Virtual Currency:

Issues and Promise

Compiled and Edited by

Michael Erbschloe

Connect with Michael on LinkedIn

Table of Contents

About the Editor

Michael Erbschloe has worked for over 30 years performing analysis of the economics of information technology, public policy relating to technology, and utilizing technology in reengineering organization processes. He has authored several books on social and management issues of information technology that were published by McGraw Hill and other major publishers. He has also taught at several universities and developed technology-related curriculum. His career has focused on several interrelated areas:

- Technology strategy, analysis, and forecasting
- Teaching and curriculum development
- Writing books and articles
- Publishing and editing
- Public policy analysis and program evaluation

Books by Michael Erbschloe

Threat Level Red: Cybersecurity Research Programs of the U.S. Government (CRC Press)
Social Media Warfare: Equal Weapons for All (Auerbach Publications)
Walling Out the Insiders: Controlling Access to Improve Organizational Security (Auerbach Publications)
Physical Security for IT (Elsevier Science)
Trojans, Worms, and Spyware (Butterworth-Heinemann)
Implementing Homeland Security in Enterprise IT (Digital Press)
Guide to Disaster Recovery (Course Technology)
Socially Responsible IT Management (Digital Press)
Information Warfare: How to Survive Cyber Attacks (McGraw Hill)
The Executive's Guide to Privacy Management (McGraw Hill)
Net Privacy: A Guide to Developing & Implementing an e-business Privacy Plan (McGraw Hill)

Introduction

There is no single commonly accepted definition of virtual or digital currency. For purposes of this volume, virtual currency is a digital representation of value that can be traded on the Internet and functions as (1) a medium of exchange; (2) a unit of account; and/or (3) a store of value, but does not have legal tender status in any jurisdiction. Virtual currency is distinguished from fiat currency (a.k.a. "real currency," "real money," or "national currency"), which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country. Virtual currency is also distinct from e-money, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism for fiat currency—i.e., it electronically transfers value that has legal tender status. Digital currency is a digital representation of either virtual currency or e-money.

Although virtual currencies may support important innovation and serve legitimate purposes, like traditional currencies or other methods of transferring value, virtual currencies may also be exploited for the purposes of money laundering, the facilitation and financing of terrorism, and to enable other crimes such as child pornography, drug trafficking, and cybercrimes.

Virtual currencies are designed to be an alternative to current payment systems. Better-known virtual currencies include Bitcoin, XRP, and Dogecoin. Often referred to in the industry as "digital currencies," they are a way for people to track, store, and send payments over the Internet, and they may have the potential to make payment processing cheaper or faster. But they are not backed by any government or central bank. In addition, because virtual currency accounts are not insured by the Federal Deposit Insurance Corporation or the National Credit Union Share Insurance Fund, if a virtual currency company fails – and many have – the government will not cover the loss.

Virtual currency companies are springing up around the world to offer products and services to consumers. There are virtual currency exchanges, which are companies that help consumers buy or sell virtual currencies. There are also online "digital wallet providers," which are companies that allow consumers to create accounts with them to store and manage their virtual currencies. Many virtual currency exchanges are also wallet providers, and vice versa.

Pitfalls include:

Exchange rates are volatile and costs unclear: The exchange rate of Bitcoins to U.S. dollars in 2013 fell as much as 61 percent in a single day. In 2014, the value of Bitcoins has dropped by as much as 80 percent in a single day. The advisory explains that consumers who buy virtual currencies should be prepared to weather this kind of volatility. Consumers should also consider

whether there are mark-ups or other fees when using an exchange or digital wallet provider. Companies may be charging consumers to buy, spend, or accept virtual currencies.

Hackers and scammers pose serious security threats: Virtual currencies are targets for highly sophisticated hackers and scammers. Individuals, digital wallet providers, and exchanges are all at risk. For example, if a hacker gains access to a consumer's Bitcoin "private keys," which are 64-character codes that unlock the consumer's funds, the consumer can lose all their virtual currency. Fraudsters are also taking advantage of the hype surrounding virtual currencies to pose as Bitcoin exchanges, Bitcoin intermediaries, and Bitcoin traders in an effort to lure consumers to send money, which is then stolen.

Companies may not offer help or refunds for lost or stolen funds: Some virtual currency companies do not identify their owners, provide phone numbers and addresses, or even specify the country in which they are located. Before using a company's products or services, consumers should carefully consider if they know how to contact the company in question, and if they know their contractual rights. If a consumer trusts a company to hold their virtual currencies and something goes wrong, the company may not offer the kind of help the consumer would expect from a bank, debit card, or credit card provider. In fact, some virtual currency companies disclaim responsibility for consumer losses if funds are lost or stolen.

In February 2014, the Mt. Gox virtual currency exchange filed for bankruptcy, stating that a security breach resulted in the loss of bitcoins worth more than $460 million at the time. This incident is one of many real-world illustrations of the risks involved in using virtual currencies.

On January 24, 2018 the CFTC Charged Randall Crater, Mark Gillespie, and My Big Coin Pay, Inc. with Fraud and Misappropriation in Ongoing Virtual Currency Scam. Defendants allegedly solicited more than $6 million for investments in a virtual currency known as "My Big Coin"

The Commodity Futures Trading Commission (CFTC) announced the filing of a federal court enforcement action under seal on January 16, 2018, charging commodity fraud and misappropriation related to the ongoing solicitation of customers for a virtual currency known as My Big Coin (MBC). The CFTC Complaint charges Defendants Randall Crater of East Hampton, New York, Mark Gillespie of Hartland, Michigan, and My Big Coin Pay, Inc., a corporation based in Las Vegas, Nevada, with misappropriating over $6 million from customers by, among other things, transferring customer funds into personal bank accounts, and using those funds for personal expenses and the purchase of luxury goods.

On January 16, 2018, Judge Rya Zobel of the U.S. District Court for the District of Massachusetts, issued a restraining Order, also under seal, freezing the Defendants' assets. The Order also freezes the assets of Relief Defendants Kimberly Renee Benge, Kimberly Renee Benge d/b/a Greyshore Advertisement a/k/a Greyshore Advertiset, Barbara Crater Meeks, Erica Crater, Greyshore, LLC, and Greyshore Technology, LLC for allegedly receiving customer funds without providing any legitimate services to clients and without any interest or entitlement

to such customer funds. The court's restraining Order also prohibits the Defendants and Relief Defendants from destroying or altering books and records.

CFTC's Director of Enforcement Comments

Director of Enforcement James McDonald, stated: "As this case shows, the CFTC is actively policing the virtual currency markets and will vigorously enforce the anti-fraud provisions of the Commodity Exchange Act. In addition to harming customers, fraud in connection with virtual currencies inhibits potentially market-enhancing developments in this area. We caution potential virtual currency customers, once again, that they should engage in appropriate diligence before purchasing virtual currencies."

Specifically, the CFTC Complaint alleges that from at least January 2014 through January 2018, the Defendants fraudulently solicited potential and existing MBC customers throughout the United States by making false and misleading claims and omissions about MBC's value, usage, and trade status, and that MBC was backed by gold. Defendants also allegedly fraudulently solicited numerous customers in the District of Massachusetts, receiving in excess of $5 million from those customers.

As alleged in the Complaint, the MBC website, maintained and operated by the Defendants, conveyed to customers numerous solicitation materials, MBC trade data, and other materials (1) misrepresenting that MBC was actively being traded on several currency exchanges, including the MBC Exchange website, when in fact it was not; (2) misrepresenting in reports the daily trading price, when in fact no price existed because MBC was not trading; (3) misrepresenting that MBC was backed by gold, when in fact it was not; and (4) misrepresenting that MBC had partnered with MasterCard, with the promise that MBC could be used anywhere MasterCard was accepted, when in fact no such partnership existed and MBC could not be used anywhere MasterCard was accepted. In reality, as alleged, the supposed trading results were illusory, and any payouts to customers were derived from funds fraudulently obtained from other customers in the manner of a Ponzi scheme.

As customers began to raise questions about their MBC accounts, Defendants attempted to conceal their fraud by issuing additional coins to customers and falsely representing that they had secured a deal with another exchange to trade MBC, according to the Complaint. Defendants allegedly encouraged customers to refrain from redeeming their MBC holdings until MBC was active on this "new" exchange.

Misappropriated Funds Used for Personal Purchases, Including a Home, Jewelry & Travel

As further alleged in the Complaint, Defendants misappropriated virtually all of the approximately $6 million they solicited from customers. Defendants allegedly used these misappropriated funds to purchase a home, antiques, fine art, jewelry, luxury goods, furniture, interior decorating and other home improvement services, travel, and entertainment.

In its continuing litigation, the CFTC seeks civil monetary penalties, restitution, rescission, disgorgement of ill-gotten gains, trading and registration bans, and permanent injunctions against further violations of the federal commodities laws, as charged.

This case is brought in connection with the CFTC Division of Enforcement's Virtual Currency Task Force, and CFTC staff members responsible for this case are Traci Rodriguez, Patricia Gomersall, Jonah McCarthy, Jason Mahoney, Hillary Van Tassel, John Einstman and Paul Hayeck.

Source: https://www.consumerfinance.gov/about-us/newsroom/cfpb-warns-consumers-about-bitcoin/

http://www.cftc.gov/PressRoom/PressReleases/pr7678-18

Virtual Currency Investigative Challenges and Opportunities

By Brett Nigh, J.D., and C. Alden Pelker

In June 2014 the U.S. Marshals Service held a first-of-its-kind auction to sell an unusual asset: 29,656 "bitcoin," units of "virtual currency," which function much like traditional currency on the Internet but are not controlled or backed by any national government.1 The bitcoin, valued at $18 million at the time of auction, were a portion of more than 179,000 units seized by the FBI in 2013 during the takedown of Silk Road, an extensive black market website. For over two years, Silk Road facilitated the sale of hundreds of millions of dollars worth of narcotics, stolen identities, and numerous other illegal goods and services.2 All transactions were conducted exclusively in bitcoin.

Use of virtual currency has evolved over nearly two decades alongside the expansion of the Internet. Every day, people across the globe use the Web to move money. Most transactions are denominated in U.S. dollars or another national currency. However, a small but increasing fraction of those transactions use virtual currency as an alternative form of payment. Until recently, all virtual currency existed within centralized systems. In the centralized model a private company controls the virtual currency, issues units to its users, determines the virtual currency's value, records transactions, and keeps track of customers' balances. The company is the controlling force that drives everything in the system.

Centralized virtual currency systems encompass a wide range of business models. The technical operation of online payment systems, such as WebMoney and the now-defunct Liberty Reserve, is nearly identical to that of traditional online systems, apart from denominating users' accounts in virtual currency, rather than a national currency. Some systems, such as Pecunix and the now-defunct e-Gold, allow users to exchange digital units of gold bullion or other precious metals, earning the systems the name "digital precious metals." Other systems operate within popular virtual worlds and online games where entire microeconomies develop among players relying on in-game currency.

Over the past six years, decentralized virtual currencies also have grown to prominence in the virtual currency landscape. Decentralized virtual currency systems afford users many of the same benefits as their centralized counterparts—users can hold funds and transfer value to other users within the system. However, unlike centralized systems, decentralized systems are not run by a company. Rather, transactions are sent across a peer-to-peer network without involving a third

party. Users anywhere in the world can download the free, open-source software specific to a particular decentralized virtual currency. Once they have done so, users can send funds securely and almost instantly across vast distances with just the click of a button. Bitcoin is by far the most popular and well-known decentralized virtual currency, with a total market value of approximately $3.4 billion as of May 2015. However, there are hundreds of other decentralized virtual currencies—often called “altcoins”—also in circulation.

VIRTUAL CURRENCY VALUATION

Most virtual currency in centralized systems has a fixed value whereby the controlling company sets an exchange rate. Often, this value is linked to some quantity of national currency. For example, one Liberty Reserve Dollar was equal to one U.S. dollar, and one unit of WMZ, a currency controlled by WebMoney, also is equal to one U.S. dollar. The value also may be fixed to some other real-world value. Companies running digital precious metals systems fix their virtual currency’s value to some quantity of a precious metal, commonly gold bullion. Alternately, a virtual currency’s value may fluctuate based on the supply of and demand for units of that currency. This model is seen frequently in decentralized virtual currencies, which have no company to enforce a pegged exchange rate.

EXCHANGERS AND THIRD-PARTY SERVICES

While users can transact entirely in virtual currency within a system, most individuals also want to cash in and out of the system, converting their dollars to virtual currency and, ultimately, back again. This exchange function is central to the virtual currency ecosystem. In centralized models the user may deal directly with the administrating company to cash in or out. However, not all companies offer this service, and decentralized systems lack the capability altogether. As a result, third-party companies have established themselves as “exchangers,” providing a venue for customers to cash in and out of virtual currency or to convert from one virtual currency to another. Exchangers are one component of a network of sites and services that have developed to support and enhance the virtual currency landscape.

Under U.S. money services business regulations, any business that transfers virtual currency from one person or location to another is obligated to register with the Financial Crimes Enforcement Network (FinCEN) and comply with Bank Secrecy Act (BSA) requirements, including implementing anti-money-laundering programs and filing suspicious activity reports (SARs).3 Additionally, many states require money transmitters to obtain state licenses. The U.S. Department of Justice has identified these regulations as "crucial tools in preventing malicious actors from exploiting virtual currency systems in furtherance of illicit activity."4

In the United States numerous virtual currency services have made significant strides to comply with regulations. However, many still struggle to implement effective anti-money-laundering programs and to comply with state-level requirements. This is particularly problematic in the current business environment, where many virtual currency companies begin operation illegally before ensuring full compliance with all applicable regulations. Where this occurs, even well-intentioned systems are left vulnerable to exploitation by criminals and terrorists.

LAW ENFORCEMENT INTERESTS

Virtual currency systems are not inherently illicit and are used by legitimate consumers every day to conduct legal transactions. These systems allow users to move funds quickly and efficiently across great distances without being tied to one country's currency or worrying about international conversions. Like nearly any financial product, however, these systems can be exploited by criminals to further their illegal activities. Therefore, law enforcement has two primary interests in virtual currency. First, officers will investigate criminals who use virtual currency to move or hide money derived from criminal or terrorist acts (i.e., money laundering). Second, investigators will look at virtual currency businesses that violate laws proscribing money laundering or illegal money transmission.

As virtual currency systems have evolved, so, too, has their criminal-user base. Early adopters of virtual currency generally were cybercriminals and perpetrators of specialized, complex financial fraud. Now, as criminals become more technologically proficient and systems grow more user-friendly, virtual currency is seeing a wider user base, spanning from the most sophisticated cyberactors to low-level drug dealers.

The illicit use of virtual currency has grown tremendously in online black marketplaces, many of which are accessible only through the Tor Network, which anonymizes users' Internet traffic by routing it through a worldwide network of volunteer nodes. Criminals have exploited Tor's privacy-enhancing features to create black market websites where users can buy or sell almost any illegal merchandise or service imaginable. Silk Road was one of many such black market sites—albeit an exceptionally successful one.

INVESTIGATIVE CHALLENGES

The particular features of virtual currency systems, especially decentralized systems, present new challenges for law enforcement. Many of the benefits that virtual currency systems promise legitimate consumers, such as increased privacy in transactions and the ability to send funds without an intermediary, serve as obstacles to law enforcement when the systems are exploited for illegal purposes. Key challenges identified by law enforcement officers dealing with virtual currency include regulatory and compliance disparities, transaction obfuscation and anonymity, and the global nature of the systems.

Regulatory and Compliance Disparities

Criminals gravitate to services with weak or nonexistent anti-money-laundering and customer identification programs. Those systems flourish in countries with poor regulatory oversight and ineffective enforcement. Because of virtual currency's unique features, namely its lack of government backing, it falls within a regulatory gray area in many foreign jurisdictions. Therefore, many systems do not identify or report suspicious transactions, fail to retain customer records, and often resist cooperation with law enforcement.

Transaction Obfuscation and Anonymity

Virtual currency transactions can be difficult to track, due in part to the structure of the systems themselves, as well as their privacy-enhancing features. Many services allow users to maintain higher levels of anonymity than would be permitted in a traditional currency-based system. Even if an investigator is successful in following the transaction, it still may be difficult to tie a virtual

account to a real-world identity. This process further is complicated by decentralized systems, where there no longer is a single company holding customer records.

Systems' Global Nature

The above challenges further are exacerbated by the inherently global nature of the virtual currency ecosystem. Customers and services can transact with little regard to national borders, creating investigative challenges and jurisdictional hurdles. Any investigation involving substantial use of virtual currency is likely to rely on international cooperation. However, the speed of the legal process cannot keep up with the pace of these transactions.

REGULATION AND GUIDANCE

Law enforcement agencies can use the existing legal framework to investigate money laundering criminals and the money-services businesses they employ. Since the BSA was passed in 1970 to combat the laundering of illicit money through banks, the financial system has changed and been innovated.5 The regulatory framework also has been extended to encompass electronic banking, prepaid cards, and other financial tools that the BSA did not originally contemplate.6 Recently, regulators and courts explicitly have addressed virtual currency.

In March 2013 FinCEN issued interpretive guidance for the regulation of virtual currency. The guidance explains that administrators and exchangers of convertible virtual currency are money transmitters under existing regulations. Therefore, these entities must register with FinCEN, keep records, and report suspicious transactions. The guidance also states that a user who merely obtains virtual currency and uses it to purchase goods or services is not a money-services business under FinCEN's regulations.7 Additional guidance in January 2014 clarified that an entity that mines or produces bitcoin and uses it for its own purposes also is not a money-services business with obligations to FinCEN under the BSA.8

The U.S. Securities and Exchange Commission (SEC) stated in a July 2013 investor alert that "any investment in securities in the United States remains subject to the jurisdiction of the SEC regardless of whether the investment is made in U.S. dollars or a virtual currency."9 The District Court for the Eastern District of Texas came to a similar conclusion a month later in Securities

and Exchange Commission v. Shavers.10 The court ruled that it had subject matter jurisdiction under the Securities Act of 1933 over a case involving allegations of a Bitcoin Ponzi scheme because the court found that investments purchased with bitcoin met the definition of an investment contract and, thus, were securities.11

The Internal Revenue Service (IRS) issued guidance in March 2014 indicating that virtual currency would be treated as property for federal tax purposes.12 General tax principles that apply to property transactions also will apply to virtual currency transactions. As a consequence, Bitcoin users, miners, and service providers must keep records of wages paid, transactions, fair market value, and loss or gain from transactions.13

The guidance issued by the federal government provides a growing framework for law enforcement to investigate the illegal use of virtual currencies. State regulatory agencies also are examining how their current laws on currency exchange and money transmission apply to virtual currency.14

CRIMINAL INVESTIGATIONS AND PROSECUTIONS

The U.S. Department of Justice has used BSA statutes to prosecute virtual currency systems intentionally designed to facilitate illegal activity. These services did not conduct any meaningful customer due diligence and did not screen for transactions related to money laundering or terrorist financing. As money transmitters, the services were required under Title 31, Section 5330, U.S. Code, to register with FinCEN.15 Most states also require money transmitters to obtain a license to conduct business in the state. A money transmitter that fails to register with FinCEN or obtain the necessary state license may be subject to prosecution under Title 18, Section 1960, U.S. Code.16 In addition, the money laundering statutes Title 18, Sections 1956 and 1957, U.S. Code, apply to transactions involving virtual currency, and the U.S. Department of Justice employs them for prosecuting criminals using virtual currency.17

In 2007 federal prosecutors indicted e-Gold on charges of money laundering and operating an unlicensed money-transmitting business. E-Gold required only a valid e-mail address to set up an account and did not conduct due diligence on customers. Identifying information provided by users often was obviously false, and, therefore, transactions were highly anonymous. As a result

e-Gold became a favorite payment method for criminals involved in credit card fraud, identity theft, and child pornography sales. In 2008 e-Gold and its three principal owners pled guilty.18

Federal prosecutors indicted Liberty Reserve and its executives in 2013 for running a $6 billion money laundering operation. The founder of Liberty Reserve allegedly designed the system to evade U.S. law enforcement. According to the indictment, the system allowed users to send and receive funds without requiring them to validate their identities and permitted customers to make untraceable transfers for a privacy fee. Liberty Reserve never registered with the appropriate U.S. authorities, even though many of its transactions originated from or were sent out of the United States.19

BITCOIN-RELATED CRIMES

The potential for state and local law enforcement officers to encounter virtual currency in investigations will increase as virtual currency becomes more popular. Bitcoin-related crimes may involve "stolen wallets," "botnet mining," "ransomware," or use of Bitcoin in furtherance of traditional crimes, such as drug dealing, fraud, or identity theft.20

Cybercriminals can steal Bitcoin wallets individually or from numerous users through exchanges and service businesses. These criminals may obtain the "private key"—the ticket to transferring a user's bitcoin—for the victim's wallet by infecting the victim's computer with malware or hacking into a wallet-service provider or exchanger.21 After the offenders have stolen the bitcoin, they may take steps to conceal their transactions. A popular technique is the use of a "tumbler" or "mixing" service, which takes bitcoin from many users, routes them through a complex funding path, and redistributes them so they no longer can be readily traced to a specific source.

INVESTIGATIVE METHODS

While considerable challenges exist in dealing with virtual currency, many traditional tools and investigative methods remain effective. Virtual currency transactions through centralized systems may be traced much the same way transactions are followed through conventional online payment services. Investigators can follow the money through decentralized virtual

currency systems, as well. Decentralized systems typically offer public transaction ledgers, which record every transaction that crosses the network.

Law enforcement officers should use standard cyber investigative techniques in a theft case involving decentralized virtual currency. Imaging the victim's computer system and obtaining Internet service provider (ISP) logs will assist in identifying the origin of the criminal activity. Officers may have difficulty obtaining the information necessary to trace the transaction if the victim uses a wallet-service provider or exchanger located in an uncooperative foreign jurisdiction. If investigators can obtain the time of the transaction and the victim's public key, they may use the public transaction ledger to determine the address to which the virtual currency was sent.

When investigating criminal activity involving, for example, Bitcoin, the greatest challenge may be linking Bitcoin addresses to a real person. Investigators may not be able to identify a person behind the crime despite the public transaction ledger revealing the address to which the virtual currency was sent. The best avenue for identifying the offender is by associating the address with information available outside the transaction ledger. FinCEN-registered exchangers are required to validate the identities of their customers. Additionally, some Bitcoin users post their Bitcoin addresses online, along with information that may reveal their true identities. If criminals have been identified by traditional investigative means as a result of other criminal activities, they voluntarily may disclose their Bitcoin addresses while cooperating.

VIRTUAL CURRENCY SEIZURE

Seizing bitcoin will require law enforcement officers to take hold of or otherwise gain lawful access to the electronic media where the wallet resides (e.g., on a laptop, thumb drive, or server). The Bitcoin address also may be recorded as printed "QR" codes or strings of letters and numbers, known as a paper wallet.22 The bitcoin immediately should be transferred to a government-controlled wallet, and the media holding the wallet should be segregated and stored without connection to the Internet. Merely seizing the wallet and storing it as evidence is insufficient because backup wallets may exist online or in another location. If the bitcoin are not moved to a government-controlled wallet, they may be transferred by a third party using a backup wallet; in that case, the original seized wallet no longer will hold any value. If a third-party business holds bitcoin in an e-wallet, investigators must serve process on the business just as one would serve a seizure warrant on a financial institution for funds in an account.

Prosecutors may forfeit bitcoin through existing asset forfeiture laws as proceeds of criminal activity or as property involved in money-laundering violations. Under federal law assets may be forfeited as proceeds of a specified unlawful activity—defined in Title 18, Section 1956, Subsection C, Paragraph 7, U.S. Code—pursuant to Title 18, Section 981, Subsection A, Paragraph 1, Subparagraph C, U.S. Code or as property involved in money laundering pursuant to Title 18, Section 981, Subsection A, Paragraph 1, Subparagraph A, U.S. Code, or Section 982, Subsection A, Paragraph 1, U.S. Code.23 Property involved in money laundering includes the money being laundered, any fees or commissions paid for laundering the money, and any property that facilitates the money laundering transaction.

Planning and coordination are important in any case concerning an unusual asset, such as virtual currency. Due to the volatile nature of virtual currency, prosecutors should consider obtaining a stipulation for interlocutory sale where possible, which will permit the sale of the virtual currency prior to completion of the forfeiture.24 In the event law enforcement officers seize a large quantity of virtual currency, prosecutors should consider breaking it up into smaller batches for sale after forfeiture or an order for interlocutory sale. Investigators may seek their local FBI field office for assistance in these matters.

CONCLUSION

The use of virtual currency by both law abiding citizens and criminals likely will continue to expand in the future. Though the use of virtual currency poses some challenges to law enforcement, these difficulties are not insurmountable. Investigators still will succeed in combating crimes that involve virtual currency by using traditional investigative techniques, adapted as necessary to address modern criminal capabilities. Law enforcement should seek to follow the money in any investigation regardless of how that value is held.

Endnotes

1 Bitcoin is capitalized when referring to the network or system and lowercased when referring to units of the virtual currency.

2 U.S. Attorney's Office, Southern District of New York, Manhattan U.S. Attorney Announces The Indictment Of Ross Ulbricht, The Creator And Owner Of The "Silk Road" Website (U.S.

Department of Justice, February 4, 2014), accessed February 12, 2015, http://www.justice.gov/usao/nys/pressreleases/February14/RossUlbrichtIndictmentPR.php.

3 U.S. Department of the Treasury, Financial Crimes Enforcement Network, accessed August 18, 2015, http://www.fincen.gov/; and Financial Crimes Enforcement Network, FinCEN's Mandate from Congress (U.S. Department of the Treasury), accessed August 18, 2015, http://www.fincen.gov/statutes_regs/bsa/.

4 U.S. Department of Justice, Acting Assistant Attorney General Mythili Raman Testifies Before the Senate Committee on Homeland Security and Governmental Affairs (Washington, DC, November 18, 2013), accessed February 12, 2015, http://www.justice.gov/criminal/pr/speeches/2013/crm-speech-131118.html.

5 12 U.S.C. § 1951 (2012).

6 U.S. Department of the Treasury, Remarks from Under Secretary of Terrorism and Financial Intelligence David S. Cohen on "Addressing the Illicit Finance Risks of Virtual Currency" (Washington, DC, March 18, 2014), accessed February 12, 2015, http://www.treasury.gov/press-center/press-releases/Pages/jl236.aspx; and 12 C.F.R. § 1005.20 (2012).

7 Financial Crimes Enforcement Network, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (U.S. Department of the Treasury, March 18, 2013), accessed February 12, 2015, http://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.

8 Financial Crimes Enforcement Network, Application of FinCEN's Regulations to Virtual Currency Mining Operations (U.S. Department of the Treasury, January 30, 2014), accessed February 12, 2015, http://www.fincen.gov/news_room/rp/rulings/html/FIN-2014-R001.html.

9 U.S. Securities and Exchange Commission, Investor Alert: Ponzi Schemes Using Virtual Currencies, SEC Pub. No. 153 (7/13), accessed February 12, 2015, http://www.sec.gov/investor/

alerts/ia_virtualcurrencies.pdf.

10 SEC v. Shavers, No. 4:13-CV-416, 2013 WL 4028182 (E.D. Tex. Aug. 6, 2013).

11 15 U.S.C. § 77a (2012).

12 Internal Revenue Service, Notice 2014-21, accessed February 13, 2015, http://www.irs.gov/pub/irs-drop/n-14-21.pdf.

13 Ibid.

14 Texas Department of Banking, Supervisory Memorandum –1037 (Austin, TX, April 3, 2014), accessed February 12, 2015, http://www.dob.texas.gov/public/uploads/files/consumer-