2015

Cryptocurrencies: An Introduction for Policy Makers

Brian Conley

Jeffrey Echert

Andrew Fuller

Heather Lewis

Charlotte Lunday

Cryptocurrencies

An Introduction for Policy Makers

Prepared by Brian Conley, Jeffrey Echert, Andrew Fuller, Heather Lewis and Charlotte Lunday on behalf of the University of Washington School of Law Technology Law and Public Policy Clinic

Acknowledgments

This paper was prepared for general education purposes by students in the University of Washington School of Law's Technology Law and Public Policy Clinic, under the guidance of Professor William Covington. The students would like to express thanks to Professor Covington for his direct assistance, as well as his efforts to connect us with industry experts. We would also like to thank the University of Washington School of Law, especially the Tech Policy Lab for allowing us to use its resources and facilities.

Table of Contents

Executive Summary

Cryptocurrencies are open-source, peer-to-peer digital currencies. Two of their most distinctive features include the use of public key cryptography to secure transactions and create additional currency units, as well as the decentralized nature of their digital payment systems.[1] The underlying technical system which all cryptocurrencies are modelled after is that of the original cryptocurrency, Bitcoin. Bitcoin was created by "Satoshi Nakamoto" a person or group credited with writing the first paper on the digital currency in 2008. Certain key elements differentiate cryptocurrencies from traditional electronic currency systems such as electronic banking and PayPal, most notably their decentralized control mechanisms.[2] That is, traditional methods involve a single entity recording, verifying, and ensuring transactions. With many cryptocurrencies, including Bitcoin, past transactions are recorded on a public ledger and verification of transactions is outsourced to users.

Bitcoin and other cryptocurrencies provide users many benefits, including ease of digital transactions, lower transaction costs, and enhanced privacy. However, these benefits come with concerns regarding consumer protection and fraud deterrence. Three pressure points persist*: the irretrievability problem* (the inability to call back a bitcoin once it has been transferred), *bitcoin mining malware*, and *exchange services*. Also problematic is the lack of uniformity from state-to-state regarding cryptocurrencies' (predominately Bitcoin's) categorization as either currency or property. Defining cryptocurrencies as currency facilitates its use as a method of exchange, while categorizing it as property may be easier for tax collection purposes.

Bitcoin's encrypted nature problematizes the digital currency as abandoned property. Traditionally, abandoned property reverts to the state after a statutorily set period of time. In instances of cash, gold, etc. this is fairly easy – ownership of the valuable goods transfers to the state after the statutory period. Generally, banks and financial institutions are required by state laws to retain a customer's property for a period of time, usually five years, before the property will escheat to the state. However, Bitcoin creates circumstances in which the value of the abandoned property is permanently lost rather than transferred to the state. Finally, a fear concerning Bitcoin and other digital currencies is the potential for use in criminal activity. The pseudonymous nature of the transactions, the ease with which funds can be transferred across geographical distances, and the inherent risk in the currency have fueled hesitation and fear. This paper defines cryptocurrencies, Bitcoin, and explains the processes and vulnerabilities facing Bitcoin user, as well as the currency's potential as a tool for criminal activity. Additionally, each section concludes with policy suggestions to help inform legislators and general audiences on the nature and Bitcoin, as well as provide insights into the digital currency's' general usage.

[1] Brito, J.; Castillo, A. (2013) Bitcoin A Primer for Policy Makers
http://mercatus.org/sites/default/files/Brito_BitcoinPrimer.pdf
[2] Ibid.

Introduction

What are Cryptocurrencies?

Cryptocurrencies are open-source, peer-to-peer digital currencies. Two of their most distinctive features include the use of public key cryptography to secure transactions and create additional currency units, as well as the decentralized nature of their digital payment systems.[3] [4] The dispersed nature of cryptocurrencies' payment systems sets them apart from other online payment systems such as online banking and PayPal, which both require a third party to act as an intermediary between payers and payees.[5] All past transactions are recorded in a public, online ledger.

Cryptocurrencies: A Brief History

The underlying technical system which all cryptocurrencies are modelled after is that of the original cryptocurrency, Bitcoin. Bitcoin was created by "Satoshi Nakamoto" a person or group credited with writing the first paper on the digital currency in 2008: *Bitcoin: A Peer-to-Peer Electronic Cash System*.[6] Bitcoin as a digital currency system was published as open-source software in 2009.[7] It is a peer-to-peer system, meaning that bitcoins can be transferred between users without requiring an intermediary.[8] Transactions are verified by network nodes – which broadcast information across the internet, and are then recorded in a public ledger known as the "block chain".[9] The Bitcoin system works without a central repository or single administrator, which has led institutions such as the US Treasury to classify it as a "virtual

[3] Brito, J.; Castillo, A. (2013) Bitcoin A Primer for Policy Makers http://mercatus.org/sites/default/files/Brito_BitcoinPrimer.pdf

[4] Greenberg, A. (2011, April 20). *Crypto Currency.* Retrieved from Forbes: http://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html

[5] Brito, J.; Castillo, A. (2013) Bitcoin A Primer for Policy Makers http://mercatus.org/sites/default/files/Brito_BitcoinPrimer.pdf

[6] Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Retrieved from Bitcoin.Org: https://bitcoin.org/bitcoin.pdf

[7] Davis, J. (2011, October 10). *The Crypto-Currency.* Retrieved from The New Yorker: http://www.newyorker.com/magazine/2011/10/10/the-crypto-currency

[8] Brito, J.; Castillo, A. (2013) Bitcoin A Primer for Policy Makers http://mercatus.org/sites/default/files/Brito_BitcoinPrimer.pdf

[9] A. Antonopoulos, What Is Bitcoin? (2014). In A. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurriences* (p. Chapter 6). O'Reilly.

currency", though a more accurate classification is that of a "digital currency". The Bitcoin ledger uses its own unit of account, called bitcoins.[10]

As of February 2014, there exist hundreds of cryptocurrencies, but Bitcoin remains the most popular.[11] Each system relies on a public ledger (much like Bitcoin's block chain) which is protected by parties of "miners" who remain mutually distrustful of one another.[12] Miners ensure that the ledger is up-to-date and accurate by continuously verifying and collecting newly occurring transactions, and by placing them into new "blocks" or groups of transactions.[13]

Miners were initially members of the general public who used their computers' processing power collectively to secure and timestamp transactions, then add them to the public ledger, in accordance with the cryptocurrency's time stamping system.[14] Bitcoin mining has since become so energy intensive, that ordinary computers do not have the processing power to carry out these tasks. Mining now requires highly specialized and expensive equipment.

Most cryptocurrencies model themselves after Bitcoin on the issue of gradual decreased production, placing a cap on the total number of units/amount of currency allowed to reach circulation. This mimics the scarcity principle and value which help prolong the value of precious metals and also discourages hyperinflation.[15] Existing digital currencies are predominately psuedononymous- which allows users to maintain a degree of anonymity.

ISSUES IN CONSUMER PROTECTION

Bitcoin and other cryptocurrencies provide users many benefits: ease of digital transactions, lower transaction costs, and enhanced privacy. These payment system innovations however also raise questions about consumer protection and fraud deterrence. Questions revolve around three pressure points, which include the "irretrievability problem" (the inability to call back a bitcoin once it's been transferred), bitcoin mining malware, and exchange services and wallet security. Several federal agencies and international governments have offered guidance

[10] Kopstein, J. (2013, December 12). *The Mission to Decentralize the Internet*. Retrieved from The New Yorker: http://www.newyorker.com/tech/elements/the-mission-to-decentralize-the-internet

[11] http://cryptocoincharts.info/

[12] Brito, J.; Castillo, A. (2013) Bitcoin A Primer for Policy Makers http://mercatus.org/sites/default/files/Brito_BitcoinPrimer.pdf

[13] Ibid.

[14] Ibid.

[15] Greenberg, A. (2011, April 20). *Crypto Currency.* Retrieved from Forbes: http://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html

for dealing with bitcoin; and three states—New York, Kansas, and Texas—have created some laws and regulations aimed at moving bitcoin into the mainstream economy securely. This section (1) examines the consumer protection problems bitcoin presents, (2) presents consumer protection policies promoted by various governing bodies, and (3) offers a recommendation for moving forward.

Bitcoin Vulnerabilities

Irretrievability Problem: By eliminating the charge back fraud problem, bitcoin places the burden of loss on buyers if a seller does not deliver a product as promised. Without protection of a governing body and enforcement of anti-fraud and anti-theft laws, the buyer has no recourse if the seller refuses to re-transfer bitcoin back to the buyer.

Mining Malware: Because bitcoin mining becomes increasingly more challenging over time, miners form collectives that pool their computing resources to uncover new bitcoin. This presents a lucrative opportunity for criminals and hackers. For instance, in November 2013, the New Jersey State Office of the Attorney General settled with an online gaming company for $1 million dollars for placing malware on its customers' computers.[16] E-Sports Entertainment, LLC infected 14,000 computers with bitcoin mining software that would mine undetected while the computer user was away.[17] E-sports' founders created wallets where the bitcoin were to be routed.[18] The founders then sold the bitcoin for cash and deposited the money in personal bank accounts.[19] E-Sports' actions are not unique, and use of mining malware is increasing.[20]

Hacking of Wallet and Bitcoin Exchanges:

In July of 2014, the Congressional Research Service issued a report on bitcoin in which they list some of the largest security breaches on the bitcoin network.[21] Among these were a hacking attack against bitcoin exchange Mt. Gox in 2013 that forced the exchange into bankruptcy, the theft of more than 35,000 bitcoins from hacking of web-based wallet provider Instawallet in April 2013 (a theft worth nearly $5 million at the time), and bitcoin "banks" that were either

[16] New Jersey Office of the Attorney General. (2013, November 19). *Acting Attorney General Announces $1 Million Settlement Resolving Consumer Fraud, Unlawful Access Claims Against ONline Gaming Company*. Retrieved from The State of New Jersey: http://nj.gov/oag/newsreleases13/pr20131119a.html).

[17] *Ibid.*

[18] *Ibid.*

[19] *Ibid.*

[20] *Third Quarter Threats Report Identifies Android Malware That Bypasses App Validation as Signed PC Malware Continues to Surge; Bitcoin Popular in Illicit Trade and Cybercrime*. (2013, November 20). Retrieved from McAfee: http://www.mcafee.com/us/about/news/2013/q4/20131120-01.aspx

[21] Craig K. Elwell, M. M. (2015, January 28). *Bitcoin: Questions, Answers, and Analysis of Legal Issues*. Retrieved from Congressional Research Service: http://fas.org/sgp/crs/misc/R43339.pdf

shut down or hacked, causing all bank users to lose all bitcoin stored in the banks.[22] Because wallets and other bitcoin financial services have no insurance requirements, the users bear the risk of loss. Furthermore, many users may be using these financial services or investing in bitcoin without full disclosure of the risks.[2324] Worse still, users may be persuaded in making investments with scammers.[25]

Attempts at Regulating Bitcoin for Consumer Protection

The following is a brief overview at regulatory schemes and proposed schemes for mitigating the consumer protection problems presented by bitcoin. This overview will include a brief discussion of international, federal, and state action, as well as scholarly proposals.

International Sources of Regulation

Some countries, like Russia and Bolivia, have chosen to ban cryptocurrencies rather than contemplate a legal scheme that could bring cryptocurrencies into the mainstream economy, while mitigating the risks such currencies pose.[26] Other countries, such as Belgium, have only gone so far as to warn users of the risks of fraud, price volatility, and other concerns.[27] Many countries are investigating cryptocurrencies and ways to bring them into the formal economy, if only for tax purposes.[28] The European Banking Authority (EBA), however, proposed both long- and short-term regulatory frameworks in August of 2014.[29]

The EBA identified several potential "risk drivers" and proposed ways of reducing those risks.[30] First, the EBA provides that relevant market participants be registered and authorized by a

[22] Ibid.

[23] *Risks to consumers posed by virtual currencies* . (2014, August). Retrieved from Consumer Financial Protection Bureau: http://files.consumerfinance.gov/f/201408_cfpb_consumer-advisory_virtual-currencies.pdf

Investor Alerts and Bulletins, U.S. SEC, Investor Alert: Bitcoin and Other Virtual Currency-Related Investments (May 7, 2014) (available at http://www.sec.gov/oiea/investor-alerts-bulletins/investoralertsia_bitcoin.html#.VHKkK1fF83Q.

[24] *Investor Alert: Bitcoin and other Virtual Currency- Related Investments* . (2014, May 7). Retrieved from U.S. Securities an Exchange Commission: http://www.sec.gov/oiea/investor-alerts-bulletins/investoralertsia_bitcoin.html#.VHKkK1fF83Q.

[25] SEC Investor Alert, *supra* n. 24.

[26] *Is Bitcoin Legal?* (2014, August 19). Retrieved from Coindesk: http://www.coindesk.com/information/is-bitcoin-legal/

[27] *Ibid.*

[28] *Ibid.*

[29] European Banking Authority Opinion on 'Virtual Currencies.' (2014, July 4). Retrieved from EBA.Europa.EU: https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf.

[30] *Ibid.* at 38.

government prior to marketing virtual currency services.[31] Governance authorities that ensure that market participants prove their competence, ethics, and financial soundness are to be established.[32] Furthermore, participants that hold virtual currency on behalf of others must separate their clients' virtual currencies from their own, and maintain a certain level of capital in a fiat currency with a fixed component and a variable component that increases with business volume.[33] Those engaged in a transaction should refund payers in the event of an unauthorized transaction, and any additional compensation required by applicable contract law.[34] The EBA also contemplates a proxy system in which a proxy holds funds until the merchant has fulfilled their end of the transaction, at which point, the proxy will deliver the buyers' funds to the seller.[35] Finally, the governance authorities would be required to provide certain information technology security guarantees.[36]

Federal Sources of Regulation

There are three primary sources of federal regulation regarding consumer protection issues inherent in cryptocurrencies: the Financial Crimes Enforcement Network (FinCEN), the Federal Trade Commission (FTC), and the Securities and Exchange Commission (SEC).

FinCEN guidance: Services that exchange a virtual currency for another currency, real or otherwise, or that act as an intermediary (where the intermediary accepts virtual currencies from a buyer, and gives the seller a different currency to facilitate the transaction between buyer and seller) are money transmitters.[37] As money transmitters, they are subject to FinCEN's recordkeeping, registration, and reporting requirements, and are potentially subject to similar state laws.[38] Such licenses can lend legitimacy to virtual currency businesses, but may not be favored by early bitcoin adopters that value de-regulation.

FTC: The FTC accepts complaints regarding any potential bitcoin scams. For example, using its authority to regulate unfair and deceptive trade practices, the FTC brought a lawsuit against Butterfly Laboratories, a company that deceptively marketed bitcoin mining software, charged consumers for a purchase of the software, and then failed to deliver the product or provide refunds to the buyers.[39] The court ordered Butterfly Laboratories to stop misrepresenting its products and services, and it placed a freeze on the company's assets while the court

[31] *Ibid.* at 41.
[32] *Ibid.*
[33] *Ibid.*
[34] *Ibid.* at 42.
[35] *Ibid.*
[36] *Ibid.* at 41.
[37] Financial Crime Enforcement Network Guidance on Virtual Currencies. (2013, March 18). Retrieved from FinCEN.gov: http://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.
[38] Ibid.
[39] FTC v. Butterfly Labs Inc., Case No. 4:14-CV-00815-BCW (2014, Dec. 12, W.D. Mo.).

deliberates whether Butterfly Laboratories committed fraud.[40] In similar future cases, cryptocurrencies may be inaccessible by the courts, but the Butterfly Laboratories case suggests that courts may place liens on other assets as a way to compensate victims of cryptocurrency scams.

SEC: The SEC has released investor alerts regarding bitcoins and has sent inquiries to hundreds of bitcoin businesses regarding the issuance of unregistered securities. In *SEC v. Shavers*, the Commission also prosecuted the perpetrator of a bitcoin Ponzi scheme.[41]

The SEC derived its authority from the broad definition of a security as "any note, stock, treasury stock, security future, security-based swap, bond . . . [or] investment contract . . ." 15 U.S.C. Section 77b.[42] "An investment contract is any contract transaction or scheme involving (1) an investment of money, (2) in a common enterprise, (3) with the expectation that profits will be derived from the efforts of the promoter or a third party."[43] Because Bitcoin could be used as money, the Bitcoin Savings and Trust (BST), a so-called bitcoin bank, was a common enterprise where the investors expected profits to be derived from perpetrator's efforts.[44] Thus, the court ruled that investment in BST was a security within the SEC's jurisdiction.[45] For this reason, the SEC will likely monitor investment schemes involving cryptocurrencies. Because these schemes fall within SEC jurisdiction, investment opportunities could be required to comply with SEC registration requirements.

State Sources

Three states—New York, Texas, and Kansas—have all attempted classification and regulation of bitcoin. New York proposed requiring businesses accepting bitcoin obtain special licenses, but is revising that proposal after receiving significant criticism.[46] Under Texas law, Bitcoin cannot be defined as currency because it is not backed by a government.[47] Therefore, in Texas, exchanges that operate similarly to an escrow may be considered money transmitters, but other cryptocurrency services, including bitcoin ATMs are not and are not subject to licensing

[40] Ibid.
[41] SEC v. Shavers, Case No. 4:13-CV-416 (2013, Aug. 6, E.D. Tex.).
[42] Ibid.
[43] Ibid.
[44] Ibid.
[45] Ibid.
[46] Tom Groenfeldt (2014, Dec. 18). *New York is Ready with Revision of Bitcoin Regulation*. Retrieved from Forbes.com: http://www.forbes.com/sites/tomgroenfeldt/2014/12/18/new-york-is-ready-with-revision-of-bitcoin-regulations/.
[47] Texas Department of Banking Supervisory Memorandum – 1037. (2014, Apr. 3). Retrieved from dob.texas.gov: http://www.dob.texas.gov/public/uploads/files/consumer-information/sm1037.pdf.

requirements as a result.[48] And in Kansas, many cryptocurrency services also do not qualify as money transmitters.[49]

Nevertheless, states may protect consumers in absence of robust regulatory and licensing schemes. The New Jersey Attorney General, for example, as described above, is monitoring and prosecuting malware attacks under existing law.

A Suggested Response

Although Bitcoin and other virtual currencies pose some risks, such as price volatility, that cannot yet be adequately addressed by legal means, other risks may be mitigated by existing regulatory strategies and enforcement mechanisms. First, as the FTC and SEC cases demonstrate, federal and state consumer protection and securities agencies may be able to enforce existing consumer protection and investing laws against those who offer Bitcoin services. Attorneys general can also seek justice for hacking, malware, and fraud on behalf of citizens. However, any regulatory attempts must involve careful consideration of how "money" and "money transmitters" are defined.

Secondly, exchanges, Bitcoin ATMs, and other cash-for-bitcoin services should be classified as money transmitters. This would subject them to licensing, registration, and record-keeping requirements. Consumers would be better protected because they would have legitimized services to exchange between bitcoin and government-backed currency rather than trading with an anonymous stranger.

Finally, virtual currency services that hold currency for users should be required to prove a sophisticated level of data security. Because bitcoin and other virtual currencies are decentralized and irretrievable, a compromised wallet or exchange results in the user's money being lost forever. Consumers should have peace of mind before entrusting their money to non-traditional financial services.

Taxation of Cryptocurrencies

The central issue for cryptocurrency taxation is how the tax authority chooses to define cryptocurrencies. Currently, tax authorities define cryptocurrencies either as currency or property. Defining cryptocurrencies as currency facilitates its use as a method of exchange, while defining cryptocurrencies as property and subjecting them to capital gains rates diminishes their capacity as a method of exchange, but may serve to put those who trade or would trade in cryptocurrencies on notice that they are a speculative commodity prone to

[48] Ibid.
[49] Regulatory Treatment of Virtual Currencies Under the Kansas Money Transmitter Act. (2014, June 6). Retrieved from osbckansas.org: http://www.osbckansas.org/mt/guidance/mt2014_01_virtual_currency.pdf

dramatic fluctuations in value, as well as allowing the tax authority to recover taxes on the profits earned by cryptocurrency owners.

Federal Treatment

In the United States, the IRS has designated cryptocurrencies as "convertible virtual currency." IRS Notice 2014-21. This definition is misleading, however, because the treatment is the same as in a property regime. Cryptocurrencies cannot generate foreign currency gains or losses; instead they are subject to capital gains treatment. *Id.* at Section 4. The full market value of the currency at the time of the acquisition must be recorded because using the cryptocurrency to purchase a good triggers a taxable event. *Id.* The result is mining a cryptocurrency is treated as receipt for the calculation of basis. *Id.* In the event that it is received as income by an independent contractor it is subject to the self-employment tax or, if by an employee, the employment tax. *Id.* The notice applies retroactively so that taxpayers who treated virtual currency transactions in a manner inconsistent with the notice prior to the notice date may be subject to penalties. *Id.* However, there is a potential reasonable cause excuse for failures to comply. *Id.*

State Treatment

With the uniform Federal approach presented by the IRS it may not be surprising that states have done little to address cryptocurrency taxation. For instance, when it comes to state income tax there is no current guidance from the states. However, given the IRS treatment is likely that state income taxes would apply in the same manner they do to earnings on securities.

Some states have provided guidance when it comes to their sales tax. For instance, Wisconsin, California and Kentucky have all stated that purchases of taxable goods or services made with cryptocurrencies are subject to state sales tax, determined via sales price computed in dollars. See, e.g., CA BOE Special Notice L382 (June 2014), Wisconsin DOR, Sales and Use Tax Report, Issue 114 (March 2014), Kentucky DOR, Sales Tax Facts (June 2014). However, Wisconsin and Missouri have stated that sales of a cryptocurrency itself (conversion into a fiat currency) are not subject to sales tax because a cryptocurrency is intangible, rather than tangible personal property. See, e.g., Wisconsin DOR Report (March 2014), Missouri DOR, Letter Ruling LR 74111 (September 2014). In Wisconsin, however, where the sale of a cryptocurrency is used merely as a proxy for the purchase of taxable goods sales tax will apply. The sales tax exemption is not uniform across states; for instance, Nebraska, in line with the IRS treatment of cryptocurrencies as property has stated that tax exempt treatment of traditional currency sales does not apply to cryptocurrencies. Nebraska DOR, Frequently Asked Questions About Currency and Bullion (April 2014).

The designation as property also complicates transactions from the side of the retailer. In California retailers must maintain sufficient records to verify taxable sales prices at the time of

transaction; evidence can be the standard sales price in US dollars. CAL BOE Special Notice L 382. Wisconsin has a similar rule, requiring taxable sales price to be based on the value of consideration, in dollars, received on the date of sale. Wisconsin DOR Report (March 2014). The same holds true in Kentucky, where retailers "must maintain documentation to verify the value of the [cryptocurrency] at the time of the transaction." Kentucky June 2014 Sales Tax Facts.

International Approaches to Treatment

International regimes differ drastically in their treatment of cryptocurrencies. Some countries have applied a similar regime to that employed by the federal government. Other countries, like Thailand, have gone so far as to make the buying and selling of cryptocurrencies illegal. Others have taken a more nuanced, hybrid approach.

Canada considers cryptocurrency a hybrid between traditional fiat currencies and property. According to the Canadian Tax Authority, the trading or sale of a cryptocurrency as a commodity results in capital gains rate treatment similar to any other security. CRA Document No. 20140052411E5, "Virtual Currencies (Bitcoins)" (March 2014). However, the use of cryptocurrencies in the purchase of goods or services is a "barter transaction." CRA Document No. 2013-0514701I7, "Bitcoins" (December 2013). Under this solution the business must report its income from the transaction in Canadian dollars on the full market value of the cryptocurrency at the time of sale. GST and/or HST apply to the full market value as determined. If one mines a cryptocurrency in a commercial manner income is determined with reference to the amount of cryptocurrency in inventory at the end of the year.

Germany treats cryptocurrencies similar to the United States. German law currently states that cryptocurrencies are a "unit of account" and subjects any profit on said unit of account to a short term capital gains tax of 25%, unless long term capital gains applies due to being held for more than a year. A pending EU ruling on cryptocurrencies may change this treatment in the future.

The United Kingdom has carefully outlined its treatment of cryptocurrencies, assessing how VAT, corporate, income and capital gains taxes apply. For the purposes of VAT, the UK asserts that income from cryptocurrencies is generally outside the scope of VAT as there is an insufficient link between any services provided and consideration received. Revenue and Customs Brief 9 (2014): Bitcoin and other Cryptocurrencies. Also, the income derived from mining a cryptocurrency is exempt from VAT treatment under Article 135(1)(d) of the EU VAT Directive. *Id.* When the cryptocurrency is exchanged for Sterling or for a foreign currency, there is no VAT due on the value on the cryptocurrency itself; additionally, charges made over and above the value of the cryptocurrency for arranging or carrying out any of those transactions are exempt from VAT under Article 135(1)(d). *Id.*

For the purposes of the corporate tax profits or losses on exchange movements between currencies are taxable and the general rules on foreign exchange and loan relationships apply

to virtual currencies, with exchange movements being determined between the company's functional currency and the other currency in question. *Id.* Subjecting cryptocurrencies to the foreign exchange regime is more supportive of using cryptocurrencies as mediums of exchange, at least for the purposes of business. When it comes to the profits and losses of a non-incorporated business on cryptocurrency transactions the income is taxable under the normal income tax rules.

The normal income tax rules for cryptocurrencies are the same as the United States. Where there are "gains or losses incurred on Bitcoin or other cryptocurrencies" they are "chargeable or allowable for capital gains treatment if they accrue to an individual." *Id.*

A Suggested Approach to Treatment

Cryptocurrencies are still untested either as methods of exchange or as investment. They are also prone to dramatic volatility, as the fluctuations in the value of Bitcoin in recent years dictates. It is thus appropriate for the tax authority to treat cryptocurrencies as speculative investments subject to capital gain treatment. This serves two functions: first, it allows the tax authority to assess capture any gains on fluctuations in valuation when the Bitcoin is used, either in a purchase or in a sale. Second, it puts prospective investors on notice of the volatility and speculative nature of the cryptocurrency. Of the various capital gains regimes cited above, the IRS treatment may have advantages over more nuanced international regimes by providing a simple calculus for cryptocurrency owners.

Cryptocurrencies as Abandoned Property

If cryptocurrencies are classified as property, then one might assume that they can be abandoned like traditional forms of property. Traditionally, ownership of abandoned property reverts to the state after a statutorily designated period of time. For instance, when a person passes away and leaves no heirs, banks and financial institutions are generally required by state laws to retain a customer's property for a period of time, usually five years, before the property will escheat to the state.1 Cryptocurrencies, however, complicate this system because they are encrypted and may only be accessed by key holders. Therefore, if a person does not divulge his or her key to another person, that person's abandoned cryptocurrencies will be inaccessible and their value permanently lost rather than transferred to the state.

> Unlike most valuable property, the value of held cryptocurrency units is not inherent. That is, the value is not in the mere possession of the currency data, but rather in the ability to transfer the ownership of that data within a peer-to-peer verification network.

It could be argued that cryptocurrencies are data saved on hardware somewhere-perhaps a server. If the state were to acquire the server holding abandoned cryptocurrency units, it could be said that the state has acquired those units. Nevertheless, the value would still be lost. This is because the cryptocurrency value is purely speculative; it is determined on a per-transaction basis and is dependent on the ability to transfer ownership of a cryptocurrency unit. In contrast, most property that can be abandoned, be it cash, jewelry, stock certificates, bonds, etc., have an inherent value. For example, a twenty- dollar bill has twenty dollars of value. Because cryptocurrency value is dependent on the ability to transact, unless a possessor is able to access the former user's key and enable transactions, the currency data is essentially valueless. Although each state has a different approach how they deal with abandoned property, cryptocurrencies present novel technological challenges to this practice that will be difficult for any state to navigate.

A Suggested Response

Given the difficulties described above, cryptocurrency users must take precautionary steps, such as entrusting their key to someone in the event of an accident, to enable successors and the state to possess the value of the cryptocurrency rather than useless data. Professor Anita Ramsastry from the University of Washington, for instance, once suggested people with digital assets should consider two things: being aware of the terms of service of internet services impose regarding data and property after death, and leaving information behind for a loved one to access and control networked information.[50] A cryptocurrency wallet, host, or exchange could claim cryptocurrency units upon a death in terms of use. Many other types of online services already do.[51] Furthermore, Professor Ramsastry noted that Facebook had an app that would allow users to send messages to others that would be received only after the user was deceased.[52] If technology allows, a system like that may be worthwhile for users of cryptocurrencies to pass value on to others.

Bitcoin and Criminal Behavior

Another major concern about Bitcoin and other virtual currencies is their potential for use in criminal activity. The pseudonymous nature of the transactions, the ease with which funds can be transferred across geographical distances, and the inherent risk in the currency have fueled hesitation and fear. Russia, for example, has expressed concerns about the potential for criminal activity and terrorism; the country has even gone so far as to block a number of Bitcoin-related websites, though it has yet to explicitly ban virtual currencies.[53] In the United States, the FBI has paid special attention to virtual currencies' potential for abuse.[54] The Department of Defense is also investigating Bitcoin (along with many other technologies), with a specific focus on potential for terrorism.[55] While virtual currencies as terrorism funding is currently still mostly a theoretical issue, issues of financing criminal activity are quite real.

Money-Laundering and Illegal Marketplaces

For many users, the elusiveness of virtual currencies is a feature, not a bug. The potential for money-laundering seems obvious – Bitcoin can be exchanged for multiple different national currencies, and many exchanges, like the defunct Mt. Gox, are not likely to ask many questions

[50] Ramsastry, Anita. (2012, April 17). *Facebook's If I Die App Should Remind Us That We Each Need a Digital Death Plan*. Retrieved from Justia.com: https://verdict.justia.com/2012/04/17/facebooks-if-i-die-app-should-remind-us-that-we-each-need-a-digital-death-plan.

[51] Ibid.

[52] Ibid.

[53] (Cooper, 2015)

[54] (Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity, 2012)

[55] (Southurst, 2014)

about the source of traded currency. The issue of money laundering and, by extension, the use of that laundered money for use in private black or gray markets is a concerning one.[56]

Perhaps the most high-profile case in the United States has been the trial of Ross Ulbricht, who allegedly founded and operated the anonymous online marketplace, Silk Road. Silk Road billed itself as a marketplace for illegal drugs.[57]5 Launched in 2011, Silk Road operated mostly outside jurisdictional bounds, though by mid-2013 a couple of users in Australia and New Zealand had been convicted on drugs charges.

Arrested in October of 2013, Ulbricht was indicted on a number of counts, including six attempted murder charges stemming from him supposedly spending hundreds of thousands of dollars to have six people killed (though ultimately he was not prosecuted for those charges).[58] Ulbricht was convicted in February, 2015, on charges of money laundering, narcotics-trafficking, computer hacking, and engaging in a continual criminal enterprise.[59] The conviction was victory for the FBI, who also seized millions in Bitcoin from Ulbricht.[60]The message was clear: if you engage in criminal activity using virtual currency, you'll be treated no differently than if you use non-virtual currency.

Ulbricht's case may be the most visible one, but it's not the only one. While Bitcoin cases are in short supply currently, United States courts generally treat them the same as non-virtual currencies for the purposes of securities regulation and money laundering. A Texas court considered Bitcoin to qualify as a currency for use in an investment contract, thereby fitting within the definition of "security" in a suit alleging securities fraud.[61] And in a New York money-laundering case against defendants nominally associated with Silk Road, the United States District Court for the Southern District of New York found that, under plain meaning principles, Bitcoin qualifies as "money" or "funds."[62] While criminals may believe that they are being

[56] Bryans, D. (2014). Bitcoin and Money Laundering: Mining for an Effective Solution. *Indiana Law Journal , Vol. 89:441* , pp. 441-472.

[57] Chen, A. (2011, June 1). *The Underground Website Where You Can Buy Any Drug Imaginable.* Retrieved from Gawker: http://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160

[58] Mac, R. (2013, October 2). *Who Is Ross Ulbricht? Piecing Together The Life Of The Alleged Libertarian Mastermind Behind Silk Road.* Retrieved from Forbes: http://www.forbes.com/sites/ryanmac/2013/10/02/who-is-ross-ulbricht-piecing-together-the-life-of-the-alleged-libertarian-mastermind-behind-silk-road/

[59] Mullin, J. (2015, February 4). *Ulbricht guilty in Silk Road online drug-trafficking trial.* Retrieved from Ars Technica: http://arstechnica.com/tech-policy/2015/02/ulbricht-guilty-in-silk-road-online-drug-trafficking-trial/

[60] Greenberg, A. (2013, October 25). *FBI Says It's Seized $28.5 Million In Bitcoins From Ross Ulbricht, Alleged Owner Of Silk Road.* Retrieved from Forbes: http://www.forbes.com/sites/andygreenberg/2013/10/25/fbi-says-its-seized-20-million-in-bitcoins-from-ross-ulbricht-alleged-owner-of-silk-road/

[61] U.S. v. Faiella, 39 F.Supp.3d 544, 545 (S.D.N.Y. 2014).
[62] U.S. v. Faiella, 39 F.Supp.3d 544, 545 (S.D.N.Y. 2014).

creative by using Bitcoin, U.S. courts don't feel that the virtual vehicle doesn't require any special treatment.

Bitcoin's Potential for Terrorism?

In the United States, the FBI has paid special attention to virtual currencies' potential for abuse. In 2012, the agency released a preliminary report, outlining the reasons why it felt that Bitcoin could easily become a major source of funding for terrorist organizations.12 But the FBI also noted that Bitcoins, by themselves, are not anonymous – if Bitcoin users do not take additional steps to protect their identities, the IP addresses associated with the transactions are visible, and traceable.13 The FBI concluded that Bitcoin, if stabilized, would be an "increasingly useful tool" for illegal activity, including terrorism.14 However, the Department of the Treasury, conducting its own study, came up with a different conclusion: that the Bitcoin market was too volatile and the use of bitcoins too limited for terrorists, who generally prefer "real" currency for things like bribes and travel.[63]

The FBI may be closer to the mark, at least going forward. Technological advances such as DarkWallet (a Bitcoin wallet that encrypts and mingles together various Bitcoin transactions) may make Bitcoin transactions more anonymous and difficult to trace.[64] The program has been called "money-laundering software" by one of its own creators, Cody Wilson, who also expressed a desire to facilitate private, black market transactions.[65] And in 2014, a blog supposedly linked to ISIS proposed adopting Bitcoin as a method for financing terrorism, explicitly mentioning DarkWallet.[66] As marketplaces expand and bitcoins become a more commonly-accepted currency, terrorist organizations may increasingly turn to it as an anonymous source of funding. While it remains to be seen whether or not it will be adopted on a wide scale, it is clear that the technology poses some serious risks.

Bitcoin and other virtual currencies have the potential to be used to fund all manner of activities, legal or not. In that respect, they are much the same as standard, "real" currencies. If virtual currencies stabilize in value, and as anonymizing technologies become stronger, they will become more attractive to criminals and terrorists. But in many respects, they are not special, and not new. Courts and law enforcement agencies have not been stymied by virtual

[63] *Remarks From Under Secretary of Terrorism and Financial Intelligence David S. Cohen on "Addressing the Illicit Finance Risks of Virtual Currency".* (2014, March 18). Retrieved from U.S. Department of Treasury: http://www.treasury.gov/press-center/press-releases/Pages/jl236.aspx

[64] Greenberg, A. (2014, April 29). *'Dark Wallet' Is About to Make Bitcoin Money Laundering Easier Than Ever.* Retrieved from Wired: http://www.wired.com/2014/04/dark-wallet/

[65] Ibid.

[66] Higgins, S. (2014, July 7). *ISIS-Linked Blog: Bitcoin Can Fund Terrorist Movements Worldwide.* Retrieved from CoinDesk: http://www.coindesk.com/isis-bitcoin-donations-fund-jihadist-movements/

currencies; the FBI seized Ulbricht's Bitcoins much as it would have seized a pile of cash. While the technologies may change, even drastically.

Conclusion

Bitcoin is a trail blazer in the digital currency space. Bitcoin offers users pseudonymity, significantly reduced transaction fees, and removes intermediaries which hinder efficiency in other payment systems. Bitcoin transactions are verified through the decentralized block chain by miners who continuously update the Bitcoin public ledger. However, included with these selling features are potential risks to consumers, including the irretrievably problem, issues with abandoned property retrieval, and the potential for Bitcoin and other cryptocurrencies to be used for illegal purposes. Our final recommendation is that policy makers interested in learning more about Bitcoin and cryptocurrencies generally read our recommendations at the end of each section, and that national uniformity be prioritized in any future legislation that attempts to regulate cryptocurrencies.