the business model, and underground fan base, may favor decentralization, this new technology is not merely another social network or "app" to display photos, but engaged in significant financial transactions, imposing appropriately commensurate responsibilities on the developers and supporters.[16][20].

4. Conclusions

Reasonable, industry-imposed reforms coupled with existing regulatory oversight by government authorities would strengthen the reputation of crypto-currencies as appropriate intermediaries of online commerce while preserving them from exploitation by criminal organizations.

5. References

[1] FinCEN. Networking Bulletin, Crypto-currencies, Mar. 2013.
[2] European Central Bank, Virtual Currency Schemes, ECB Report, Oct. 2012. ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf ; accessed on 19 November 2013.
[3] Sealed Second Post Complaint Protective Order. U.S. v. Ross William Ulbricht, CIV6919. U.S. District Court for the Southern District of New York. justice.gov/usao/nys/pressreleases/October13/SilkRoadSeizurePR.php; accessed on 19 November 2013.

[16] Reportedly on November 22, 2013, a $147 million worth of bitcoins was transferred, without being cashed out for fiat currency. This transaction, of only 1.6% of the bitcoins in existence, might have been an inter-company transfer by a bitcoin exchange as a housekeeping measure. But the exchange reportedly refused comment, leaving commentators to claim that the largest ever bitcoin transfer was, as are all Bitcoin transactions, anonymous.

[4] Indictment. U.S. v. Liberty Reserve, 13CRIM368. U.S. District Court for the Southern District of New York. justice.gov/usao/nys/pressreleases/May13/LibertyReserveetalDocuments.php ; accessed on 19 November 2013.
[5] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System, 2008. Bitcoin.org/bitcoin.pdf ; accessed on 19 November 2013.
[6] bitcoin.org/en/faq; accessed on 19 November 2013.
[7] S. Meikeljohn, et. al. A Fistful of Bitcoins: Characterizing Payments Among Men with No Names. Oct. 2013. cs.gmu.edu/~mccoy/; accessed on 19 November 2013.
[8] The Economist, Digital Currencies, A New Specie. Apr. 13, 2013. economist.com/news/leaders/21576104-regulators-should-keep-their-hands-new-forms-digital-money-such-bitcoin-new-specie; accessed on 19 November 2013.
[9] T. Carmody. Money 3.0: How Bitcoins May Change the Global Economy. National Geographic Daily News. Oct. 14, 2013. news.nationalgeographic.com/news/2013/10/131014-bitcoins-silk-road-virtual-currencies-internet-money/ ; accessed on 19 November 2013.
[10] Affidavit in Support of Seizure Warrant. In the Matter of the Seizure of the contents of one Dwolla account. 13-1162 SKG. U.S. District Court for the District of Maryland news.cnet.com/8301-13578_3-57584511-38/homeland-security-cuts-off-dwolla-bitcoin-transfers/ ; accessed on 19 November 2013.
[11] P. Olson. We Are Anonymous, pages 304-06. Little Brown & Company, 2012.
[12] Remarks of Jennifer Shasky Calvery, Director, FinCEN, The Virtual Economy: Potential, Perplexities and Promises, June 13, 2013, Washington, D.C. fincen.gov/news_room/testimony/ ; accessed on 19 November 2013.
[13] FinCEN. Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies. Mar. 18, 2013. fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html; accessed on 19 November 2013.
[14] Financial Action Task Force. International Standard of Combating Money Laundering and the Financing of Terrorism & Proliferation The FATF Recommendations. 2012. fatfrecommendations/documents/internationalstandardsoncombatingmoneylaunderingandthefinancingofterrorismproliferation-thefatfrecommendations.html; ; accessed on 19 November 2013.
[15] Testimony of Patrick Murck, Senate Committee on Homeland Security and Governmental Affairs. Nov. 18, 2013. hsgac.senate.gov/hearings/beyond-silk-road-potential-risks-threats-and-promises-of-virtual-currencies; accessed on 19 November 2013.
[16] R. McMillan. $1.2M Hack Shows Why You Should Never Store Bitcoins on the Internet. Wired. Nov. 7, 2013. wired.com/wiredenterprise/2013/11/inputs/; accessed on 19 November 2013.
[17] Federal Bureau of Investigation. Bitcoin Virtual Currency Unique Features Present Distinct Challenges for Deterring Illicit Activity. Intelligence Assessment, Cyber Intelligence and Criminal Intelligence Section, Apr. 2012. wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf; accessed on 19 November 2013.

[18] Blockchain. Total Bitcoins in Circulation. blockchain.info/charts/total-bitcoins; accessed on 19 November 2013.
[19] C. Daugherty and G. Huang. Mt. Gox Seeks Bankruptcy After $480 Million Bitcoin Loss. Bloomberg Businessweek. Feb. 28, 2014. businessweek.com/news/2014-02-28/mt-dot-gox-exchange-files-for-bankruptcy; accessed on 9 March 2014.
[20] T. Lee. Here's who (probably) did that massive $150,000,000 Bitcoin transaction. Washington Post. November 23, 2013. washingtonpost.com/blogs/the-switch/wp/2013/11/23/heres-who-probably-did-that-massive-150000000-bitcoin-transaction/; accessed on 9 March 2014.
[21] F. Manjoo. For Bitcoin, Secure Future Might Need Oversight. New York Times. Mar. 5, 2014. nytimes.com/2014/03/06/technology/personaltech/for-bitcoin-a-secure-future-might-require-traditional-trappings.html; accessed on 10 March 2014.
[22] M. Even, A. Gery, B. Louis-Sidney. Virtual Currencies and Cybercrime: Current State of Play and Future Prospects. Compagnie Européene d'Intelligence Stratégique (CEIS). 2013.