Bitcoin and modern alchemy: in code we trust

Jeffrey Simser
Government of Ontario, Toronto, Canada

Abstract

Purpose – This paper aims to explore the challenge posed by Bitcoin to regulators, particularly anti-money laundering regulators. Bitcoin is a crypto-currency based on open-source software and protocols that operates in peer-to-peer networks as a private irreversible payment mechanism. The protocol allows cross-border payments, for large and small items, with little or no transactional costs.

Design/methodology/approach – Case studies and case law are examined as are relevant reports by regulators.

Findings – Bitcoin is based on complex computer code supported by a robust community in a peer-to-peer network. Unlike other virtual currencies, Bitcoin appears to have obtained purchase and as such poses unique challenges to regulators.

Research limitations/implications – Bitcoin is at a nascent stage and the evolution of the virtual currency is difficult to predict.

Practical implications – Those who study financial systems, anti-money laundering regimes and asset forfeiture laws will have an interest in this topic.

Originality/value – This is a new and emerging currency; there is limited literature on the implications of this currency to anti-money laundering systems.

Keywords Bitcoin, Money laundering, Virtual currency, Asset forfeiture

Paper type Research paper

> Unlike credit card transactions, which leave a digital trail, Bitcoin transactions are designed to be anonymous and untraceable. When you transfer Bitcoins to someone else, it is as if you handed over a paper bag filled with $100 bills in a dark alley. Sure enough, as best as anyone can tell, the main use of Bitcoin so far, other than as a target for speculation (on the markets), has been online versions of those dark alley exchanges, with Bitcoins traded for narcotics and other illegal items (Krugman, 2013).

1. Introduction

The Library of Alexandria, by the third century BC, was believed to hold the sum of human knowledge; today there is enough information floating around the world, big data, to give every single person alive 320 times as much information as that great library held, 1,200 exabytes worth (Cukier and Mayer-Schoenberger, 2013). Big data offers unique opportunities to solve problems, potentially threatens our privacy and

The views expressed in this paper are the personal views of the author and do not represent the views of the Government of Ontario. The author (jeffsimser@yahoo.ca) is a co-author of *Civil Asset Forfeiture in Canada* (Toronto: Canada Law Book, 2012). The author is grateful for the thoughtful suggestions of his friend and colleague Michael Ryan, BBA, LLB, retired police Inspector and currently a senior associate with Toddington International Inc., although any errors in the paper are the author's.

Journal of Financial Crime
Vol. 22 No. 2, 2015
pp. 156-169
© Emerald Group Publishing Limited
1359-0790
DOI 10.1108/JFC-11-2013-0067

create unique challenges. With oceans of data floating around, governments in particular have found it challenging to keep track of their secrets. Consider the drama in 2013 surrounding Edward Snowden, who worked for a National Security Agency contractor. In May 2013, he landed in Hong Kong with at least four computers loaded with US government secrets. In June, he met with reporters and leaked a number of documents that revealed that the US government had accessed data and documentation from telecommunication entities, like Verizon, and Web sites like Google and Facebook. At the time of writing, Snowden has fled to Moscow where he remains (Gidda, 2013; Myers and Kramer). A curious link between Snowden and a virtual currency, called Bitcoin, emerged as a lesser known part of the narrative. When WikiLeaks founder Julian Assange praised Snowden as a hero, Bitcoin donations to WikiLeaks increased from $20 a day to $700 a day. WikiLeaks, an organization devoted to whistleblowing, had initially been funded by donations through credit cards and PayPal, a source of funding choked off in 2010; the organization now accepts Bitcoin (Ross, 2013; Grinberg, 2013). This curious virtual currency, which is designed to allow anonymous transactions, has drawn serious attention from regulators, particularly in respect to anti-money laundering (AML) regimes. Bitcoin, at the moment, exists largely in the ether of the Internet. Those wanting to buy or sell Bitcoin can do so through online exchanges, like Mt. Gox, which will allow one to exchange fiat currency like Yen or Euros for Bitcoin. Alternatively, one can accept Bitcoin in exchange for goods or services; the currency works through open-source software and various e-wallets can be downloaded to your phone or computer. A Las Vegas company has built a kiosk, which looks very much like an ATM, where consumers can convert cash into Bitcoin (Posadzki, 2013). The paper explores this virtual currency, Bitcoin that has been associated with drug dealers, gold bugs, fraudsters, terrorists, whistleblowers, pornographers, Internet freedom activists, unregulated gaming enterprises and a man with four computers full of information that the American government does not want in the public domain.

1.1 What is Bitcoin?

Bitcoin is a crypto-currency based on open-source software and protocols that operates in peer-to-peer networks as a private irreversible payment mechanism. The protocol allows cross-border payments, for large and small items, with little or no transactional costs. The Bitcoin transactional system is often described as an anonymous system, although it might be more accurate to describe the system as one in which users can invoke privacy. The ledger of account for all Bitcoin transactions is public and distributed. Actors in the system have a "public" key to access Bitcoin and can use any combination of 33 letters and numbers to publicly describe themselves; a random and meaningless string in the public key can offer anonymity. Proponents describe Bitcoin as a vibrant and evolving payment system with the means to disrupt conventional systems. Gold bugs see Bitcoin as a way of avoiding fiat currencies that lack precious metal backing (although ironically, Bitcoin also lacks such backing). Venture capitalists, angel investors and high-net-worth investors are intrigued by the investment possibilities (Murck, 2013). Libertarians see Bitcoin as an offset to traditional currencies, where, in their view, governments can simply print money through quantitative easing. Law enforcement and security officials have raised alarms about Bitcoin as the crypto-currency of choice on deep Web site like Silk Road (a black market for drugs) and

Black Market Reloaded (offering everything from illegal guns to the services of those that use them) (Cottle, 2013).

2. Money

Gertrude Stein once opined: “whether you like it or whether you do not, money is money and that is all there is about it[1]”. Almost 80 years later, our conventional notion of money remains a relatively simple intellectual construct: money is a dispassionate quantitative device that enables “unfettered individuals” to “behave as rational participants in market transaction”, where money allows for simple distinctions of “price and quantity” (Zelizer, 2013; European Central Bank 2012). Money is a means of exchange, a store of value and a unit of account. Money is “something we can use to buy stuff that has a standard that does not change much” (O’Brien, 2013). Governments and central banks work hard to ensure that fiat currency is guaranteed as an acceptable form of money and to ensure that the supply of money into the economy is neither inflationary nor deflationary. Obviously, at another level, the concept of money is considerably more complex. Money is not a purely neutral concept: we routinely distinguish, for example, between clean and dirty money and have complex systems to address the laundering of money.

2.1 In code we trust

There is a long-standing philosophical debate about money itself. Does money have an inherent value or is it a creature of legally enforced social norms? Paper money, when introduced, was generally backed by currency reserves of precious metal (giving it something of an inherent value); when the gold standard was abandoned, the power of the state ensured that paper currency had value. Bitcoin has neither feature. So how does it have value? Bitcoin emerged from a confluence of events: the 2008 financial crisis diminished trust in financial institutions; as noted above, governments pressured private intermediaries, like credit card companies, to cut off the flow of funds to WikiLeaks; there was dissatisfaction with some processing intermediaries, like PayPal (particularly around their anti-fraud measures); finally, financial intermediaries, like Western Union, charges fees for cross-border transactions. Bitcoin appealed to certain dissatisfied factions in society concerned about these issues. Advocates of free speech, particularly on the Internet, were unhappy that governments could censor their views by shutting down payment systems for WikiLeaks. Bitcoin, anonymous and without a central body to process transactions, appeals as a censorship-free form of currency. Iranians are apparently using Bitcoin to get around international sanctions[2]. Gold bugs, alarmed by central banks printing money and quantitative easing, wanted a return to currency backed by precious metals. The Bitcoin system uses language to encourage that kind of comparison; for example, programmers in the system “mine” for Bitcoins. Bitcoin can be used in cross-border transactions with little transactional cost. Finally, Bitcoin users have formed a community where trust is placed in the computer code and the collective strength of the network to sustain its value (Maurer, 2013).

This is perhaps the most important feature of the system. Until the gold standard was abandoned, paper currency was generally backed by precious metal reserves. Now, money in circulation is backed by the authority of the state. As long as people and markets accept the currency, paper money has value; most countries sustain confidence and trust in currency through calibrated monetary and fiscal policy. When those policies fail, for example, when the mint prints mountains of money until it becomes valueless, confidence in paper money is shattered. This happened not that long ago in Zimbabwe, where hyperinflation attacked the Zimbabwe dollar to the point, in 2009, where the government in essence abandoned their own currency (foreign currency is now Zimbabwe's fiat currency). One of the reasons Bitcoin has attracted users is that its architecture limits how much "money" the system will produce. That is not to say that the value of Bitcoin relative to fiat currencies has remained constant; the market for Bitcoin is highly illiquid and there have been wild swings in the value of the currency. However, monetary supply of Bitcoin is constrained by the system's computer code. Most importantly, users trust that code and they trust the community that verifies transactions with that code. That trust underpins the "value" of Bitcoin: users expect that others will accept Bitcoin as a payment mechanism.

2.2 The virtual currency dream

The idea of digital currency is hardly new. In 1982, a blueprint for anonymous electronic cash was proposed and hundreds of papers were subsequently published, particularly in the cryptography community where Bitcoin was first proposed (Barber *et al.*, 2012). Libertarians have been attracted to the notion of an anonymous currency that can operate outside of fiat currencies. For example, e-Gold offered an online currency which its promoters claimed was backstopped by gold deposits held in St. Kitts and Nevis. As with Bitcoin, e-Gold transfers were anonymous and irrevocable. Unfortunately for the enterprise, e-Gold became an attractive vehicle for fraudsters, Ponzi operators and boiler rooms hustling pump-and-dump scams (Simser, 2013)[3]. When this problem was pointed out to the company by law enforcement, e-Gold cooperated in providing information about potential abusers of the system when they cashed out their holdings for real currency. That cooperation did not prevent authorities from charging the company with a series of money laundering offences, which resulted in guilty pleas (Condon, 2013)[4]. Cryptographer David Chaum created E-Cash, but it too floundered because it relied on the existing infrastructure of government and financial intermediaries.

2.3 Other virtual currencies

From a regulatory perspective, the best to way to conceptualize virtual money is to examine its relationship to fiat currency. For example, World of Warcraft Gold is a virtual currency used in a computer role-playing game. Players can obtain the "gold" when they set up an account or they can earn gold in the course of playing the game. The currency is needed to advance within game levels. That said, trading the gold in the real world is strictly prohibited under the terms and conditions of the game; the currency operates in a closed system. Facebook credits might be considered another form of virtual currency; users can buy the credits, and in turn buy virtual goods with applications in the Facebook platform. Facebook credits have a unidirectional flow, not unlike a stored-value card, where a customer places money into the system and then can buy goods and services. Finally, Second Life is an online game where players create avatars within a virtual community. Players, through their avatars, can "live" a life that is entirely different from their real world life. There is a self-contained economy with Second Life which uses Linden Dollars as a virtual currency. As Linden Dollars can be converted back into fiat currency, it surfaces issues similar to those raised by Bitcoin[5].

3. The creation of Bitcoin

Bitcoin was first proposed in early 2009, through a research paper written by "Satoshi Nakamoto" and posted on a cryptography listserv (Nakamoto, 2009). Nakamoto was unknown to the listserv's veterans and little is known about him (or her). His online profile claimed he resided in Japan; his e-mail address was German; Nakamoto appears to be a pseudonym. Nakamoto's posts were related largely to discussions around the source code; his English language skills were flawless. In his last post, in December 2010, he discouraged WikiLeaks from using Bitcoins for donations, fearing that the small "beta community" was "in its infancy" and the "heat" brought by donations would destroy the currency. One early Bitcoin developer observed that the system was "awfully well designed for one person to crank out" and speculated that Nakamoto was in fact a consortium of developers (Wallace, 2011).

3.1 Bitcoin alchemy

Bitcoin is an Internet payment protocol which operates like a virtual currency. Bitcoin lacks a physical form and does not require the intermediation of government or a private third party to settle transactions. At a basic level, a Bitcoin is simply a computer file, similar to a song or piece of text, which can be stored on a computer; the virtual currency can be spent in a fashion similar to sending an e-mail online. Users download open-source software and store Bitcoins, once acquired, in a digital wallet on their computer or smart phone (or with a third-party provider). The operation of the currency, at a technical level, is immensely complex.

Bitcoin relies on a pseudonymous digital real-time ledger of transactions called a "block chain", which is maintained publicly and collectively by users who regulate and verify through a proof-of-work mechanism known as mining. Each owner possesses two keys, one public and one private. To purchase a Bitcoin, the buyer sends the seller her public key. The seller adds her private key and Bitcoins are then transferred electronically through a hash of the current and previous transactions. The ledger of account for Bitcoin is public and distributed, containing an electronic history of all transactions. Once the transaction occurs, it is sent to the peer-to-peer network. The creator of Bitcoin identified the prevention of "double-spending" as a key feature of the system. If someone could cut and paste multiple versions of the same currency, electronically counterfeiting it, Bitcoins would quickly have no value. The solution: when the transaction is posted publicly, it needs to be verified. Volunteers within the peer-to-peer network verify transactions and create a timestamp "by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof of work[6]". The time stamp becomes part of the coding of that particular Bitcoin, meaning it cannot be duplicated or spent more than once.

3.2 Mining Bitcoin

There is no central authority to settle or clear a Bitcoin transaction. Rather, the disbursed peer-to-peer network relies on volunteers to verify transaction, a computational process called vetting that requires time and computing power. The volunteers are rewarded for their mining with Bitcoins every time their system navigates the complex mathematical calculations needed for verification (the amounts available are halved every four years). Once verified, the transaction is irrevocable. The architecture for the system is widely distributed, making it less vulnerable to attack; actors within the system are incentivized, through mining, to maintain its integrity.

CPU power is devoted to solving "irreversible cryptographic puzzles that contain data from several transactions[7]". Once the puzzles are solved, a computer-generated "key" is transmitted to the rest of the network and the transaction in question can clear. Once cleared, the transaction is irreversible. It generally takes between 10 and 60 minutes to verify a transaction. To incent the system, miners are given Bitcoin currency; they compete to solve the puzzle and the winner receives Bitcoins. As the number of miners increase, so does the difficulty of each puzzle. Further, the bounty for a successful miner decreases incrementally, so that, in theory, the preordained limit of 21 million Bitcoins is reached in 2140 (assuming the currency does not flame out prior to then). Each Bitcoin is divisible by up to eight decimal places, so the potential available quantum is actually quite large. Nakamoto himself mined the first 50 Bitcoins on January 3, 2009, in what came to be called the genesis block.

3.3 Storing Bitcoins

There are two ways to hold Bitcoins. You can store the currency on the hard drive of your computer (or phone) through an e-wallet or you can trust a third-party provider, such as Coinbase, to hold your Bitcoins. As will be discussed below, storing Bitcoins on your own computer leaves you vulnerable to hackers, user error and hard drive failures. Bitcoin is, in a sense, like cash. If you lose your cash, you lose your money. If you lose the digital data for a Bitcoin, it too is gone forever. Online wallet services are "prone to the same security and reliability pitfalls as individuals", although one hopes that their encryption and back-up protocols are stronger (Lee, 2013).

3.4 Is Bitcoin viable as a currency?

Money works as a medium of exchange because users know, with some measure of reliability, what their currency can do. A shopper in Paris knows roughly how many Euros it will take to buy their groceries. How many Bitcoins will it take to buy groceries? Our Paris consumer has no idea. Bitcoin grew slowly as a currency, initially the domain of libertarians and hackers. The currency was traded on Mt. Gox, a site that evolved from a place to trade fantasy cards (Magic the Online Gathering Online Exchange), to become the favorite clearing house for Bitcoins. There was a bit of a wobble in 2011, when the value of the currency surged, but generally Bitcoins evolved to a trading band of around US$10. Then, in the spring of 2013, Bitcoin went on a wild ride driven by events in Cyprus: depositors lost portions of their bank accounts to prevent a larger collapse of their financial system. The market thinking on Bitcoin seemed to be that bank accounts were not safe, but this virtual currency somehow was. In April 2013, prices went from $266 to $105 the next day, rebounding to $180 and then collapsing to $120. As one commentator has noted, money needs to be reasonably stable to be broadly accepted as a medium of exchange. Bitcoin, noted this commentator, acts not as a currency but as a dot-com stock. When it rises wildly in value, people hoard it; when it falls, no one wants it. The absence of a central bank to match the supply of Bitcoins to the demand means Bitcoin is more like a dot-com enterprise than a currency[8]. That said, Bitcoin is a new idea. Increased use of the conventional market techniques used to stabilize currency values and commodity prices, hedges for example, might bring some stability to a marketplace which, at the moment, is highly illiquid and unstable.

4. Bitcoin: regulators and institutions

In March 2013, FinCEN (the Financial Crimes Enforcement Network), America's Financial Intelligence Unit, issued a guidance statement on virtual currencies[9]. FinCEN is responsible for the administration of anti-money laundering (AML) provisions under the Bank Secrecy Act. Users of virtual currencies, the Guidance stated, were not subject to AML rules but administrators and exchangers were subject as money transmitters. An exchanger is someone engaged in the business of converting virtual currency into real currency or another virtual currency. An administrator issues virtual currency into circulation and has the authority to redeem or withdraw that virtual currency from circulation. The FinCEN rules apply to e-currencies, e-precious metals and virtual currencies with a central repository. For de-centralized virtual currencies, like Bitcoin, FinCEN's guidance advises that people who create the currency (e.g. through mining) and use it are users and therefore not the subject of AML oversight. However, those who mine Bitcoins and sell them to someone else are subjected to AML oversight as money transmitters. The AML obligations mean that administrators and exchangers were now subject to registration requirements, AML responsibilities, as well as record-keeping and reporting obligations.

Recently, the Financial Services Superintendent in New York indicated that Bitcoin would come under regulatory scrutiny. A large group of financial intermediaries have received subpoenas seeking documentation related to the virtual currency. Twenty-two subpoenas sought records related to AML compliance, consumer protection and promotional materials for investors. The Superintendent indicated that the documentation was required to determine the proper regulatory guidance for the burgeoning currency. He also cited concerns about the use of Bitcoin in illegal activity, including "drug smuggling, money laundering, gun running and child pornography" (CBC News 2013). As the Liberty Reserve Case shows, virtual currencies are a highly desirable commodity in the criminal underworld.

4.1 The Liberty Reserve case

Liberty Reserve allowed anonymous transfers around the world, operating like a virtual currency; when disrupted, there were 1 million users worldwide (200,000 in the USA) conducting 12 million transactions annually with a value of $1.4 billion. As a result, Liberty Reserve was named in 2013 by FinCEN as a financial institution of "primary money laundering concern under Section 311" of the Bank Secrecy Act[10]. In a related criminal action brought by the US Department of Justice, Liberty Reserve was described as an online money transmitter who deliberately designed their transactions to avoid regulatory scrutiny and to launder money. Illicit actors using Liberty Reserve included those involved in credit card fraud, identity theft, investment fraud, hacking, drugs and child pornography[11]. Liberty Reserve was founded in 2006 in Costa Rica by Andrew Budovsky and Vladimir Kats. Budovsky had previously dabbled in e-precious metals, as an exchanger for e-Gold, but was convicted in 2006 for running an unlicensed money transmitting business. When US law enforcement made initial inquiries, they were initially told by Costa Rican authorities that the company had been sold and was no longer operating. In fact, Liberty Reserve, according to prosecutors was actively moving tens of millions of dollars through shell accounts and companies into Cyprus, Russia, Hong Kong, China, Morocco, Spain and Australia. Prosecutors allege that virtually of

Liberty Reserve's business is unlawful and that the company laundered $6 billion in criminal proceeds.

Liberty Reserve allowed users to open an account with basic identifying information (name, address and date of birth), but did not require users to validate their identity; fictitious or anonymous users were welcomed. With an account, users could transact with other Liberty Reserve clients for a 1 per cent transfer fee. Further, for an additional $0.75 fee, users could completely hide their identity, making the transfer completely untraceable, "even within Liberty Reserve's already opaque system[12]". Liberty Reserve did not allow direct deposits or credit card transfers by their users, who instead had to deal with "exchangers" or third parties with a direct relationship to Liberty Reserve. A user transferred hard currency to the exchanger, who in turn paid Liberty Reserve in exchange for a credit to the user's account. Exchangers, largely in Malaysia, Russia, Nigeria and Vietnam, operated without AML oversight and charged fees of 5 per cent on transactions. Liberty Reserve also allowed transfers to certain merchants, many of them criminal enterprises (stolen credit card information, online Ponzi schemes, computer hackers, unregulated gaming concerns and underground drug-dealing Web sites). In May 2013, Budovsky was arrested in Spain at the request of US authorities and Kats, his co-founder, was in custody in New York[13].

4.2 Mt. Gox

Law enforcement were able to disrupt Liberty Reserve as an ascertainable entity. The challenges for Bitcoin are different. Mt. Gox is the largest Bitcoin exchange provider; at the time of writing (July 2013), they processed over 50 per cent of Bitcoin transactions. The Tokyo-based entity was started in 2010 as a forum to trade cards for the game "Magic" (hence Mt. Gox: Magic the Gathering Online Exchange). In May 2013, a seizure warrant was granted in Maryland seizing a Dwolla account associated with Mt. Gox (Dwolla is an online payment processor based in Iowa). The supporting affidavit alleged that Mt. Gox violated US laws because they opened accounts in a fiat currency, exchanged those accounts into a crypto-currency (Bitcoin) and, following transactions, allowed users to withdraw fiat currency[14]. Mt. Gox then announced a strategic partnership with an entity called CoinLab for business in Canada and the USA. CoinLab intend to register as a money-services business and operate in compliance with AML rules[15].

4.3 PayPal as precedent

PayPal is an online intermediary that processes payments between users over the Internet. The system has close to 290 million users[16]. PayPal is most commonly used in e-commerce transaction. For example, a purchaser can buy something online. In cyberspace, you cannot always trust the vendor and PayPal became an ideal intermediary, complete with a dispute resolution process. The purchaser gives their money to PayPal who then transmits it, for a fee, to the vendor to complete the transaction. As often happens, regulation lags behind innovation. When the system became popular, regulators had a difficult time sorting it out. The Federal Deposit Insurance Corporation gave an opinion that it was not a bank. However, from an AML perspective, PayPal was treated as a money transmitter (Kaminski, 2003). PayPal obtained a banking license in Luxembourg in 2007 (previously, they were regulated in the UK as an electronic money institution)[17]. The PayPal example might provide a regulatory template for Bitcoin intermediaries.

5. Bitcoin: weaknesses and vulnerabilities

Black Market Reloaded and the Silk Road are Web sites operating in the "deep web", also known as Tor. Tor was originally an acronym for The Onion Router, an open-source software designed to enable online anonymity (the interfaces have changed and Tor is no longer capitalized as an acronym). Internet traffic is routed through a free worldwide network of relays that conceal the user's location from anyone conducting network surveillance or traffic analysis. As data moves through the system, is it "onion routed" whereby layers of encryption are added each time it moves through the various relays[18]. The deep web allows individuals, like whistleblowers and political dissidents, to communicate with some measure of anonymity, although the privacy protections of the system are not invulnerable. Sites, like Silk Road and Black Market Reloaded, have created anonymous marketplaces where all manner of things can be bought and sold. One can purchase illegal narcotics and contract with hackers. The currency in this realm is Bitcoin (Greenberg, 2013). Bitcoin, like cash, is irrevocable; once a Bitcoin transaction is verified there is no going back.

5.1 Crime – theft of Bitcoins

Malware, computer software designed to steal the private key of a Bitcoin owner, has been used to steal the currency. Researchers in California have noted that threshold cryptography countermeasures, like splitting private keys into random shares, and "super-wallets" split across multiple computing devices can address this risk (Barber *et al.*, 2012; FBI Directorate of Intelligence 2012). The risk of theft is likely to increase to the extent that Bitcoin becomes more prevalent. For example, the Bitcoin Foundation recently warned users that some Android wallet applications had programming flaws; users were encouraged to upload patches from the developers. Apparently, the wallets had an inadequate ability to generate the random number sequences needed to maintain security and thousands of dollars had been stolen by hackers (Gadkari, 2013)[19].

5.2 Misadventures – loss of Bitcoins

Bitcoins really just consist of a computer file. One Bitcoin owner, Stefan Thomas, accidentally erased two copies of his e-wallet and lost the password to his third copy. In a very short period of time, he lost about 7,000 Bitcoins (worth $140,000 in 2011, worth considerably more now)[20]. Bitcoins are only as good as the computer user in this respect. Further, computers are machines that, if personal experience is any guide, are prone to packing up every few years. There are third-party providers, some more reliable than others, who will "bank" your Bitcoin for you. As noted above, there are fraudsters and hackers, who will quite happily steal your Bitcoin.

5.3 Privacy – is it an anonymous transaction?

A casual scan of blogs and articles could leave one with the impression that Bitcoin transactions are all completely anonymous. This is not actually correct. Every Bitcoin transaction is published online, although this does not make the transaction public. Users are identified by a "pseudorandomly generated Bitcoin address" and the level of anonymity depends on the user. Internet Protocol (IP) addresses are associated with each transaction. A user can choose an anonymous IP address if they do not want their physical location identified. Users can enhance anonymity through a number of techniques: creating a new Bitcoin address for each payment; routing Bitcoin traffic through an anonymizer; using third-party e-wallet services to consolidate addresses.

Researchers in Germany and Switzerland noted that notwithstanding the use of pseudonyms, there were "serious concerns with respect to the privacy of users" (Androulaki *et al.*, 2012). The research focused on the use of Bitcoins to support everyday transactions in a university setting. The researchers found that knowledge about Bitcoin users can be gathered by exploiting the properties of the system and by applying behavior-based clustering techniques. In a university setting, the researchers found that the profiles of 40 per cent of the Bitcoin users could be identified, even where the users attempted to enhance their privacy by manually creating new IP addresses.

As the Liberty Reserve case (see 4.1 above) shows, criminals are alive to privacy concerns; money launderers were apparently willing to give up points on their transactions to improve privacy in a system that was already opaque. There are efforts underway to improve the anonymity of the Bitcoin system through a "zerocoin" process (Miers *et al.*, 2013)[21]. One of the enduring strengths of the Bitcoin system is the computing and programming community and their willingness to improve the open-source code.

5.4 Hacking and denial of service

Bitcoin relies on mining to verify transactions and produce more currency. If individuals or a group obtained control over a majority of the computational power in the Bitcoin network, transactions could not be processed. As discussed above, the market for Bitcoin generally is highly illiquid and subject to wild swings in price. Governments wanting to shut down Bitcoin or speculators desiring to profit from a collapse (e.g. someone with a future liability denominated in Bitcoins) or even a hacker wanting to blackmail a company that relies on Bitcoins could be motivated to launch a denial of service attack (Grinberg, 2012). Hackers can use malware to harness of the computing power of infected computers and mine Bitcoin for their own benefit[22].

5.5 Bitcoin-denominated fraud

In July 2013, the Securities and Exchange Commission (SEC) charged a Texas man with fraud; his company ran a Ponzi scheme. A Ponzi scheme purports to reward investors with handsome returns, but in fact uses the "investment" funds lodged by new victims to pay early victims. In other words, there is no investment at all, with one victim being paid "returns" either with their own money or those of other victims (Simser, 2013). This SEC case was unremarkable other than the currency: the Bitcoin Savings and Trust offered and sold Bitcoin denominated investments. The scam was typical. Investors were told that they could earn seven per cent per week through Bitcoin arbitrage activity and could conduct under-the-radar transactions involving the virtual currency. Promoted on Bitcoin discussion websites, the fraudster promised fantastic returns with a risk that was "almost 0". The scam raised 700,000 Bitcoins (worth $4.5 million based on average trading values; at the time of the charges the Bitcoin bubble meant that the value exceeded $60 million). The court, in considering technical defences, ruled that Bitcoin is a currency[23].

5.6 Unregulated gaming enterprises

There are two corners of the Internet that have quietly innovated and become technology's early adopters: gaming and pornography sites. Often the innovations, like new scripting languages, make their way into mainstream commercial websites. Consumers using, for example, online gaming do not trust conventional payments methods, like credit cards. For gaming enterprises, credit cards may be a blocked merchant category code, alternatively charge backs can be disputed by an unhappy consumer. Bitcoin has proven to be a frictionless medium for at least some consumers and merchants. In terms of gaming operators, Bitcoin is only appearing at the fringes with upstart operators. Mainstream gaming enterprises concerns about regulatory oversight and AML compliance rules, make Bitcoin more of a problem than an opportunity (Matonis, 2013).

5.7 Information asymmetry

Bitcoin is a highly complex system and the currency market is illiquid. Bitcoin users perform technically complex tasks within the decentralized peer-to-peer network. There is a risk that some users, with superior technical knowledge, can trade with informational advantages not available to those with less sophisticated knowledge. The latter category of user can suffer losses through hacking, theft, improvident trades, and so on[24].

5.8 Taxation

One question that needs to be asked is how might taxation impact Bitcoin. Bitcoin is an anonymous currency used in a variety of goods and services transactions. I suspect that the tax implications have not been deeply explored to date. If Bitcoin is to move from the fringes to the mainstream as a virtual currency, then taxation authorities and institutional enterprises will need to take this issue on board. There are many instances when value-added taxes need to be withheld by a vendor; there will be income tax implications for all sides, particularly given the wild shifts in the value of Bitcoin relative to fiat currencies. Within a certain bound, money launderers are not likely to worry about this issue, but legitimate consumers and commercial entities may be concerned about the tax-cost added to transactions[25].

6. Conclusions

In 2011, *Wired* magazine declared that Bitcoin had both risen and fallen (Wallace, 2011). The *Atlantic Magazine* claimed, in 2013, that Bitcoin was not a currency and compared it to a dot-com stock in a bubble[26]. Bitcoin's resilience and acceptance comes in no small part from the robust code and more importantly from the support the currency garners in the computing community. Their patches to the technical alchemy of the code have generated trust amongst Bitcoin users. For some, Bitcoin holds promise as a frictionless and low-cost way of transacting across borders. Bitcoin offers an anonymous transactional mechanism that appeals to criminals and others who want to evade the scrutiny imposed by AML rules; Bitcoin is a virtual paper bag of $100 bills. For governments, Bitcoin's decentralized operation and a lack of a central settling authority make this a challenging form of currency to regulate. There are solutions. The same questions were asked when PayPal emerged as a payment mechanism. The challenge will be to impose the right framework without stifling the innovation underlying the currency and driving the problem underground. Whether Bitcoin becomes a trivia question (akin to who was Edward Snowden?) or whether Bitcoin endures to enter mainstream commerce is still an open question.

Notes

1. Stein, G., *Money* 208 Saturday Evening Post 88 (July 13, 1936).
2. Dion, D., *I'll Gladly Trade you two bits on Tuesday for a Byte Today*, [2013] U. Ill. J. L. Tech and Policy 165 at 182.
3. A penny stock is heavily promoted to victims, the price of the stock is then pumped up and the fraudsters then dump their holdings on a unsuspecting market and walk away with great profit.
4. Dion, D., *I'll Gladly Trade you two bits on Tuesday for a Byte Today*, [2013] U. Ill. J. L. Tech and Policy 165 at 179-180.
5. European Central Bank *Op Cit* note 10.
6. Nakamoto, S., Op Cit note 18.
7. Wallace, B., Op Cit note 19.
8. O'Brien, M., Op Cit note 11.
9. Department of Treasury, Financial Crimes Enforcement Network, *Guidance: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies* (Washington: FIN-2013-G001, March 18, 2013).
10. Shasky Calvery, J., (Director of FinCEN) *Remarks: The Virtual Economy: Potential, Perplexities and Promises* (Washington: US Institute of Peace, June 13, 2013).
11. The US Attorneys Office, Southern District of New York, Indictments and Supporting Materials in *US v. Liberty Reserve S.A.* et al filed May 28, 2013 and available at www.justice.gov/usao/nys/pressreleases/may13/libertyreserveetaldocuments.php (last viewed July 19, 2013).
12. Ibid, paragraph 15 of Exhibit A to the sealed indictment.
13. Associated Press, *Digital Currency Dealers Charged with Money Laundering* (May 28, 2013).
14. US District Court – District of Maryland, Seizure Warrant, Case Number 13-1162 SKG, issued May 14, 2013 by Gauvey,J.
15. How they will do so is uncertain. Banks are concerned about the risk posed by Bitcoin transactions and regulators in places like Canada have yet to land on how one becomes compliant. *Mt.Gox & Coinlab Announce Strategic Partnership to Bolster American Presence, Celebrate $1/2 Billion per Year in Annualized Trades* at www.mtgox.com/press_release_20130228.html (last viewed July 28, 2013).
16. www.paypal.com
17. European Central Bank Op Cit note 10 at p. 44.
18. See for example www.torproject.org (last retrieved August 17, 2013).
19. www.bitcoinfoundation.org
20. Wallace, B., Op Cit note 19.
21. See http://zerocoin.org/ (last viewed on August 20, 2013).
22. Goodin, D., *Malware Mints Virtual Currency*, August 16, 2011, The Register.

23. Securities and Exchange Commission *SEC Charges Texas Man with Running Bitcoin Denominated Ponzi Scheme* (Washington: SEC July 23, 2013).
24. European Central Bank Op Cit note 17 at p. 21.
25. I'm grateful to Mike Ryan, see footnote 1, for suggesting that this question needs to be asked.
26. O'Brien, M., *Bitcoin is No Longer a Currency*, The Atlantic, April 11, 2013.

References

Androulaki, E., Karame, G., Roeschlin, M., Scherer, T. and Capkun, S. (2012), "Evaluating user privacy in Bitcoin", available at: http://eprint.iarc.org/2012/596.pdf (accessed 3 August 2013).

Barber, S., Boyen, X., Shi, E. and Uzun, E. (2012), "Bitter to better – How to make bitcoin a better currency", available at: http://crypto.standford.edu/~xb/fc12/bitcoin.pdf (accessed 21 July 2013).

CBC News (2013), *New York Investigates Wild West of Bitcoin*, Associated Press, available at: www.cbc.ca/news/business (accessed 13, August 2013).

Condon, S. (2013), "Judge spares E-Gold directors jail time posted", available at: http://news.cnet.com/8301-13578_3-10104677-38.html (accessed 17 August 2013).

Cottle, M. (2013), *The Government's Perilous Bitcoin Chase*, The Daily Beast, 25 June.

Cukier, K. and Mayer-Schoenberger, V. (2013), "The rise of big data", *Foreign Affairs*, Vol. 92, p. 3.

European Central Bank (2012), *Virtual Currency Schemes*, ECB, Frankfurt.

FBI Directorate of Intelligence (2012), *Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Unlawful Activity*, 24 April, Wired Magazine.

Gadkari, P. (2013), "Bitcoins at risk of theft BBC", 12 August, available at: www.bbc.co.uk/news/technology-23664743 (accessed 20 August 2013).

Gidda, M. (2013), "Edward Snowden and the NSA files – a timeline", *The Guardian*, 26 July, available at: www.guardian.co.uk/world/2013/jun/23/edward-snowden-nsa-files-timeline (accessed 28 July, 2013).

Greenberg, A. (2013), *Founder of Drug Site Silk Road Says Boom and Bust won't Kill His Black Market*, Forbes, April 16, 2013, available at: www.forbes.com/sites/andygreenberg/2013/04/16/founder-of-drug-site-silk-road-says-bitcoin-booms-and-busts-wont-kill-his-black-market/ (accessed 17 August 2013).

Grinberg, R. (2012), "Bitcoin: an innovative alternative digital currency", *Hastings Science & Technology Law Journal*, Vol. 159 No. 4, pp. 180-181.

Kaminski, K. (2003), *Online Peer-to-Peer Payments: PayPal Primes the Pump*, 7 NC Banking Inst, NC, p. 375

Krugman, P. (2013), "The antisocial network", New York Times, 14 April.

Lee, T. (2013), "Four reasons you shouldn't buy bitcoins forbes 4/03/2013", available at: www.forbes.com (accessed 13 August 2013).

Matonis, J. (2013), "Bitcoin payments could quickly become competitive wedge in online gaming", Forbes, 27 June, available at: http://themonetaryfuture,blogspot.ca (accessed 13 July 2013).

Maurer, B., Nelms, T. and Swartz, L. (2013), "When the real problem is money itself: the practical materiality of Bitcoin", *Social Semiotics*, Vol. 23 No. 2, p. 261.

Miers, I., Garman, C., Green, M. and Rubin, A. (2013), *Zerocoin: Anonymous Distributed E-Cash from Bitcoin*, IEEE Symposium on Security and Privacy.

Myers, S. and Kramer, A. (2013), *Snowden Thanks Russia*, The Globe and Mail, 2 August, p. A3.

Murck, P. (2013), "*Bitcoin* a webinar", in *Association of Financial Crime Specialists*, Murck is general counsel to the Bitcoin Foundation, 26 April.

Nakamoto, S. (2009), *Bitcoin: A Peer-to-Peer Electronic Cash System*, available at: http://bitcoin.org/bitcoin.pdf (accessed 11 July 2013).

O'Brien, M. (2013), *Bitcoin is No Longer a Currency*, The Atlantic, 11 April.

Posadzki, A. (2013), *Kiosks to Convert Cash Into Bitcoin*, Toronto Star, 9 September, p. A4.

Ross, W. (2013), "How to pay for Snowden's getaway without being caught? Bitcoins", *The Daily Beast*, 25 June, available at: www.thedailybeast.com/articles/2013/06/25/how-to-help-pay-for-snowden-s-getaway-without-being-caught-bitcoins.html (accessed 28 July 2013).

Simser, J. (2013), "Recovering the stolen sweets of fraud and corruption", Working Paper Observatario de Economica a Gestao de Fraud, University of Porto.

Wallace, B. (2011), "The rise and fall of bitcoin wired magazine", 23 November, available at: www.wired.com/magazine/2011/11/mf_bitcoin/ (accessed 18 August 2013).

Zelizer, V. (1997), "Her thesis revolves around the broader sociological meanings of money", *The Social Meaning of Money*, Princeton University Press, Princeton, NJ, p. 5.

Corresponding author
Jeffrey Simser can be contacted at: jeffsimser@yahoo.ca