CENTER FOR FINANCIAL STABILITY

Private Roundtable: Bitcoin

Wednesday, October 30, 2013

3:00 p.m.

Sofitel New York

45 West 44th Street

New York, New York 10036

Evan L. Greebel, Esq.
Partner

Kathleen H. Moriarty, Esq.
Partner

Katten Muchin Rosenman LLP

I. Introduction

Bitcoin is an emerging global technology that has developed since the 2008 publication of the seminal paper "Bitcoin: A Peer-to-Peer Electronic Cash System"[1]. To date, it is the best known example of a novel asset class sometimes referred to as "digital assets", "math-based assets" or "digital currency". Bitcoins are not issued by a government, bank or any central organization. Rather, they are based upon open source computer-generated mathematical and cryptographic protocols, existing on an online, peer-to-peer computer network that hosts the public transaction ledger, known as the "Blockchain," and the software source code ("Source Code") that provides the rules for Bitcoins and the peer-to-peer computer network ("Bitcoin Network"). The Bitcoin software Source Code includes the math-based protocols that govern the creation of Bitcoins and the cryptography system that secures and verifies transactions in Bitcoins.

Bitcoins have no physical existence beyond the record of transactions on the Blockchain. The Blockchain serves as a public record of the chain of custody of all Bitcoins issued and registers all Bitcoin transactions, including the issuance of new Bitcoins, as discussed below, and all subsequent movements of Bitcoins in later transactions between users. The Bitcoin Network utilizes the Blockchain to evidence the existence of Bitcoins in any user's digital "Wallet" (analogous to a Bitcoin account) used to hold Bitcoins. Wallets are accessed, and may be used to receive or send Bitcoins, through a digital address coupled with the use of a "public key" and a "private key" that are part of the Bitcoin Network's cryptographic security mechanism, which is a form of what is known as "public key cryptography".

The practical operations of the Bitcoin Network, Bitcoins, and their mathematical underpinnings are complicated and therefore do not lend themselves to "sound byte" explanations. Nonetheless, many discussions of these topics by the media, pundits and bloggers are at best, superficial, or at worst, contain inaccurate explanations, give rise to incorrect inferences or urge future policy actions based upon erroneous assumptions. (See Appendix A for an example of a common misunderstanding concerning Bitcoin's anonymity.) These misconceptions, coupled with public curiosity about illicit enterprises, have focused primary attention on the use of Bitcoin as an "anonymous" tool in connection with unlawful activities, such as dealing in narcotics. This media attention and resulting public discussion, in part, have led to increased governmental scrutiny of Bitcoin use worldwide and in particular in

[1] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (http://bitcoin.org/bitcoin.pdf). Many believe that Satoshi Nakamoto is an alias or pen name of the author or group of authors.

the US, the most recent example of which is the FBI seizure of the notorious Silk Road black market[2].

Although new uses for Bitcoins continue to be discovered, it is clear that Bitcoins can be used as an innovative financial tool with a number of applications, including the purchase and sale of goods, payment for services and facilitation of conversion into fiat currencies at rates determined in the public market. As Bitcoins can be used for a variety of purposes, they should be viewed as both a financial tool and "commodity money"[3], similar to gold bullion. Despite its digital, rather than physical existence, Bitcoin shares several characteristics with gold bullion: both can act as a store of value, there is a limited amount available, an infinite supply will never be created and they are difficult and expensive to "mine" (*i.e.*, generate).[4]

This paper provides a summary explanation of the salient features of Bitcoins and the Bitcoin Network, as well as a brief overview of the current regulatory regimes grappling with Bitcoin, with particular emphasis on the US.

II. Overview of Bitcoins And The Bitcoin Network

Bitcoins and the Bitcoin Network

Bitcoins have been succinctly explained as follows: "Simply put, a bitcoin is an algorithm-based mathematical construct—a unit of measurement invented to quantify value"[5]. Bitcoins are issued by, and transmitted through, the Bitcoin Network that is established by the Source Code and distributed through software downloaded by Bitcoin Network users and persons who create new Bitcoins ("Miners"). As mentioned above, the Bitcoin Network hosts both the public transaction ledger, known as the "Blockchain" and the Source Code. The Bitcoin Network has been, and continues to be, under active, unofficial development by a group of engineers at the Bitcoin Foundation, which works to organize the Bitcoin community and helps to develop and protect the Source Code.

Unlike certain prior digital math-based assets and electronic assets, Bitcoin is not operated by a unitary entity or central server and does not rely on either governmental authorities or financial institutions to create, transmit or value Bitcoins. Rather, the value of Bitcoins is determined by the supply of and demand for Bitcoins in the BTC Markets (defined

[2] "FBI Seizes Silk Road Online Drug Marketplace," Mashable, October 2, 2013 (http://mashable.com/2013/10/02/silk-road-seized/).
[3] George Selgin, University of Georgia, "Synthetic Commodity Money," April 10, 2013 (http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000118).
[4] Ibid.
[5] "7 things you need to know about Bitcoin", PC World, April 11, 2013, http://www.pcworld.com/article/2033715/7-things-you-need-to-know-about-bitcoin.html

below), as well as by the number of merchants and other users that accept them. There are several benefits provided by a decentralized network such as the Bitcoin Network, such as lower transaction costs and confirmation times. The Bitcoin Network's decentralized nature also serves to reduce exposure to the actions of a single large party, thereby limiting such entity's ability to manipulate the network and/or to commit malfeasance with Bitcoins (in contrast, for example, to the very different Liberty Reserve payment system which was allegedly used by its centralized issuer to launder money[6]). This decentralized structure also reduces risk to users, including consumers, businesses, investors and financial institutions, by eliminating a possible singular point of failure. The open-source nature of the security protocols in the Source Code provides a good example of the Bitcoin Network's decentralized structure; this vastly increases the likelihood that a defect in such protocols will be quickly discovered and corrected, because all Bitcoin users store and run the Source Code, thereby reducing the risk of fraud, manipulation and reversal of transactions. Furthermore, because all protocols are determined by consensus of all users on the Bitcoin Network via downloads of the protocol, the risk of a single entity or central authority manipulating the supply of Bitcoin is virtually eliminated. Unless users possessing a majority of the then-current operating power on the Bitcoin Network (collectively, "Majority") agree to alterations, the Bitcoin Network and the protocols underlying Bitcoin cannot be changed.

Each Bitcoin is a digital file that can be transferred from one user to another without the involvement of intermediaries or third parties, thus facilitating direct end-user-to-end-user transactions with little or no transaction costs. In addition, various third party service providers have been established to process transactions between end-users for a fee. Bitcoins are "stored" or reflected on the Blockchain which is a digital file downloaded and stored in a decentralized manner on the computers of each Bitcoin Network user. The Blockchain records the transaction history of all Bitcoins in existence and, through the transparent reporting of all transactions, allows the Bitcoin Network to verify the association of each Bitcoin with the digital Wallet that owns them. The Bitcoin Network and Bitcoin software programs can interpret the Blockchain to determine the exact Bitcoin balance, if any, of any Wallet listed in the Blockchain as having taken part in a transaction on the Bitcoin Network.

[6] In May 2013, the US Attorney for the Southern District of New York and FinCEN took measures against Liberty Reserve S.A. and certain affiliated persons in respect of an indictment on money laundering and other charges, including operation of an unlicensed money transmitting business. Unlike Liberty Reserve, Bitcoin is decentralized and transparent, making it a less attractive tool for money laundering.
See SDNY Indictment at:
http://www.justice.gov/usao/nys/pressreleases/May13/LibertyReserveetalDocuments/Liberty%20Reserve,%20et%20al.%20Redacted%20PIRO.pdf) and
FinCEN Notice of Finding at: (http://www.fincen.gov/statutes_regs/files/311--LR-NoticeofFinding-Final.pdf).

The Bitcoin Network's Structure and Operations

As all Bitcoins are held on the Bitcoin Network and users store and access their Bitcoins through the use of their digital Wallets, a person generally must connect to the Bitcoin Network through Internet access in order to own, transfer or use Bitcoins. Therefore, prior to engaging in any Bitcoin transaction, a user must first install on its computer or mobile device a Bitcoin software program running either the full version, or a compressed "lightweight" version, of the Source Code, that will allow such user to generate a Wallet in which to store its Bitcoins. The Bitcoin Network software program and Wallets also enable users to connect to the Bitcoin Network and engage in the purchase, sale, exchange, transfer or receipt of Bitcoins. Each Wallet has one or more associated individual digital address, each of which is a unique public address (akin to a bank routing code) that is mathematically liked to the "Public Key" – "Private Key" pair of codes[7] that control the Wallet. Transactions in Bitcoins involving a transfer from one user to another are recorded on the Blockchain, which shows the transfer made from the transferor's public address to the transferee's public address. Users access their Wallet through the Public Key and associated Private Key, which are separate but mathematically linked private codes that permit a Wallet to transfer or receive Bitcoins in a transaction. The cryptography behind Public Keys and Private Keys is complex and difficult to explain; however, the standards for Bitcoin's cryptographic security are the same as those designed and published by the NSA[8].

The Bitcoin Network is designed to provide confirmation against "double-spending" a single Bitcoin by memorializing and publishing every transaction in the Blockchain, which is publicly accessible, transparent and is downloaded in part or in whole by all users' Bitcoin Network software programs. This memorialization and verification against double-spending is accomplished through the Bitcoin mining process (discussed below); prior to engaging in any Bitcoin transaction, a user must first notify and update the Bitcoin Network about such forthcoming transaction.

Bitcoin transactions between parties made on-line occur very rapidly (within several seconds). Once a transfer of Bitcoins is initiated, the transaction verification process begins with a broadcast of such transaction information to the Bitcoin Network. The Bitcoin Network memorializes and verifies every transaction in the Blockchain through the Bitcoin "mining" process, which adds "Blocks" of data, including recent transaction information, to the Blockchain. Each transaction will be confirmed when accepted by Miners on the Bitcoin Network and memorialized in the Blockchain, into which a new Block of information (including

[7]For a brief explanation, see "Learn Crypography: Bitcoin Addresses" at: http://learncryptography.com/bitcoin-addresses/

[8] See the discussion of SHA-256, used by Bitcoin, "SHA-2" at http://en.wikipedia.org/wiki/SHA-2

recent transactions) is written approximately every 10 minutes. Currently, a Bitcoin transaction is considered confirmed to a high degree of certainty after it has been written onto the Blockchain and five subsequent Blocks have been added (*i.e.*, after about one hour passes and six Blocks have been added to the Blockchain since the time of the original transaction).

The method for generating new Bitcoins is mathematically established in the Source Code and is deliberately structured so that the supply of Bitcoins will grow at a limited rate pursuant to a pre-set schedule. The number of Bitcoins awarded for solving a new Block is automatically halved every 210,000 Blocks[9]. This intentionally controlled rate of Bitcoin creation ensures that the number of Bitcoins in existence will never exceed 21 million[10] and that Bitcoins cannot be devalued through excessive production, unless the Source Code (and the underlying protocol for Bitcoin issuance) is altered. Users and Miners must accept any changes made to the Bitcoin Network by downloading the proposed modification of the Source Code. A modification of the Source Code is only effective with respect to the Bitcoin users and Miners that download it. Consequently, as a practical matter, a modification to the Source Code will only become part of the Bitcoin Network if accepted and implemented by the Majority.

The process by which new Bitcoins are generated, or "mined", adds new Blocks to the Blockchain and results in new Bitcoins being issued to Miners. Miners engage in a set of prescribed complex mathematical calculations in order to add a Block to the Blockchain and in doing so they also confirm all Bitcoin transactions included in that Block's data. Those Miners successful in adding a Block to the Blockchain are automatically awarded a fixed number of newly generated Bitcoins for their effort; this reward system motivates Miners to add new Blocks to the Blockchain. As the Bitcoin Network is designed so that the reward for adding Blocks to the Blockchain programmatically decreases over time, production and reward of Bitcoins can be expected to eventually cease, unless a new form of compensation is made to Miners. Many participants in Bitcoin believe that Miners will seek transaction fees (whether embedded in the cost of a Bitcoin or otherwise) as compensation to provide adequate incentive to continue their mining activities.

Bitcoin Global Market Participants

A variety of participants are currently involved in the global Bitcoin market, including Miners, retail merchants, their customers, third party service providers, as well as speculators and investors. Market participants include Miners, who range from individual Bitcoin

[9] See, "Mining," at https://en.bitcoin.it/wiki/Mining

[10] As of June 2013, over 11 million Bitcoins have been mined. It is estimated that more than ninety percent (90 percent) of the 21 million Bitcoins will have been produced by 2140. Bitcoins are divisible to 8 decimal places (see: http://gigaom.com/2013/04/04/yes-you-should-care-about-bitcoin-and-heres-why/)

"hobbyists" to groups of computer professionals referred to as "mining pools" that design and build dedicated machines and data centers; today, due to the computational difficulty and the large power requirements, the vast majority of Bitcoin mining is now undertaken by mining pools.

Private and professional investors, as well as speculators, are involved in Bitcoin investment and trading activities. These participants include individual investors, hedge funds, day-traders and dark pools who engage in transactions on one or more Bitcoin exchanges where Bitcoins are publicly bought, sold and traded (collectively "Bitcoin Exchanges"), in off-exchange, over the counter ("OTC") markets (collectively, "BTC Markets") and/or in private, end-user-to-end-user transactions.

A growing number of companies provide a variety of services to Bitcoin users, many related to the buying, selling, payment processing and storing of Bitcoins. These participants include registered money service businesses such as Bitcoin retailers and remittance services, as well as service providers that allow individuals to purchase Bitcoins with fiat currency. Payment processors and commercial gateway service providers allowing retail or commercial businesses to transact in Bitcoin, as well as companies providing Wallets to store Bitcoins for individual users, have been established. The number of merchants accepting Bitcoins as payment and service providers providing offerings to Bitcoin users continues to steadily increase. Yesterday, a Robocoin ATM installed in a Vancouver, Canada coffee shop was readied to exchange cash for Bitcoins, and vice versa (no credit or debit cards are taken)[11]. As the Bitcoin Network continues to gain acceptance, it is anticipated that service providers will expand the currently available range of services and that additional parties will enter the service sector for the Bitcoin Network.

Bitcoin Value

Global trade in Bitcoins currently consists of individual end-user-to-end-user transactions, together with OTC and facilitated exchange-based Bitcoin trading. Due to the peer-to-peer structure of the Bitcoin Network and the protocols thereunder, transferors and recipients of Bitcoins can determine their value of the Bitcoins transferred by mutual agreement or barter with respect to their transactions. These participants generally assess the current value of Bitcoins by reference to the price discovery occurring on one or more Bitcoin Exchanges, usually by surveying the daily trading values and closing prices for Bitcoin on one or more of the Bitcoin Exchanges. Bitcoins are traded on each Bitcoin Exchange with publicly

[11] "Bitcoin ATM installed at Vancouver coffee shop", Peter Meiszner, Global News, October 29, 2013 at http://globalnews.ca/news/931713/bitcoin-atm-installed-at-vancouver-coffee-shop/

disclosed valuations for each transaction, measured by one or more fiat currencies such as the U.S. Dollar or the Chinese Yuan[12].

Since the inception of trading in Bitcoins, prices on Bitcoin Exchanges have fluctuated greatly, and frequently, during certain time periods, and since their introduction in 2009 have experienced a low of $0.00 to a high of $266[13] . Both the amount and rate of change in Bitcoin prices have been significant from time to time. and their price is characterized as "volatile" by most market participants and observers.

Certain Benefits of Bitcoin Adoption

The decentralized nature of the Bitcoin Network and its hardwired protocols, coupled with comparatively low transaction costs, have led some businesses, investors and financial institutions to invest in and/or use Bitcoins on a commercial basis and thereby experience certain benefits. These include:

- *Efficient Remittance and International Wire Transfer*s. The significant reduction of transaction fees and confirmation times provided by Bitcoin relative to existing international wire transfer and/or remittance payment systems has the potential to greatly facilitate secure, direct payments made between individuals. Transactions in Bitcoin occurring directly between sending and receiving parties, or through service providers, can be made in a cost- and time-efficient manner.
- *Rapid Confirmation of Transactions*. Direct peer-to-peer processing of Bitcoin transactions eliminates the need for a trusted third party and permits disintermediated payments between any two consumers with rapid confirmation. In this way, a Bitcoin transaction mimics the payment of cash in-person, but eliminates concerns about counterfeit payments.
- *Reduced Chargeback Risk*. The Bitcoin protocol does not include a mechanism for "chargebacks" (the reversal of a fraudulent or erroneous payment via the payer's banking or financial institution). Although chargebacks provide some consumer protection, the incidence of chargeback fraud has resulted in heightened costs and risks experienced by those merchants accepting credit card and electronic payments. In contrast, merchants accepting payment in Bitcoin do not have to assume the risk of fraudulent chargebacks. (Note that truly erroneous chargebacks can be remedied via a different payment method, such as a bank check or wire transfer.)

[12] See, for example, Mount Gox at MtGox.com; BTC China at https://vip.btcchina.com/, and Bitstamp at https://www.bitstamp.net/

13. "An Illustrated History Of Bitcoin Crashes", Timothy B. Lee, Forbes, 4/11/2013 at http://www.forbes.com/sites/timothylee/2013/04/11/an-illustrated-history-of-bitcoin-crashes/

- *Micropayments/Charitable Contributions*. The low transaction costs resulting from Bitcoin's direct payment methodology make it effective for use in "micropayments" that are otherwise too small, hence commercially infeasible, to be paid via credit card transactions or other electronic payment means. Those businesses who regularly sell products for small amounts of money, such as music, software and e-book companies, as well as news and other organizations with web presences who could sell individual articles, videos and podcasts or administer low-cost "pay walls", may find the Bitcoin structure very attractive. Bitcoin micropayment systems, such as those developed by Bitwall[14] and Bitcoin[15], may enable readers to make small payments and permit media producers to efficiently collect such payments in exchange for individual articles or subscriptions. Additionally, Bitcoin can provide an easy, cost-efficient way for charitable organizations to raise money, especially in small denominations, without being burdened by high processing fees. While organizations such as the Red Cross have experimented with SMS-text initiated payments to permit quick, small-denomination donations, excessive transaction fees have limited the deployment of those donations to their targeted beneficiaries.[16]
- *Bringing Financial Services to "Under-Banked" Communities*. The Bitcoin Network permits two or more parties using their individual Wallets, or accounts with third-party service providers, to engage directly in bank-like transactions with cost-efficient options and greater control over their funds. These features may provide new options to communities for whom banking and transactional services are not readily available or for whom higher banking fees create barriers to use. The mobile payment system M-Pesa in Kenya has been cited as an example of the way in which electronic payment systems controlled by individual users using self-maintained accounts can improve the ability to make and receive payments easily.[17] Similarly, recent press has examined the use of Bitcoin among the homeless community in certain tech-savvy neighborhoods.[18]

[14] See http://www.bitwall.io/.
[15] See "Bitcoin Client BitcoinJ Implements Bitcoin Micropayments," CoinDesk, July 1, 2013 (http://www.coindesk.com/bitcoin-client-bitcoinj-implements-bitcoin-micropayments/) and "Can Bitcoin Enable the Fabled Micropayments Revolution," Gigaom, August 6, 2013 (http://gigaom.com/2013/08/06/can-bitcoin-enable-the-fabled-micropayments-revolution-coinbase-thinks-its-worth-a-shot/).
[16] "Mobile phone charges drain text donations to charities," The Guardian, March 26, 2011 (http://www.theguardian.com/money/2011/mar/27/charities-mobile-phones-text-donations-charges).
[17] See "M-Pesa: Kenta's Mobile Wallet Revolution," British Broadcasting Corporation, November 22, 2010 (http://www.bbc.co.uk/news/business-11793290) and "M-PESA meets Bitcoin with new service in Kenya," Mobile Payments Today, July 12, 2013 (http://www.mobilepaymentstoday.com/article/216119/M-PESA-meets-Bitcoin-with-new-service-in-Kenya).
[18] "Homeless, Unemployed, and Surviving on Bitcoins," Wired, September 20, 2013 (http://www.wired.com/wiredenterprise/2013/09/bitcoin-homeless/).

III. Regulatory Stances Toward Bitcoin

Currently, users and service providers participating in the nascent technology of digital math-based assets operate with limited regulatory guidance. There is confusion as to whether Bitcoins and other digital math-based assets are (i) subject to existing regulations or (2) currently unregulated pending newly adopted regulation specific to the digital math-based asset environment. Furthermore, existing regulations, adopted before the invention of digital math-based assets, are often ill-suited to address their hybrid features as a technology and an asset class, as discussed by the Mercatus Center in "Bitcoin: A Primer for Policymakers".[19] In a report published in May 2013, the General Accounting Office echoed this sentiment when urging the Internal Revenue Service to issue guidance to avoid confusion in the application of US tax law to Bitcoin and other digital math-based assets.[20]

Bitcoin and other digital math-based assets including "alt-coins", such as PrimeCoin and LiteCoin, operate across borders on US state, US federal and global levels. Consequently, an examination of the regulatory landscape necessarily requires consideration of US regulation on all such levels. Additionally, any inquiry into regulation must be mindful that the regulatory stance of any particular region may have an impact on the amount and degree of technological and entrepreneurial activity that occurs in such jurisdictions.

The discussion below is a brief summary of the current legal environment, but given technological development and the increasing use of digital math-based assets, change in this arena can occur quickly, sometimes with little notice. Any jurisdiction that has expressly declined to regulate Bitcoin, tacitly refused to adopt such regulations or has implemented legislation/ regulation of digital math-based assets is free to modify its prior position or alter its actions at any time. Additionally, future court cases may establish precedents different from, or opposed to, regulators' approaches concerning the legality or classification of digital math-based assets.

A discussion of the most suitable characterization of Bitcoin and other digital math-based assets (*e.g.,* a commodity, currency or security) is beyond the scope of this paper, but is an extremely important issue to examine when analyzing the possible legal and regulatory approaches to such assets. In addition, serious consideration should be given to the issue of federal pre-emption to assure uniform treatment of Bitcoin, perhaps in a manner similar to that adopted by the National Securities Markets Improvement Act of 1996 ("NSMIA") with respect to state "blue sky" laws. Finally, it will be important to assess the likelihood that potential regulation or legislation will encourage or stifle Bitcoin innovation, or be more or less

[19] Jerry Brito and Andrea Castillo, George Mason University, "Bitcoin: A Primer for Policymakers," Aug 19, 2013 (http://mercatus.org/publication/bitcoin-primer-policymakers).

[20] "Virtual Economies and Currencies: Additional IRS Guidance Could Reduce Tax Compliance Risks," US Government Accountability Office, May 2013. (http://www.gao.gov/assets/660/654620.pdf).

"friendly" to Bitcoin start-ups. As the fluidity of the Bitcoin technology enables easy migration from one jurisdiction or location to another, it will permit entrepreneurs and others in the digital math- based assets industry to operate in those jurisdictions affording opportunities for growth and advancement.

US Federal Regulation

To date, US federal legislation has not directly addressed the legality or regulation of Bitcoin or other digital math-based assets. Similarly, none of the Internal Revenue Service, the Commodities Futures Trading Commission or the Securities and Exchange Commission have issued express guidance or interpretations with respect to the regulation of the use or classification of Bitcoin and the Bitcoin Network; indeed , each has expressed an awareness of the lack of regulatory certainty.[21] Note that the states and other regulating jurisdictions could benefit from clear guidance on the federal level, which could assist them in making decisions relating to whether or not Bitcoin businesses and activities should be additionally regulated.

- *Legality* The US government and related regulators have not publicly indicated a position as to the legality of using Bitcoin and the Bitcoin Network, or other digital math-based assets. Nevertheless, currently there is no indication that any US federal entity views Bitcoin or the Bitcoin Network as inherently illegal, though the application of existing regulation or the publication of regulation specific to digital math-based assets such as Bitcoin appears to be a priority of certain governmental bodies. Indeed, the Assistant US Attorney, in a criminal complaint against Ross William Ulbricht (the founder/operator of "Silk Road"), noted that "Bitcoins are not illegal in and of themselves and have known legitimate uses."[22]

  Furthermore, a Magistrate Judge in the Shavers case noted that Bitcoin was a form of money and that: "[Bitcoin] can be used to purchase goods or services, and as Shavers

[21] The Internal Revenue Service has been monitoring digital math-based assets and their predecessors since 2007 (http://www.forbes.com/sites/robertwood/2013/06/18/bitcoin-in-irs-crosshairs-says-government-report/). Bart Chilton, a Commissioner of the Commodity Futures Trading Commission indicated that the Commission's staff is considering whether regulation of Bitcoin is needed, and expressed a belief that if it is a commodity that is used as a derivative , Bitcoin would fall within the Commission's jurisdiction http://www.ibtimes.com/cftc-commissioner-bart-chilton-considers-regulating-bitcoin-1242063 Meanwhile, the Securities and Exchange Commission has provided no guidance on Bitcoin itself, but, in the wake of the Bitcoin Savings and Trust indictment, warned investors of financial schemes that involved investment in Bitcoin (http://investor.gov/news-alerts/investor-alerts/investor-alert-ponzi-schemes-using-virtual-currencies).

[22] US vs. Ulrbicht, criminal complaint (http://www.scribd.com/doc/172766650/Criminal-Complaint-Against-Alleged-Silk-Road-Proprietor-Ross-William-Ulbricht).

stated, used to pay for individual living expenses. The only limitation of Bitcoin is that it is limited to those places that accept it as currency." [23]

A forthcoming inquiry by the US Senate Homeland Security Committee will likely focus on the legality of Bitcoin and the Bitcoin network. Additionally, the US House of Representatives has reported to committee an appropriations bill that, as a part of its funding of the Federal Bureau of Investigations, calls for an inquiry into the nature and uses of Bitcoin and other digital math-based assets. [24]

- *Money* T*ransmission (*Note that money service businesses are regulated on both the federal and state level in the US.) The Federal government's regulation of money service business is administered by the Financial Crimes Enforcement Network ("FinCEN"), a bureau of the US Department of the Treasury. On March 18, 2013, FinCEN became the first major governmental agency to directly provide guidance on Bitcoin and other digital math based assets when it released guidance on money transmission and money service business regulation with respect to math-based digital assets. [25] FinCen's guidance called for broad registration of participants in the Bitcoin marketplace, excepting users acquiring Bitcoins for use "to purchase real or virtual goods or services."
  In the only well publicized enforcement action strictly relating to the failure to register with FinCEN as a money service business, the Department of Homeland Security froze a payment account of the largest US Dollar denominated Bitcoin Exchange (Mt. Gox, a Japanese exchange). [26] In the wake of FinCEN's guidance and the freeze of the Mt. Gox account, more US Bitcoin service businesses have sought FinCEN registration, in no small part because of the streamlined registration process, which imposes limited costs and, in substance, requires the reasonable step of adopting anti-money laundering and "know your client" policies and procedures.
- *Classification as Asset Class* Also lacking clarity is Bitcoin's classification as an asset. In the Shavers case, the federal Magistrate Judge stopped short of calling Bitcoin a conventional currency, but correctly noted that it has characteristics akin to a "form of money." [27] The Government Accountability Office has utilized the term "virtual currency" and cited Bitcoin as something akin to virtual property, but did not classify Bitcoin more formally. [28]

---

[23] Securities and Exchange Commission v. Trendon T. Shavers and Bitcoin Savings and Trust, Memorandum Opinion Regarding the Court's Subject Matter Jurisdiction filed August 6, 2013 (http://ia600904.us.archive.org/35/items/gov.uscourts.txed.146063/gov.uscourts.txed.146063.23.0.pdf).
[24] H.R. 2787: Commerce, Justice, Science, and Related Agencies Appropriations Act, 2014 (http://appropriations.house.gov/uploadedfiles/hrpt-113-hr-fy2014-cjs.pdf).
[25] "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," FinCEN, March 18, 2013 (http://fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf).
[26] "Additional $2.1M Seized from Mt. Gox Accounts – Now Over $5M Total," The Genesis Block, August 22, 2013 (http://thegenesisblock.com/warrant-for-mt-gox-wells-fargo-accounts-shows-additional-2-1m-seized/).
[27] See note 23, *supra.*
[28] See note 20, *supra.*

US State Regulation

- *Legality* To date, it appears that no individual state has conducted an examination or made any statements as to whether Bitcoin or any other digital math-based asset is illegal under state law. In August 2013, the New York Department of Financial Services announced an inquiry into the use of Bitcoins and digital math-based asset, which may result in a recommendation regarding future regulation, and may touch on the topic of legality.[29]
- *Money Transmission* Although federal standards apply across the US, local governments also are empowered to regulate money transmission and related businesses within their borders. While federal regulation largely involves registration and standards for the adoption of anti-money laundering and "know your client" policies and procedures, state regulation usually includes a requirement that money service businesses apply for, and receive, licenses from state regulators in order to legally operate within their borders. Pursuant to extraterritorial jurisdiction, certain state regulators require that any business servicing or soliciting residents of a state must register in that state, regardless of whether that business has a physical presence within such state's borders.

  To date, two states (California and Virginia) have issued cease and desist orders to Bitcoin related enterprises that were believed to be violating the requirement of money transmitter licensure.[30] An additional state (Idaho) has provided formal guidance that a state regulatory body believes that Bitcoin service businesses, such as digital currency exchanges, serving state residents are required to seek a license under the Idaho Money Transmitters Act.[31] In the announcement of its aforementioned inquiry, the New York Department of Financial Services also indicated its belief that Bitcoin related businesses were engaged in money transmission, which requires licensure from, and regulation by, New York State.[32] Additional states may have made less publicized determinations.

  Note that the process of obtaining licenses to operate in all states and jurisdictions within

[29] "Notice of Inquiry on Virtual Currencies," New York Department of Financial Services, August 22, 2013 (http://www.dfs.ny.gov/about/press2013/memo1308121.pdf).

[30] California Department of Financial Institutions mailed a cease and desist letter warning to the Bitcoin Foundation, warning that it may be conducting the business of money transmission in the State of California without license as a money transmitter from the California Commissioner of Financial Institutions (http://www.scribd.com/doc/149335233/CA-State-Cease-and-Desist-May-30#page=1). Similarly, as described in a statement put forth by the recipient of the letter, the Virginia Corporation Commission determined that Tangible Cryptography's FashCash4Bitcoins operations may constitute money transmission under Virginia law, requiring licensure (https://fastcash4bitcoins.com/index.aspx).

[31] Money Transmitter No Action Opinion Letter, August 21, 2013 http://finance.idaho.gov/MoneyTransmitter/Documents/Money_Transmitter_No_Action_Opinion_Letters_2009-2013.pdf.

[32] See note 29, *supra*.

the US, including the District of Columbia, requires a substantial investment of time and money; currently, the combined fees for state filings and licenses are in excess of $30,000.

Foreign Regulation of Bitcoin and its Users

European Central Bank: Issued a report on virtual currencies in October 2012 that noted that the legal status of Bitcoin and other digital math-based assets was unclear, but that "some initial attempts to define the legal status of Bitcoin are already happening in Europe."[33]

Germany: In August 2013, the German Ministry of Finance released an interpretation that labeled Bitcoin as "Rechnungseinheiten" (i.e., private money or a unit of account that is not recognized as a full currency, but is subject to German tax laws).[34] The report recognized the legality of Bitcoin, but did not institute a regulatory regime outside of tax treatment.

Canada: Canada has stated that income from Bitcoin activities is taxable (i) as barter if Bitcoins are provided as income or sold as goods/services or(ii) as capital gains if held as an investment.[35] At the same time, the Canadian government regulator FINTRAC has declined to apply money services business rules to Bitcoin service providers including Bitcoin exchanges.[36]Also, the Bitcoin ATM mentioned above will not be monitored by the Ottawa Financial Transactions and Reports Analysis Centre because Bitcoin is not recognized as a currency in Canada[37].

United Kingdom: As in Canada, the United Kingdom has indicated that standard tax laws apply to Bitcoin activity and investments, but that Bitcoin exchanges and other service providers need not register with HM Revenue & Customs under Money Laundering

---

[33] "Virtual Currency Schemes," October 2012 (http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf).

[34] "Bitcoin recognized by Germany as 'private money,'" CNBC, August 19, 2013 (http://www.cnbc.com/id/100971898).

[35] "Revenue Canada says BitCoins aren't tax exempt," Canadian Broadcasting Corporation, April 26, 2013 (http://www.cbc.ca/news/business/revenue-canada-says-bitcoins-aren-t-tax-exempt-1.1395075).

[36] "Canadian regulator takes lighter view of Bitcoin," PCWorld, May 21, 2013 (http://www.pcworld.com/article/2039347/canadian-regulator-takes-lighter-view-of-bitcoin.html). In a letter sent to Bitcoin exchanges, the Canadian Financial Transactions and Reports Analysis Centre of Canada wrote:
"Your entity is not, at this time, engaged as a money services business in Canada as per the Proceeds of Crime (Money Laundering) and Terrorist Financing and its associated Regulations.
In fact, your entity doesn't provide the services of remitting and/or transferring funds for the sake of the service. The transfer of funds is simply a corollary of your actual service of buying and selling virtual currency. Therefore, you do not have to register your entity with us."
"Canadian regulators welcome US Bitcoin refugees with open arms," The Register, May 20, 2013 (http://www.theregister.co.uk/2013/05/20/canada_welcomes_bitcoin_traders_fintrac_letter/).

[37] A Vancouver Coffee Shop Has The World's First Bitcoin ATM", Julie Gordon, Reuters, Oct. 29, 2013, http://www.businessinsider.com/bitcoin-atm-canada-2013-10

regulations at the present time.[38]

Finland: On August 28, 2013, the Finnish Tax Authority released guidance regarding the taxation of virtual currencies (including Bitcoin). The guidance includes income tax, taxing transactions, taxing mining and gaming revenue and taxing corporations and investments in virtual currencies.[39]

Australia: the Australian Taxation Office has noted that income from Bitcoin trading activities is subject to taxation, and transactions conducted in Bitcoin are subject to the same taxes as those conducted using fiat currencies.[40]

Netherlands: In June, 2013, Dutch Finance Minister Jeroen Dijsselbloem, when questioned by parliament, noted that income on Bitcoin transactions would be subject to taxation, but that Bitcoin was not "electronic money" because it fails the definitional test set forth in Dutch law.[41]

Other jurisdictions: Other jurisdictions that have experienced activity involving Bitcoin or other digital math-based assets, including *India*,[42] *China*[43] and *Japan*, either have displayed little public stance toward Bitcoin or have affirmatively declined to regulate digital math-based assets. The "hands off" stance of the Chinese government has led to significant adoption of Bitcoin and other digital math-based assets among small users and, more recently, Baidu Inc., China's equivalent to Google.[44]

---

[38] "HMRC: UK bitcoin exchanges don't have to register under money laundering regulations," CoinDesk, July 8, 2013 (http://www.coindesk.com/hmrc-uk-bitcoin-exchanges-dont-have-to-register-under-money-laundering-regulations/). The no-action letter providing the guidance clarified that the United Kingdom does not now view Bitcoin as a currency.

[39] Virtuaalivaluuttojen tuloverotus, August 28, 2013 (http://vero.fi/fi-FI/Syventavat_veroohjeet/Verohallinnon_ohjeet/Virtuaalivaluuttojen_tuloverotus%2828450%29).

[40] "ATO targets Bitcoin users," Financial Review, June 24, 2013 (http://www.afr.com/p/technology/ato_targets_bitcoin_users_oawpzLQHDz2vEUWtvYLTWI).

[41] "Bitcoin income shall be taxes, Dijsselbloem says," 24Oranges, June 17, 2013 (http://www.24oranges.nl/2013/06/17/bitcoin-income-shall-be-taxed-dijsselbloem-says/). The Dutch law on financial control defines electronic money as monetary value that i) is stored electronically, ii) represents a claim on the person or organization who issues it, iii) is issued in exchange for money to make payments with, and iv) can be used to pay both the issuer and others.

[42] "Reserve Bank of India Won't Regulate Virtual Currency Bitcoin, Yet," Economic Times, August. 14, 2013 (http://articles.economictimes.indiatimes.com/2013-08-14/news/41409715_1_bitcoin-gox-virtual-currency). "India's central bank is 'watching' Bitcoin, the virtual currency that is gaining popularity among Net users, but has no intention of regulating it right now."

[43] "China Banking Regulatory Commission [actually said]: 'As of today, there are no regulatory policy plans directed against Bitcoin,'" BitByBitByBitcoin, October 17, 2013 (http://bitbybitbybitcoin.wordpress.com/2013/10/17/china-banking-regulatory-commission-actually-said-as-of-today-there-are-no-regulatory-policy-plans-directed-against-bitcoin/), discussing a translation of a report in Mandarin (http://finance.sina.com.cn/money/lczx/20131017/071917018288.shtml).

[44] "Baidu (BIDU) Approves Bitcoin Payment, Virtual Currency Value Skyrockets," International Business Times, October 23, 2013 (http://www.ibtimes.com/baidu-bidu-approves-bitcoin-payment-virtual-currency-value-skyrockets-1437956).

APPENDIX A

Bitcoin Anonymity and Money Laundering

Despite widespread reports to the contrary, Bitcoin is not an anonymous payment network. Bitcoin users are "pseudonymous", in that they adopt one or more digital addresses (string of alphanumeric characters that serve as a routing address for a Bitcoin user's account(s)). These digital addresses are the user's pseudonym(s) on the Bitcoin Network. They can be traced to a Bitcoin user in several ways, through:

- the IP addresses used to send data relating to spending transactions, which are typically published on the Blockchain;
- the anti-money laundering and know your client information provided by service providers, particularly exchanges, retail sellers of Bitcoin or commercial enterprises who transact business with the digital address; and
- any public activity that ties a person's real world identity to the digital address.

It is important to understand the open nature of the Blockchain permits real-time analysis of user activity.[45] Typically, points of access to Bitcoin *(i.e.,* where Bitcoin is converted into fiat currency or goods and services) can be used to tie a user's identity to its pseudonymous digital address. The full transparency of transactions on the Bitcoin Network through the Blockchain permits open analysis of user activity, as described in an academic publication from the Weizmann Institute of Science.[46] A more complete discussion of issues relating to Bitcoin and its pseudonymous nature is available in a prominent paper from the University of California at San Diego and George Mason University.[47]

While sophisticated steps utilizing "dark webs", such as the Tor Network[48] , or "coin mixing" services[49], allow some users to make it more difficult to connect their pseudonyms to their

[45] Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker and Stefan Savage, University of California, San Diego and George Mason University, "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names," October 2013 (http://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf)

[46] Dorit Ron and Adi Shamir, Weizmann Institute of Science, "Quantitative Analysis of the Full Bitcoin Transaction Graph," October 18, 2012 (http://eprint.iacr.org/2012/584.pdf).

[47] See note 45, *supra*.

[48] "Dark web" systems such as the Tor Network use various servers and software in an attempt to make their use untraceable and/or anonymous. Although it has uses other than for illicit purposes, it is often associated with black market services such as Silk Road. See http://en.wikipedia.org/wiki/Tor_%28anonymity_network%29.

[49] Coin mixing services are services that intentionally attempt to launder coins by mixing large numbers of coins and sending them back to their owners at new digital wallets that may not be tied to a user's identity. See The Politics Of Bitcoin Mixing Services, Forbes, June 5, 2013 (http://www.forbes.com/sites/jonmatonis/2013/06/05/the-politics-of-bitcoin-mixing-services/).

actual identities anonymity within the Bitcoin Network has been mistakenly reported and vastly overstated. The ability of users to "launder" money through Bitcoin requires a level of technological expertise far beyond that possessed by the average individual and such expertise does not eliminate the traces of activities that are common markers of money laundering *(i.e.*, transactions using coin mixing services can be at least partially traced through a quantitative analysis of the transaction graph). Furthermore, the use of the Tor Network and other sophisticated measures to hide illicit activity did not have the intended effect for the individuals arrested in the FBI's recent raid on the Silk Road black market.[50] The resources of the US law enforcement and intelligence communities are well equipped to handle challenges relating to analysis and tracking of the Blockchain and illegal activities related thereto. In fact, because the Blockchain records the flow of funds and logs certain IP addresses, it provides law enforcement and intelligence offices with a tool to track attempted money laundering and other illicit transactions using Bitcoin, a tool that is not available when criminals use cash.

[50] See, e.g., "How the FBI Brought Down Cyber-Underworld Site Silk Road," USA Today, October 21, 2013 (http://www.usatoday.com/story/news/nation/2013/10/21/fbi-cracks-silk-road/2984921/).