LEGAL CONSIDERATIONS OF CRYPTOCURRENCY IN DIVORCE, MONEY LAUNDERING, AND TAX EVASION

Shaelyn Comiskey, University of North Georgia

Bryson R. Payne, University of North Georgia

Victor C. Parker, University of North Georgia

ABSTRACT

There are relatively few current academic resources related to the evolving issues regarding the use of cryptocurrencies to divide or hide marital assets in divorce cases, as well as for the purposes of tax evasion and money laundering. Cryptocurrencies are decentralized digital currencies that do not require transactional approval by a third party like a bank. Instead, users are assigned a random, encrypted pseudonym that allows them to store and trade currency for goods and services in an anonymous and unregulated manner. Since the introduction of the first cryptocurrency, Bitcoin, in 2009, cryptocurrencies have revolutionized online payment processing, but they have also provided a new medium for hiding assets. Hiding funds via Bitcoin and related cryptocurrencies has captured the international attention of divorce lawyers, digital forensic experts, governmental tax agencies, and law enforcement bodies including the FBI. The constantly fluctuating value, anonymity, and rapid transfer of bitcoins and other virtual currencies have posed significant problems for law enforcement as well as courts and regulatory agencies. Because the use of cryptocurrencies is a comparatively new way to finance crime, fund illicit activities, and hide assets from spouses and governments, the rules and regulations governing the use of cryptocurrencies have struggled to keep pace with the technology. The purpose of this research is to assemble and review existing literature, along with relevant, up-to-date case law related to these emerging topics in the use of cryptocurrency.

Keywords: Cryptocurrency, Bitcoin, Money Laundering, Divorce, Tax Evasion, Regulation

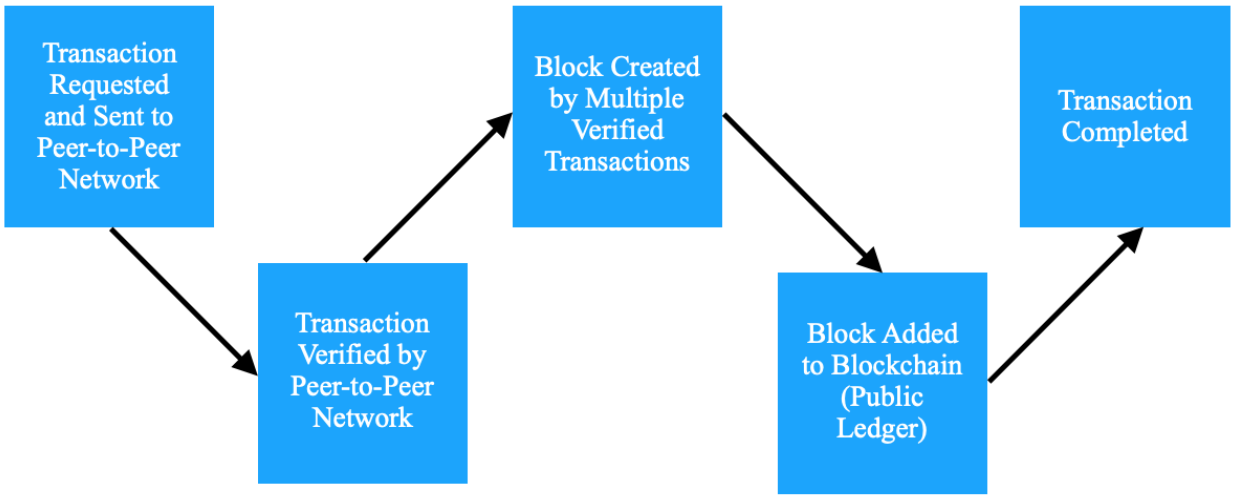
INTRODUCTION

In 2008, the revolutionary paper, "Bitcoin: A Peer-to-Peer Electronic Cash System," was published by Satoshi Nakamoto, whose identity remains unknown and could represent an individual or a group. Nakamoto (2008) proposed a system of electronic cash in which an individual can directly send payments to another person without the use of a centralized, trusted third party like a financial institution. Examples of trusted service providers include various online vendors who send confirmations of payment and receipt. Because of the prevalence of online communication and transactions, people trust and depend on third parties for security and privacy of digital assets (Crosby, Nachiappan, Pattanayak, Verma, & Kalyanaraman, 2016). However, due to potential hacking, third parties themselves are not necessarily secure.

In order to create a currency system that eliminates the need for trust, Nakamoto's electronic payment system relies on cryptographic proof (Nakamoto, 2008). The proof derives from cryptography, which is the science of making and breaking codes. Following the publication of "Bitcoin: A Peer-to-Peer Electronic Cash System," the concept of cryptocurrency was brought to life when Nakamoto mined the first Genesis Block, which contained 50 coins, in the Bitcoin blockchain in 2009 ("Genesis Block," 2018). Today, hundreds of other cryptocurrencies, including Ethereum, Ripple, Litecoin, and Monero, exist (K.A. Smith, 2018). Although this paper primarily focuses on Bitcoin, the concepts discussed generally apply to other forms of cryptocurrency.

Cryptocurrencies cannot exist without the concept of the blockchain. A blockchain is a database that permanently stores every transaction and digital event that takes place between involved parties (Crosby et al., 2016). Blockchain technology was originally created for Bitcoin to store digital transactions, but it is no longer specific to cryptocurrency. Lawyers utilize blockchain technology to record deeds, while banks and other financial institutions express interest in blockchain technology for the purpose of storing financial transactions and records. In terms of cryptocurrency, the blockchain is often referred to as a public ledger. The ledger uses a peer-to-peer system to maintain records of where individual pieces of bitcoin are stored. Thus, the entire network of peers, identified only by their usernames, can see every transaction that has been confirmed by miners. A graphic outlining this verification process is given in Figure 1.

Figure 1. A brief depiction of how blockchain technology works



According to West and Kainen (2018), there are three steps to any transaction: the input, the output, and the amount of currency exchanged. The input consists of a user's private address, and the output consists of the public address of the money's projected location. For cryptocurrency transactions, miners can confirm more than one input and output. To add a block to the blockchain, miners use computers to solve an algorithm that authenticates the transaction ("What is cryptocurrency," 2018). Thus, mining is the process by which individuals or companies provide their computer power "to verify and record payments into the public ledger" (Jafari, Vo-Huu, Jabiyev, Mera, & Farkhani, 2018, pg.2). The process requires "specialized hardware that has a

certain amount of computational power, measured in hashes per second" (Jafari et al., p. 2). Miners are rewarded for their work and resources with bitcoin payments. As the quantity of miners attempting to solve the algorithm increases, the algorithm becomes more complex, and "the odds of the average miner getting the reward decrease" (Slattery, 2018, p. 839). Additionally, a fixed amount of bitcoins circulates within the system, so mining is the only way new bitcoins are released (Brown, 2016).

There is considerable debate as to whether the reward is profitable due to the offset costs of heat and electricity for the mining hardware. Unfortunately, this constraint has spawned a collateral illegal enterprise, cryptocurrency-mining malware, in which malicious software infects victim computers and uses their processing power to mine cryptocurrency on behalf of the attacker. In one such case, up to 50,000 servers were infected with a crypto-miner virus over the course of two months in a coordinated attack dubbed the Nansh0u campaign (Harpaz and Goldberg, 2019).

Cryptocurrency transactions on the blockchain are possible because of the peer-to-peer network previously mentioned. The idea behind this network is that centralized authorities do not approve transactions. In contrast to standard financial systems, the decentralized Bitcoin network contains no single authority, so every user has access to a list of every transaction. The problem of double-spending ceases to exist within cryptocurrencies because members of the network hold each other accountable and "check if future transactions are valid or an attempt to double spend" ("What is cryptocurrency," 2018). Network users make pseudo-anonymous transactions using a randomly assigned public address that typically consists of a string of around 30 characters ("What is cryptocurrency," 2018). Users can analyze other anonymous transactions; however, the transactions and usernames cannot be traced back to someone's real identity.

Besides anonymity and decentralization, Bitcoin attracts users because of desirable properties like security and speedy, global transactions. In contrast to traditional bank accounts that can contain "pending" transactions for hours or even days, confirmation of crypto-transactions takes minutes or even seconds. Additionally, cryptocurrency transactions can occur anywhere in the world—as long as both users have access to a computer or phone and internet. Because the creation of a Bitcoin account requires no approval from a financial institution, anyone can set up an account in any location at any time. Users with reservations of traditional banks are attracted to the ease and unregulated manner of Bitcoin. Finally, according to blockgeeks.com (2018), "cryptocurrency funds are locked in a public key cryptography system [and] only the owner of the private key can send cryptocurrency." Thus, Bitcoin offers an additional layer of security.

The volatility of bitcoin's value stems from the supply and demand of the 21 million bitcoins in regulation (Brown, 2016, p. 332). Every time a miner provides his or her services, he or she is paid in an increasingly small, fractional portion of a coin due to the fixed number of coins circulating the system. However, just like investments with fiat currencies, there is potential for economic profit if the purchaser buys the cryptocurrency at a low price and later sells it for a higher price. For example, the steady trading and mining of bitcoin caused the price to rise from $2,000 to almost $20,000 in 2017 (Sharma, 2017). Just like with the Stock Market, users should expect a crash after a substantial increase in value.

Buying and Cashing Out Bitcoin

Compared to the complexity of the science behind cryptocurrency, the processes of buying, selling, and cashing out bitcoin are relatively simple and straightforward. Numerous companies have digital wallets through which the purchaser is directly connected to the Bitcoin exchange. Of these exchange companies, Coinbase is popular within the crypto-community due to its convenience and phone app (Fiorillo, 2018). Once the purchaser owns a wallet, which consists of the public and private key, he connects a credit or debit card to fund purchases. Since third parties operate the credit and debit cards that enable bitcoin purchases, the crypto-transactions will also appear on monthly credit and debit card statements. If a purchaser wishes to exchange bitcoins for cash, he can utilize worldwide bitcoin ATMs or websites like LocalBitcoin that facilitate in-person cash exchanges (Fiorillo, 2018). Using fake emails or a false identity when submitting requested information on LocalBitcoin and purchasing prepaid credit cards at stores help users remain completely anonymous. If purchasers, especially those with criminal intentions, wish to go one step further to conceal their identities when buying bitcoins, they can buy an untraceable burner phone with a prepaid SIM card and use the phone's number to validate an alias email address (Brown, 2016, p. 333).

Some people choose to keep their investments in the Bitcoin exchange, while others wish to exchange the cryptocurrency for real money. Cashing out bitcoins occurs via a third-party broker exchange or an in-person interaction. For third party broker exchanges, the owner requests a fiat currency withdrawal, typically via a bank or wire transfer, after the exchange receives the bitcoin (King, 2018). Websites like LocalBitcoin let people buy and sell bitcoin. LocalBitcoin allows flexible payment methods, but sellers typically prefer cash deposits, bank transfers, or meeting in person (King, 2018). Anonymously cashing out bitcoin can also take place by purchasing gift cards or physical goods from select retailers and then selling the gift cards or items for government-issued money (David, 2018). For example, a user can purchase an expensive item from Amazon with bitcoins and turn around and sell the item for cash.

DIVORCE

Divorce is messy, time-consuming, and emotionally tolling for both parties. Depending on the state in which the divorce is filed and the circumstances of the particular case, the full process can take several months or even years. During the early stages of divorce, the discovery process begins. The purpose of discovery is for each party to exchange financial and personal information to determine the most appropriate and fair way of dividing property and to determine spousal and child support ("Exchange of documents," n.d.). According to O.C.G.A. §9-11-26 (2010), discovery can occur informally or via depositions upon oral exam or written questions, written interrogatories, production of documents, physical and mental exams, and requests for admission. "Parties may obtain discovery regarding any matter, not privileged, which is relevant to the subject matter involved in the pending action, whether it relates to the claim or defense of the party seeking discovery or to the claim or defense of any other party, including the existence, description, nature, custody, condition, and location of any books, documents, or other tangible things and the identity and location of persons having knowledge of any discoverable matter" (O.C.G.A. §9-11-26(b)(1)). It is essential for each party to disclose his or her properties and assets during the discovery stage.

Each state has its own statute regarding how assets are divided during divorce. If spouses cannot agree on how to divide their property, the court falls back on the concepts of community property and equitable distribution (Stim, 2018). In the nine existing states that utilize community property, each spouse gets to keep his or her individual property, and the community property, which is owned by both spouses, is generally divided equally (Stim, 2018). Other community property jurisdictions, "using various terms, call for equitable distribution of the community assets" (Ratner, 2011, p. 21). The remaining states utilize equitable distribution in which property is divided fairly but not necessarily equally. When contemplating how to divide the property fairly, courts examine a number of factors including, but not limited to, the value of each spouse's separate property, future financial needs of each spouse, and the ages and health of each spouse ("Equitable distribution," 2018).

Issues arise when one spouse wants to keep a particular asset after the divorce and the other spouse disagrees. He or she may take part in illicit behaviors to impede the court from dividing such assets (Hou, 2015, p. 82). There are multiple methods in which divorcing spouses attempt to hide assets. Spouses can "transfer funds to family or friends, . . . falsify documents to make the record appear as though he or she has already sold the asset" (Hou, 2015, p. 82), invest in company holdings, or, in extreme cases, transfer money to offshore accounts. No matter how the spouse chooses to hide assets, the action is immoral (and even illegal in some jurisdictions) and can ultimately lead to significant punishment. One example of this is the Canadian case where a husband went to jail instead of paying $10 million to his ex-wife (Humphreys, 2017). A much more severe case involved a Philadelphia man who served 14 years in jail for contempt of court rather than pay his ex-wife money the court ordered him to pay (Avila & Ruppel, 2009).

Cryptocurrency Complications in Divorce

Since the introduction of Bitcoin, family lawyers who deal with divorce have seen a rise in cases involving cryptocurrencies. In divorce cases, cryptocurrencies are similar to any other type of property or asset. Therefore, ownership of cryptocurrencies should be revealed during discovery. The involvement of cryptocurrencies in divorce cases is changing the way in which lawyers currently conduct their cases. For example, New York divorce lawyer David Centeno (2017) explains that "in contested divorces, we now go through emails and hard drives more than we examine actual hard copies of the mail." Complications with cryptocurrency in divorce cases suggest one of two problems. The first problem addresses spouses attempting to hide marital assets in Bitcoin accounts. The second problem addresses how to value and divide any cryptocurrency that was disclosed in discovery.

Spouses investing in Bitcoin for the purpose of hiding assets appear to be less prevalent than spouses who simply disagree on how to divide Bitcoin holdings. Peter Walzer of the American Academy of Matrimonial Lawyers expresses that cryptocurrencies are a desirable alternative for hiding assets because of their supposed privacy and anonymity (as cited in Bloomberg, 2017). Interestingly, it has been suggested by Kieran Smith (2018b) that most Bitcoin holders are males under the age of 30, which just so happens to be similar to the age of the average divorcing couple in America. Furthermore, it is the husband who generally owns the cryptocurrency (Smith, 2018b). Ed Kainen, a divorce attorney in Florida, explains that investing in cryptocurrencies is "definitely more prevalent among younger folks because of the way they do business . . . [due to] a

generational difference" (E. Kainen, personal communication, October 2, 2018). Males may hide assets in Bitcoin because of the large potential for financial growth. For example, Vananda Chitroda, a partner at Royds Withy King in England, has a high-profile case in which the divorcing spouse's original investment of £80,000 in November 2016 was valued at £1 million in December 2017 (Peachey, 2018). The volatility of cryptocurrency can either be beneficial or catastrophic depending on the circumstances.

In order to discover hidden assets in divorce, the other party must first have a hunch that his or her spouse is concealing funds. Two ways of storing bitcoin exist. The first is by the use of an E-Wallet, which is the app that contains the account and the account's transactional history. The other way is via an offline "Cold Storage" method in which a jump drive or personal word file stores the number or identity used to access the account (E. Kainen, personal communication, October 2, 2018). In Cold Storage cases, the opposing spouse has no way to access the private address, which is essential to discover crypto-information. According to Richard West, account information stored on a jump drive is "virtually untraceable" (West & Kainen, 2018). If this is the case, forensic accountants can investigate the matter through a timely and costly process.

The more desirable case would be for the spouse to have an app like Coinbase, which stores purchased bitcoins along with transactional information. Bitcoins are typically purchased from the Coinbase app using a credit card or a bank transfer. At this point, lawyers can analyze the opposing party's bank statements that may be required in discovery. The complication arises when spouses have separate, private bank accounts. If lawyers or investigators find withdrawals for Bitcoin or large sum transfers, and the bitcoins were not clearly identified in the discovery process, it is inferred that the spouse attempted to hide assets. Divorce attorney David Badanes predicts that a divorcing spouse often attempts to hide assets in cryptocurrency to avoid paying alimony (as cited in "Men's rights activists," 2017). However, if the hidden assets are discovered after the divorce, the spouse can go back to court where alimony and child support are typically reassigned (McAfee, 2017).

As technology advances, the situation of hiding assets with cryptocurrencies will likely only get worse. This is why it is important for both spouses to be honest and for divorce lawyers to be thorough during initial discoveries. It is essential for state statutes to "add standard interrogatories and requests for production with the right language aimed at obtaining information and documentation regarding the opposing party's potential cryptocurrencies" (Wright, 2018). Until then, divorce attorneys must be "diligent" (Hochberg, 2018) when asking questions regarding bitcoins and the associated transactions and values.

The greater, more prevalent issue revolving around cryptocurrency and divorce is determining how to divide the cryptocurrency when both parties are aware of the virtual currency's existence. Because of the constantly fluctuating value of bitcoin, agreeing on how to split the assets can create difficulties. During a divorce, cryptocurrencies can be valued and split in one of many ways (E. Kainen, personal communication, October 2, 2018). Divorcing couples can choose to split the value at a certain point in time, split the cryptocurrency in-kind (each party takes half), split the initial investment value, or declare a bad-faith investment (E. Kainen, personal communication, October 2, 2018). Kainen has personally dealt with cryptocurrency issues in divorce at his practice, and he states that the easiest way to split cryptocurrency is "to give the party who is not engaging

in misconduct the option of how to do it" (E. Kainen, personal communication, October 2, 2018). If parties choose to split the bitcoin in-kind, one party may still have to pay an equalization payment to the other (Wright, 2018). Nonetheless, each party must come to an agreement on the division of bitcoin before the divorce can proceed.

Cryptocurrency issues in divorce are relatively new, so many of the cases are currently in court. Therefore, there is not a significant amount of available data regarding the topic. Until more laws regarding the specificities of bitcoin in divorce are enacted and enforced, the problem will continue to prevail.

MONEY LAUNDERING

Introduction to Money Laundering

According to Jason Bloomberg (2017), tax evasion, money laundering, contraband transactions, and extortion are sectors of criminal activity that readily benefit from cryptocurrencies. The characteristics of cryptocurrencies that appeal to the average investor, including anonymity, rapidity, and lack of regulation, are concurrently the same characteristics that attract criminals. For example, cryptocurrency technology can be advantageous by easing the process of international purchases, but perpetrators can just as easily commit illegal cybercrimes including blackmail, fraud, dark-web purchases, and money laundering (Heaven, 2018).

By definition, money laundering is a "financial transaction scheme that aims to conceal the identity, sources and destination of illicitly-obtained money" ("Money laundering," n.d. a). The process of money laundering consists of three stages: placement, layering, and integration ("Money laundering: A three-stage process," 2017). As its name suggests, the placement stage is when the laundered money first enters the economy. The purposes of placement are to diminish the criminal's physical possession of large amounts of cash and to place the money into the "legitimate financial system" ("Money laundering: A three-stage process," 2017). In order for so-called "dirty" money to enter an economic network, criminals turn to institutions like banks and casinos that readily deal with cash. During the layering stage, various secondary transactions occur throughout multiple locations in order to further disguise the money trail (Burke, 2018). As more transactions take place, the laundered funds become further separated and dissociated from their origins. Finally, during integration, the money is reincorporated into society and disguised as lawful funds that are consequently used to pay employees' salaries, support business ventures, and purchase expensive goods, services, and properties (Burke, 2018).

Traditional Beneficiaries of Money Laundering

Drug traffickers, embezzlers, and terrorists are among the criminals who most commonly engage in activities that require money laundering to conceal the crimes (Layton & Curran, n.d). Because significant bulks of cash or large sum transfers have a high potential to attract law enforcement agencies (Layton & Curran, n.d.), money launderers traditionally attempt to mask their illicit transactions by funneling the cash into multiple, seemingly legitimate businesses and accounts. The original dirty money then appears cleansed after going through various transactions and being deposited. Popular money laundering techniques include smuggling cash into other countries and

accounts, structuring by making smaller purchases, trading to alter invoices, and operating cash-intensive businesses and shell companies to disguise the launderer ("Money laundering," n.d. b). Furthermore, bank captures help relieve stress on money launderers who own banks, real estate allows for buying property with dirty money and selling it for legitimate money, and, finally, casinos help claim illicitly gambled money as winnings ("Money laundering," n.d. b).

Prevention of Money Laundering

In order to combat the international money laundering dilemma, many governments have developed anti-money laundering (AML) efforts that financial institutions must abide by. AML laws consist of confirming the legitimacy of large transactions and reporting any suspicious transfers of funds. In the United States, the Bank Secrecy Act of 1970, the Money Laundering Control Act of 1986, and the Patriot Act are among core AML efforts ("Money laundering," n.d. b). "The Currency and Foreign Transactions Reporting Act of 1970 (the legislative framework commonly referred to as the "Bank Secrecy Act" or "BSA") requires U.S. financial institutions to assist U.S. government agencies to detect and prevent money laundering. Specifically, the act requires financial institutions to keep records of cash purchases of negotiable instruments, to file reports of cash transactions exceeding $10,000 (daily aggregate amount), and to report suspicious activity that might signify money laundering, tax evasion, or other criminal activities" (Financial Crimes Enforcement Network). Further, the Money Laundering Control Act of 1986 declares money laundering to be a federal crime ("Money laundering," n.d. a). If money laundering occurs, certain banks have developed watch lists to monitor the transactions of clients who have been flagged as suspicious in the past (Burke, 2018).

Additionally, organizations such as the Financial Action Task Force, or FATF, unite to help countries prevent money laundering on an international level. The primary goal of the FATF is to create a standard by which its 33 members can unite to uniformly combat international money laundering and the financing of terrorism ("Anti-money laundering," n.d.). In each country that is a member, the FATF analyzes money laundering techniques, identifies money laundering patterns, and encourages further AML efforts ("Anti-money laundering," n.d.). According to Edgar Sánchez (2017), the most significant penalties for money laundering range from the greater of a fine of $500,000 or twice the value of the property that fulfilled the transaction, up to twenty years in prison, or a combination of both.

Cryptocurrency Complications in Money Laundering

Although the behaviors of criminals remain largely unchanged, the methodology behind committing crimes adapts to the evolving technology. Anonymity, rapidity, and lack of regulation of cryptocurrencies attract money launderers. Cryptocurrency exchanges often offer low exchange rates and can "act as a substitute for bank accounts in countries with immature financial systems" (Brenig, Accorsi, & Müller, 2015, p. 2). Cash helps money launderers disguise their transaction trails and thus conceal their identities; however, Bitcoin's random, untraceable pseudonyms take anonymous money laundering to a new level.

According to a recent Bloomberg Businessweek article, bitcoin ATMs (BTMs) are increasingly being used to launder money (Bloomberg Businessweek, 2018). According to Bloomberg, there

are more than 4000 of these machines worldwide and 2389 in the U.S. alone as of 2018. And, the authors add, "to date, U.S. regulators haven't had the interest or resources to investigate BTMs, so it's more or less an open secret that they're used by drug dealers and other criminals" (Bloomberg Businessweek, 2018).

As criminals become more aware and knowledgeable of the technology behind cryptocurrencies, the amount of money laundered through Bitcoin continues to increase. A company called CipherTrace noted that criminals illicitly gained a total of $1.2 billion via cryptocurrency exchanges between 2017 and 2018 (Malwa, 2018). Furthermore, a report published in American Banker estimates that approximately $761 million has been laundered using cryptocurrency thus far in 2018 (Crosman, 2018, p. 128). Since the year is not over, this number is predicted to increase.

Because of the transactional information listed on the public ledger, law enforcement agencies, like the FBI, can diligently analyze the flow of transactions. The primary issue revolves around tracing the money back to a specific identity. After the Financial Crimes Enforcement Network stated that cryptocurrencies are not classified as money service businesses, tracking the money has been especially difficult because cryptocurrency investors are not subject to the Bank Secrecy Act (Sánchez, 2017, p. 185).

Cryptocurrency money launderers facilitate a condensed version of traditional money laundering. The two-step process includes layering and integration in which the launderers must deposit and withdrawal the cash and cryptocurrency anonymously. The layering step consists of investing the dirty money in cryptocurrency via mixers or tumblers (Malwa, 2018). In summary, mixers and tumblers are money laundering services that charge a 1-3% transaction fee in order to mix various funds together and then output the funds to obscure the cryptocurrency's origin (CipherTrace, 2018, p. 7). To optimize anonymity during mixing, services spread the pay-outs over time and randomly divide the amount of bitcoin being mixed (Van Wegberg, Oerlemans, & Van Deventer, 2018). The services continually transfer cryptocurrencies within the network in order to steadily complicate the ability to track them. Once the trail is unclear enough to trace, integration takes place, and the funds are moved into the mainstream financial system (CipherTrace, 2018, p. 6).

Christian Brenig, Rafael Accorsi, and Günter Müller (2015) write that administration, flexibility, irrevocability, portability, and rapidity are among a few of the characteristics that entice money launderers to use cryptocurrencies instead of cash. As previously mentioned, Bitcoin operates on a decentralized peer-to-peer network. The nature of this network means that law enforcement agencies have no ability to delete accounts that they suspect are involved with money laundering. Furthermore, because of the network's pseudo-anonymity, individuals have the ability to own and operate more than one account, which progressively complicates the process of finding the origin.

Flexibility derives from the convenience that cryptocurrencies offer since transactions can be made internationally in a matter of minutes and from behind a computer. Instead of hiring outside help and purchasing plane tickets to invest in offshore accounts, crypto money launderers can commit the crime with the click of a button. Irrevocability decreases the risk of payment fraud and helps launderers profit because "no rational criminal would take legal action against [another criminal] . . . due to the risk of being prosecuted likewise" (Brenig et. al, 2015, p. 9). Since cryptocurrency accounts are accessed via the internet, criminals no longer feel apprehension when attempting to

smuggle bulk amounts of cash into other countries. Finally, the rapidness of transactions frees up time, money, and other resources and gives criminals ample time to engage in other illegal activities.

TAX EVASION

Introduction to the American Tax System

In the United States, citizens pay federal taxes to help provide government services and to help encourage economic growth. The U.S. utilizes a progressive tax system in which the proportion of taxes an individual or household pays directly correlates to income (Roach, 2010, p. 2). In other words, the greater the income, the higher the taxes (up to a maximum tax rate). It is the responsibility of taxpayers to voluntarily report their taxable gains or losses.

Capital gains and losses are determined by calculating how much the cost of the assets, like stocks and bonds, has increased or decreased from the time of the initial purchase to the time of the final sale (Erb, 2018). Capital gains occur when a profit exists, and capital losses occur when yearly losses exceed yearly gains. At the end of the year, the gains or losses from sales or exchanges are taxed as personal assets ("Tax tips for Bitcoin," 2018).

Taxing Cryptocurrencies

It has been argued that cryptocurrencies like Bitcoin can act as both a property and a currency (Roman, 2015, p. 451). Cryptocurrencies parallel properties like stocks and bonds in the sense that they are both subjected to capital gains and losses at the end of the fiscal year. Similarly, cryptocurrencies mirror government-backed currencies because some people use Bitcoin as a platform to buy or trade certain goods and services. However, the Internal Revenue Service released Notice 2014-21 to address the debate by declaring that virtual currencies are treated as property for the purpose of federal taxes (2014, p. 2). Notice 2014-21 clarifies how tax laws apply to virtual currencies by answering multiple questions from the public. Because of the newness and large scope of virtual currencies, the notice further acknowledges that additional questions will arise and encourages the public to submit such questions for clarification. Prior to the release of Notice 2014-21, it was predicted that the IRS would classify Bitcoin as either a security, a foreign currency, or a commodity (Slattery, 2014, p. 855).

Sánchez (2017, p. 187) further supports the IRS's categorization of virtual currencies by stating that cryptocurrencies will be regarded as "capital assets taxed at capital gains and losses." According to Kelly Phillips Erb (2018), taxable events occur when receiving or sending cryptocurrency in exchange for goods, services, cash, or even other types of cryptocurrencies. Erb's explanation can be simplified to say that general transactions consist of using currency to buy, sell, send, or receive goods, services, or other currencies. Any profits made from cryptocurrencies can be cashed out and considered income. If the taxpayer owns the cryptocurrency for at least one full year, the property is considered a long-term capital asset, and if the taxpayer owns the cryptocurrency for less than a year, the property is categorized as a short-term gain at a regular income tax rate (Roman, 2015, p. 453). Nonetheless, the owner must ensure that any cryptocurrency-related transactions are reported to the IRS.

When filing taxes, individuals, including cryptocurrency miners, must report all taxable cryptocurrency exchanges in U.S. dollars ("Notice 2014-21," 2014, p. 3). To make the conversion, the individual must evaluate the cryptocurrency's fair market value on the day of the transaction. Recording the date on which the cryptocurrency was bought and sold, the amount that was originally paid for it, and the amount received for the sale of the cryptocurrency provides fundamental information to the IRS (Bahney, 2018). In order to make the bookkeeping process easier, websites like Bitcoin.tax help determine crypto-taxes. Specifically, Coinbase generates individualized Cost Basis for Taxes reports that show the purchase prices of cryptocurrency-to-cryptocurrency trades and the resulting profits ("Taxes FAQ," n.d.).

Traditional Tax Evasion

Each individual or household has the responsibility of filing taxes and returns (or filing for an extension) with the Internal Revenue Service by April 15th of each year. Failure to file taxes by this date could be a result of negligence or, in the worst case, tax evasion. By definition, tax evasion is the illegal act in which one fails to pay taxes, underpays taxes owed, provides false information regarding income, or understates taxes by a significant amount (Murray, 2018). Failure to abide by tax laws results in federal or state penalties ranging from fines to imprisonment. According to the IRS, those who evade taxes are at risk of a maximum of five years in prison and a fine up to $250,000 ("IRS reminds taxpayers," 2018).

Similar to money laundering, offshore accounts serve as a popular strategy for those trying to evade taxes. A common misconception is that all offshore accounts are used for shady or illegitimate business. However, owning an offshore account is not illegal and is especially common for people who lived in another country before moving to the United States. Illegality arises when a person owns an offshore account for the purpose of evading taxes and knowingly fails to report the account's holdings. In order for the government to prove tax evasion, it must show that the subject under review intentionally withheld account information to avoid reports for tax requirements ("Tax evasion of offshore accounts," 2018). Regardless of the country in which the account is held, if the cryptocurrencies remain unreported, they remain untaxed.

Cryptocurrency Complications in Tax Evasion

Just like with divorce and money laundering, cryptocurrencies have created new complications regarding tax evasion. As in the previous two cases, pseudo-anonymity appeals to those who wish to hide their taxable incomes. Despite federal law and the potential to be criminally prosecuted, significant numbers of cryptocurrency owners still fail to report their holdings. A tax preparation service reported that approximately 7% of Americans own cryptocurrency and that 0.04% of tax filers in the U.S. declared their cryptocurrency gains and losses to the IRS in 2018 (Wieczner, 2018). Furthermore, in January 2018, 57% of the 2,000 American cryptocurrency owners surveyed by Credit Karma Tax and Qualtrics said they were aware of the taxable gains from their cryptocurrency investments (Wieczner, 2018). The first step to fight tax evasion via cryptocurrencies is to educate the public on the rules and regulations set forth by the IRS.

Multiple savings accounts, transaction divisions, tax-exempt agents, and foreign transactions all help facilitate cryptocurrency tax evasion by further obscuring the exchange trails (Jafari et. al, pp.

7-8). As with money laundering, an easy way to muddy the trail of transactions is to open multiple digital savings accounts. In order to successfully operate these accounts and divide transactions, one must own multiple digital wallets that only receive—and cannot send—cryptocurrencies. Again, a person can use multiple burner phones to confirm alias email addresses for various accounts that each contain a different username.

The fork and merge method is a popular distribution tactic in which the cryptocurrency owner divides the cryptocurrency into smaller portions, transfers the portions to several accounts, and finally transfers the smaller portions back to a different, singular account (Jafari et. al, p. 7). Tax-exempt agents are third parties that account for the most complex way to evade cryptocurrency taxes (Jafari et. al, p. 7). Briefly, this type of transaction involves three steps: 1) a person using cryptocurrency to pay an agent for stock, 2) the agent purchasing the stock using the dollar value, and 3) the agent returning the cryptocurrency value of the company's dividends back to the original investor (Marian, 2013, p. 43). The value of the depreciation or appreciation of the stock determines if the investor pays the agent or vice versa.

Finally, foreign transactions for the purpose of evading taxes consist of investing foreign currency into cryptocurrency accounts since bank secrecy laws prevent third-party institutions from sharing account information with other governments ("Foreign account," 2018). In an attempt to impede foreign accounts used for tax evasion, the IRS implemented the Foreign Account Tax Compliance Act (FATCA), which "generally requires that foreign financial institutions and certain other non-financial foreign entities report on the foreign assets held by their U.S. account holders" ("Foreign account," 2018).

Summary of U.S. v. Coinbase, Inc.

The use of cryptocurrencies for tax evasion gained international attention when the IRS requested personal records from the virtual currency exchange, Coinbase ("U.S. v. Coinbase," 2017). The IRS filed a "John Doe" summons, which categorizes individuals by activities as opposed to specific identities, on all U.S. Coinbase customers who made cryptocurrency exchanges between 2013 and 2015 (Erb, 2017). "Under 26 U.S.C. § 7602(a), the IRS may issue a summons for 'ascertaining the correctness of any return, making a return where none has been made, determining the liability of any person for any internal revenue tax or ... collecting any such liability....'" 26 U.S.C. § 7602(a) (U.S. v. Coinbase," 2017). The reasoning behind the initial summons was that Coinbase had roughly 5.9 million customers who exchanged $6 billion (in total) in Bitcoin, while only 800 or 900 people made potentially Bitcoin-related claims on Form 8949 (Dechert LLP, 2017). After much contemplation, the court decided that Coinbase would only have to release the records of users who spent at least $20,000 on a single transaction at any given time between 2013 and 2015 (Erb, 2017). This revolutionary case helped the IRS shed light on the importance of taxation of virtual currencies, while allowing Coinbase to protect the guaranteed anonymity and privacy of the majority of its users.

CONCLUSION

Since the time of its launch in 2009, Bitcoin has increasingly become a popular, controversial topic that frequently initiates debates between lawyers, government agencies, computer scientists,

investors, and even the general public. Aspects like anonymity and transaction processing speed are portrayed in both positive and negative ways. For example, while rapidity is beneficial for facilitating international purchases and for sending money to long-distance relatives, this speed also enables and eases the process of global money laundering and tax evasion. Even though law enforcement agencies know about these issues, only so much can be done due to the platform's original conditions and features. Even highly qualified and trained digital forensic scientists struggle to find a solution to the issues revolving around Bitcoin and other cryptocurrencies. Despite progressive advancements in both cybersecurity and the technology behind cryptocurrencies, illicit uses of cryptocurrencies still persist. As long as the technology continues to advance, so will the minds of criminals.

Bitcoin and other cryptocurrencies have introduced social, legal, and economic problems that were unimaginable twenty years ago. Although law enforcement agencies and governmental tax entities like the IRS have issued rules concerning legal reporting for cryptocurrencies, the decentralization and anonymity of the peer-to-peer network make it difficult to fully regulate and enforce such laws. Douglas Heaven (2018) declares that "even if regulation were stricter, . . . it's not clear that it would make a difference" (p. 62). Heaven (2018) also mentions that the U.S. government is in the process of creating a law that would make it illegal to deal with blacklisted cryptocurrency addresses of criminal groups like drug traffickers and terrorists. While regulations regarding illicit uses of cryptocurrencies are gaining traction around the globe, the criminal problems stemming from the nature of these virtual currencies may never truly be resolved.

REFERENCES

Anti-money laundering/combating the financing of terrorism - topics. (n.d.). *International Monetary Fund.* Retrieved from https://www.imf.org/external/np/leg/amlcft/eng/aml1.htm

Avila, J., & Ruppel, G. (2009). *ABC News.* Retrieved from abcnews.go.com: https://abcnews.go.com/2020/story?id=8101209&page=1

Bahney, A. (2018). *4 things to know about your cryptocurrency at tax time.* Retrieved from https://money.cnn.com/2018/03/26/pf/how-to-pay-taxes-on-cryptocurrency/index.html

Bloomberg, J. (2017). Using Bitcoin or other cryptocurrency to commit crimes? Law enforcement is onto you. *Forbes.* Retrieved from https://www.forbes.com/sites/jasonbloomberg/2017/12/28/using-bitcoin-or-other-cryptocurrency-to-commit-crimes-law-enforcement-is-onto-you/#6c74d5cc3bdc

Bloomberg Businessweek. (2018). Bitcoin ATMs May Be Used to Launder Money: Retrieved from https://www.bloomberg.com/features/2018-bitcoin-atm-money-laundering/

Bower, B. (2018). Money's murky origins. *Science News, 194*(3), 16-21.

Brenig, C., Accorsi, R., & Müller, G. (2015). *Economic analysis of cryptocurrency backed money laundering (2015).* ECIS 2015 Completed Research Papers. Paper 20. Retrieved from AIS Electronic Library.

Brown, S. D. (2016). Cryptocurrency and criminality: The Bitcoin opportunity. *Police Journal, 89*(4), 327-339. doi:10.1177/2F0032258X16658927

Burke, A. S. (2018). Money laundering. In *Salem Press Encyclopedia.*

Centeno, D. (2017). *Hiding assets with Bitcoin in divorce*. Retrieved from https://www.huffingtonpost.com/entry/hiding-assets-with-bitcoin-in-divorce_us_58ae640ce4b0ea6ee3d035ca

Chown, J. F. (1994). *A history of money: From AD 800.* New York, NY: Routledge.

CipherT. (2018). *Cryptocurrency anti-money laundering report.* Retrieved from https://cdn2.hubspot.net/hubfs/4345106/crypto_aml_report_2018q2.pdf

Crosby, M., Nachiappan, Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation Review, 2.* Retrieved from http://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf

Crosman, P. (2018). Crypto money laundering up threefold in 2018: Report. *American Banker, 183*(128), 1.

David. (2018). *3 best ways to convert Bitcoin to USD cash anonymously.* Retrieved from https://thedroidguy.com/2018/10/3-best-ways-convert-bitcoin-usd-cash-anonymously-1079119

Dechert LLP. (2017). *U.S. v. Coinbase: Virtual currency holders not outside the IRS's Reach.* Retrieved from https://www.jdsupra.com/legalnews/u-s-v- coinbase-virtual-currency-holders-75352/

Equitable distribution frequently asked questions. (2018). *Justia*. Retrieved from https:// www.justia.com/family/divorce/docs/equitable-distribution-faq/#q7

Erb, K. P. (2017). *IRS nabs big win over Coinbase in bid for Bitcoin customer data.* Retrieved from https://www.forbes.com/sites/kellyphillipserb/2017/11/29/irs-nabs-big-win-over-coinbase-in-bid-for-bitcoin-customer-data/#6f01ccc2259a

Erb, K. P. (2018). *What you need to know about taxes & cryptocurrency.* Retrieved from https://www.forbes.com/sites/kellyphillipserb/2018/01/09/what-you-need-to-know-about-taxes-cryptocurrency/#4031d131605f

Exchange of documents and information: "Discovery." (n.d.). *FindLaw*. Retrieved from https://family.findlaw.com/divorce/exchange-of-documents-and-information-discovery.html

Fiat money. (2018). *Corporate Finance Institute.* Retrieved from https://corporatefinance institute.com/resources/knowledge/economics/fiat-money-currency/

Financial Crimes Enforcement Network. (n.d.). Retrieved from FinCEN's Mandate From Congress: https://www.fincen.gov/resources/fincens-mandate-congress

Fiorillo, S. (2018). *How to buy Bitcoin and where*. Retrieved from https://www.thestreet.com/investing/bitcoin/where-to-buy-bitcoin-14549594

Foreign account tax compliance act. (2018). *Internal Revenue Service.* Retrieved from https://www.irs.gov/businesses/corporations/foreign-account-tax-compliance-act-fatca

Genesis block — definition and example. (2018). *Market Business News*. Retrieved from https://marketbusinessnews.com/financial-glossary/genesis-block/

Harpaz, O., & Goldberg, D. (2019, May 29). The Nanshou Campaign – Hackers arsenal grows stronger. *Gardicore.com*. Retrieved from https://www.guardicore.com/2019/05/nansh0u-campaign-hackers-arsenal-grows-stronger/

Heaven, D. (2018). Can you spot the cryptocrime in this picture?. *MIT Technology Review, 121*(3), 58-63.

Hochberg, B. S. (2018). Bitcoin and divorce. [blog]. Retrieved from http://www.familylawtopics.com/2018/03/bitcoin-and-divorce/

Hou, C. (2015). A bit-ter divorce: Using Bitcoin to hide material assets. *North Carolina Journal of Law & Technology, Online Edition, 16*(5), 74-105.

Humphreys, A. (2017). *National Post.* Retrieved from https://nationalpost.com/news/canada/this-man-would-rather-go-to-jail-than-pay-his-ex-wife-10-million-in-epic-divorce-battle

IRS reminds taxpayers to report virtual currency transactions. (2018). *Internal Revenue Service.* Retrieved from https://www.irs.gov/newsroom/irs-reminds-taxpayers-to-report-virtual-currency-transactions

Jafari, S., Vo-Huu, T., Jabiyev, B., Mera, A., & Farkhani, R. M. (2018).Cryptocurrency: A challenge to the legal system. doi:10.2139/ssrn.3172489

King, R. (2018). *How to cash out Bitcoin?.* Retrieved from https://www.bitdegree.org/tutorials/how-to-cash-out-bitcoin/

Layton, J., & Curran, O. (n.d.). *How money laundering works.* Retrieved from https:// money.howstuffworks.com/money-laundering1.htm

Malwa, S. (2018). *$1.2 billion in cryptocurrency laundered through Bitcoin, tumblers, privacy coins.* Retrieved from https://www.ccn.com/1-2-billion-in-cryptocurrency-laundered-through-bitcoin-tumblers-privacy-coins/

Marian, O. Y. (2013). Are cryptocurrencies super 'tax' havens?. *Michigan Law Review First Impressions, 112*(38), 38-48. Retrieved from https://scholarship.law.ufl.edu/ cgi/viewcontent.cgi?referer=&httpsredir=1&article=1365&context=facultypub

McAfee, D. (2017). *Bitcoin the new mattress full of cash for divorce cheats.* Retrieved from https://www.bna.com/bitcoin-new-mattress-n73014473679

Men's rights activists: Use Bitcoin to hide money from your future ex-wife. (2017). *The Daily Beast.*

Money laundering: A three-stage process. (2017). *About Business Crime Solutions Inc.* Retrieved from https://www.moneylaundering.ca/public/law/3_stages_ML.php

Money laundering. (n.d. a). *Legal Information Institute at Cornell Law School*. Retrieved from https://www.law.cornell.edu/wex/money_laundering

Money laundering (n.d. b). *Legal Dictionary*. Retrieved from https://legaldictionary.net/ money-laundering/

Murray, J. (2018). *What is the difference between tax avoidance and tax evasion?.* Retrieved from https://www.thebalancesmb.com/tax-avoidance-vs-evasion-397671

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Bitcoin*. Retrieved from https://bitcoin.org/bitcoin.pdf

Notice 2014-12. (2014). *Internal Revenue Service.* Retrieved from https://www.irs.gov/pub/irs-drop/n-14-21.pdf

O.C.G.A. §9-11-26 - General provisions governing discovery. (2010). *Justia*. Retrieved from https://law.justia.com/codes/georgia/2010/title-9/chapter-11/article-5/9-11-2 6/

Peachey, K. (2018). *Divorcing couples may clash over Bitcoin.* Retrieved from https://www.bbc.com/news/business-43070849

Ratner, J. R. (2011). Distribution of Marital Assets in Community Property Jurisdictions: Equitable Doesn't Mean Equal. *Louisiana Law Review*, 21-59.

Roach, B. (2010). Taxes in the United States: History, fairness, and current political issues. *Global Development And Environment Institute.* Retrieved from http://www.ase.tufts.edu/gdae/education_materials/modules/Taxes_in_the_United_States.pdf

Roberts, J. J. (2018). *Bitcoin and taxes: What you need to know about cryptocurrency and the IRS.* Retrieved from http://fortune.com/2018/01/29/bitcoin-taxes-cryptocurrency-irs/

Roman, J. A. (2015). Bitcoin: Assessing the tax implications associated with the IRS's notice deeming virtual currencies property. *Review of Banking & Financial Law,34*(2), 451-457.

Sánchez, E. G. (2017). Crypto-currencies: The 21st century's money laundering and tax havens. *University of Florida Journal of Law & Public Policy*, *28*(1), 167-191.

Sharma, R. (2017). *What was behind Bitcoin's insane price moves on Dec. 7?.* Retrieved from https://www.investopedia.com/news/what-was-behind-bitcoins-insane-price-moves-dec-7/

Slattery, T. (2014). Taking a bit out of crime: Bitcoin and cross-border tax evasion. *Brooklyn Journal of International Law, 39*(2), 829-873.

Smith, K. A. (2018). *13 types of cryptocurrency that aren't bitcoin.* Retrieved from https://www.bankrate.com/investing/types-of-cryptocurrency/

Smith, K. (2018a). *Tax havens for the masses: How crypto makes tax evasion easy.* Retrieved from https://www.coininsider.com/cryptocurrency-tax-evasion/

Smith, K. (2018b). *Crypto assets hidden during divorce proceedings.* Retrieved from https://bravenewcoin.com/insights/crypto-assets-hidden-during-divorce- proceedings

Stim, R. (2018). *Property division by state.* Retrieved from https://www.divorcenet.com/states/nationwide/property_division_by_state

Tax evasion of offshore accounts (2018) — IRS offshore banking rules. (2018, June 6). *Golding and Golding Attorneys at Law*. Retrieved from https://www.goldinglaw yers.com/tax-evasion-offshore-accounts-2018-irs-offshore-criminal-tax-basics/

Tax tips for Bitcoin and virtual currency. (2018). *TurboTax*. Retrieved from https:// turbotax.intuit.com/tax-tips/tax-payments/tax-tips-for-bitcoin-and-virtual-currency/L1ZOgU00q

Taxes FAQ. (n.d.). *Coinbase.* Retrieved from https://support.coinbase.com/customer/en/ portal/articles/1496488-taxes-faq

U.S. v. Coinbase, Inc. (2017). *Leagle*. Retrieved from https://www.leagle. com/decision/infdco20171130f45

Van der Speck, R. J. (n.d.). Commodity prices in Babylon 385 - 61 BC. *International Institute of Social History.* Retrieved from http://www.iisg.nl/hpw/babylon.php

Van Wegberg, R., Oerlemans, J. J., & Van Deventer, O. (2018). Bitcoin money laundering: mixed results?: An explorative study on money laundering of cybercrime proceeds using bitcoin. *Journal of Financial Crime, 25*(2).

Weigant, C. (2011). *A beginner's guide to America's tax system.* Retrieved from https://www.businessinsider.com/a-beginners-guide-to-americas-tax-system-2011-4

West, R., & Kainen, E. (2018). Taking a bite out of Bitcoin! The heads and tails of cryptocurrency [Webinar]. Retrieved from http://s3.amazonaws.com/AKI AJLYL55VQXLE4XG3Q-0-AAML/wview.html

What is cryptocurrency: Everything you need to know [ultimate guide]. (2018). *BlockGeeks*. Retrieved from https://blockgeeks.com/guides/what-is- cryptocurrency/

Wieczner, J. (2018). *Bitcoin investors aren't paying their cryptocurrency taxes*. Retrieved from http://fortune.com/2018/02/13/bitcoin-cryptocurrency-tax-taxes/

Wright, D. (2018). *An introduction to cryptocurrencies in divorce.* Retrieved from https://www.lexology.com/library/detail.aspx?g=b7a259ce-a12b-4263-9d85-7e175d1719e

QRBD

QUARTERLY REVIEW OF BUSINESS DISCIPLINES

November 2019

Volume 6
Number 3

A JOURNAL OF INTERNATIONAL ACADEMY OF BUSINESS DISCIPLINES
SPONSORED BY UNIVERSITY OF NORTH FLORIDA
ISSN 2334-0169 (print)
ISSN 2329-5163 (online)