Spring 6-2018

# Understanding the Nexus between Cryptocurrencies and Transnational Crime Operations

Sarah Durrant
*CUNY John Jay College*, sarah.durrant@jjay.cuny.edu

# Understanding the Nexus between Cryptocurrencies and Transnational Crime Operations

A Thesis Presented in Partial Fulfillment of the
Requirements for the Masters of Arts in
International Crime and Justice

John Jay College of Criminal Justice
City University of New York

Sarah Durrant

May 2018

**Abstract**

Cryptocurrencies are private, decentralized currencies that operate via the Internet and have attracted criminals because of the convenience and virtual anonymity they offer. While there are many descriptive accounts of cryptocurrencies and their use both in legal and illegal operations, to date there is no empirical research to understand the use of cryptocurrencies in transnational crime operations, specifically why transnational criminals may find them attractive to either conduct business or to launder their illicit proceeds. Using the environmental criminological framework, this study analyzed 100 cases of cryptocurrency use in transnational crime activities identified through various secondary sources, including online newspaper articles and publicly available court case information. Essentially this study used both quantitative and qualitative analysis to examine the ways in which cryptocurrencies facilitate transnational crimes. The findings indicate that criminals have been using cryptocurrencies to conceal the enormous amounts of money they are receiving for their crimes, specifically money laundering, drug trafficking (illicit drug sales), and terrorism financing. It was found that offenders can conduct business, launder money, and make a profit by using cryptocurrencies to facilitate their crimes, creating for crime opportunities permitted by cryptocurrencies. These opportunities include the ease of floating from one crime to another and using cryptocurrencies to cover offenders' tracks, where cryptocurrencies can transact, launder, and conceal all in one. It was found that offenders gravitate towards using bitcoin to facilitate their operations, most likely due to its popularity and reliability. When looking at the crime of money laundering and illicit drug sales specifically, it was found that offenders can generate higher operation amounts, spanning into billions of dollars, all while evading detection. With the assumption that transnational criminals are rational beings, money laundering using cryptocurrencies has enormous benefits with these high operation amounts. This coupled with the low chances of being caught by law enforcement, makes money laundering a feasible crime where the benefits far outweigh the risks. This exploratory research is innovative and imperative to expanding academic knowledge on the evolution of crime with the use of cryptocurrencies and assisting in reducing the opportunities cryptocurrencies allow in transnational crime operations.

*Keywords*: cryptocurrency, bitcoin, money laundering, drug trafficking, terrorism financing, crime opportunity structure and reduction

**ACKNOWLEDGEMENTS**

I would first like to thank my thesis advisor Dr. Mangai Natarajan at John Jay College of Criminal Justice. Dr. Natarajan held my hand and guided me through this journey in successfully completing a thesis. She was attentive and invested in every aspect from writing the proposal to helping me across the finish line. She has directed me well and I have learned so much from her.

I would also like to acknowledge Dr. Marie-Helen Maras at John Jay College of Criminal Justice as the second reader of this thesis. She has offered invaluable comments, especially considering this topic is within her field of interest. I am gratefully indebted to her for her patience and enthusiasm for me on this thesis.

Finally, I must express my gratitude to my parents for their love and support throughout my many years of schooling and through the process of researching and writing this thesis. This accomplishment would not have been possible without them. Thank you.

Sarah Durrant

# Table of Contents

**INTRODUCTION** ..... **6**

**LITERATURE REVIEW: CRYPTOCURRENCIES AND TRANSNATIONAL CRIMES** ..... **7**

RISE OF CRYPTOCURRENCIES ..... 7

FEATURES OF CRYPTOCURRENCIES ..... 11

*Transactional Costs.* ..... *11*

*Reliability.* ..... *12*

*Anonymity.* ..... *13*

*Financial Inclusion.* ..... *14*

*Price Volatility.* ..... *16*

*Lack of Oversight.* ..... *17*

*Crime Association.* ..... *19*

CRYPTOCURRENCIES AND TRANSNATIONAL CRIMES ..... 19

*Money Laundering* ..... *19*

Cryptolaundering Process ..... 20

Follow the Money ..... 23

*Drug Trafficking* ..... *28*

*Terrorism Financing* ..... *29*

**THE PRESENT STUDY** ..... **32**

**THEORETICAL FRAMEWORK** ..... **34**

**METHODS** ..... **42**

RESEARCH DESIGN ..... 42

RESEARCH QUESTION ..... 42

DATA COLLECTION METHODS ..... 43

DATA ANALYSIS ..... 44

*Quantitative Data.* ..... *44*

*Qualitative Data.* ..... *45*

ETHICAL CONCERNS ..... 46

LIMITATIONS ..... 46

**DATA ANALYSES AND FINDINGS** ..... **47**

QUANTITATIVE ANALYSES ..... 48

*Bivariate Analyses* ..... *49*

CONTENT ANALYSIS OF QUALITATIVE DATA ..... 53

*Theme 1: Criminals use the darknet to buy and sell drugs* ..... *54*

Types of Darknet Marketplaces Used. ..... 54

Evolving Nature of Darknet Marketplaces. ..... 55

Use of Darknet and Bitcoin to Evade Detection ..... 56

Diversification ..... 57

Types of drugs sold. ..... 57

Summary ..... 59

*Theme 2: Networking and the division of labor* ..... *59*

Division of Labor. ..... 60

Familial Ties. ..... 61

Commissions. ..... 62

Use of Middlemen ..... 63

Summary ..... 64

*Theme 3: One crime provides opportunities for other crimes* ..... *65*

Corruption. ..... 65

Misappropriation of Client Money. ..... 66

Other Crimes. ..... 68

Summary ..... 69
*Theme 4: Money laundering services* ..... *70*
Front companies ..... 70
Money Exchanges ..... 71
Bridging the Gap ..... 72
Summary ..... 73
*Theme 5: Terror support and cryptocurrencies* ..... *74*
Bitcoins Used to Fund Terrorism. ..... 74
A Variety of Cryptocurrencies are Used. ..... 75
Middlemen Collect Money. ..... 75
Summary ..... 76
*Theme 6: Challenges for law enforcement and prosecution* ..... *77*
Precedent. ..... 77
Brains versus Brawn ..... 79
Summary ..... 80
**DISCUSSION ..... 81**
CASH FLOW ..... 81
DEAL, LAUNDER, AND PROFIT ..... 84
ONE CRIME LEADS TO ANOTHER ..... 86
THEORETICAL IMPLICATIONS ..... 88
PRESCRIPTION FOR PREVENTION ..... 90
**CONCLUSION ..... 93**
**APPENDIX A: ARTICLE CITATIONS FOR ALL CASES ..... 97**
**APPENDIX B: CODE BOOK ..... 118**
**REFERENCES ..... 119**

**Understanding the Nexus between Cryptocurrencies and Transnational Crime Operations**

Globalization has redefined the way crimes are committed. What used to be limited to the regional has now been opened up to the global arena, allowing for various transnational crimes to not only grow, but to thrive as well. With innovations such as the Internet, criminal organizations can proceed with their enterprises in a more clandestine manner, allowing them to be more resilient to law enforcement, due to the anonymity and lack of oversight the Internet allows. By moving operations online, criminals have a faster and cheaper way of conducting business, while reaching consumers all over the world (Lavorgna, 2015).

In her book, Maras (2016) discusses how organized crime groups have used the Internet to their advantage as a way to facilitate the crimes they commit. She discusses how the Internet is used for communication between suppliers and consumers, as well as suppliers and subordinates, making communication easier, faster, and more efficient. She mentions that the Internet has also been used as a way to market criminal enterprises, which allows criminals to expand their reputation beyond word of mouth in the neighborhood to word of mouth across the Internet. This gives criminals the opportunity to build a diverse set of consumers and maintain these relationships in a secure manner, considering many of these exchanges no longer occur face to face. What is interesting is that even with the move of criminal operations online, particularly with black markets, they still reflect the same supply and demand trends as the traditional legal market.

Because trafficking enterprises of all kinds have gained more traction due to the use of the Internet, more proceeds have been made. However, these proceeds are not legitimate. With large sums of money needing to be laundered without raising red flags to law enforcement, money laundering has also become more prevalent online, for the same reasons criminals moved

their businesses online. This move has made money laundering also more resilient to law enforcement because of the various avenues that could be taken to launder the illegal proceeds from transnational crimes. One of these avenues is laundering money through the use of cryptocurrencies (Stuhlmiller, 2013).

This study aimed to examine the ways in which cryptocurrencies facilitate transnational crimes, particularly money laundering, online illicit drug transactions, and terrorism financing. This exploratory study is important, not only to understand the relationship between the uses of cryptocurrencies by transnational criminals, but also to find measures to control and prevent such cybercrimes from happening.

## Literature Review: Cryptocurrencies and Transnational Crimes

In order to have a solid foundation for this research study, a review of literature is important to find areas in which current research could be built upon and areas that have yet to be explored. A comprehensive look at the literature allows for innovative studies to take place based on sound logic from previous academic literature. Using library resources from John Jay College of Criminal Justice, including databases such as EBSCO, JSTOR, Academic OneFile, and Sage Journals, a literature review was undertaken and the emerging themes are discussed below.

### Rise of Cryptocurrencies

So, what are cryptocurrencies exactly? According to the Financial Action Task Force (FATF), a virtual currency is “a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value,

but does not have legal tender status…in any jurisdiction" (FATF, 2014). In other words, cryptocurrencies are private, digitalized currencies that operate similar to cash, yet all banking occurs online and no government or corporation can claim it as its own. These currencies are not regulated by any financial institution, but rather are maintained in a peer-to-peer network, meaning that those who use the currency are those who maintain and influence the currency's market, and thus imply that individual governments have no access to control this new form of globalized economy (Plassaras, 2013).

The rise of virtual currencies came around the time when the gold standard collapsed and globalization began to gain traction. The collapse of the gold standard was a turning point in history because states began to realize just how interrelated their economies were. However, it was clear some currencies bounced back more rapidly than others (Driffill, 2012). In his article about the future of the international monetary system, Fratianni (2012) states,

> The world looks to the dollar because it is the largest and most liquid market of the world, and because of its political security. Almost everyone, including many Americans, thinks that the international role of the dollar is a terrible solution to the world's currency problems. It is just that every alternative is even worse.

Every alternative did seem worse, until the concept of cryptocurrencies took off, with the help of globalization. Cryptocurrencies pose a unique challenge to individual states by encroaching on a state's right to a monopoly of its own currency, yet offer a taste of a truly global free market (Fratianni, 2012).

Cryptocurrencies started as a financial experiment to see if a decentralized and digitalized version of money could survive. Not only did it survive, but it was actually able to thrive as well. At the beginning, it was computer fanatics and people who wanted a different way of banking

who had invested in this experiment. However, soon after, average people intrigued by the currency began to join the user base. Cryptocurrencies like bitcoin were designed for ease of use that allow virtually anyone to understand how it functions, should they want to be included. No computer background is needed in order to hold cryptocurrencies, allowing people from different backgrounds to be included in this global experiment. These currencies are now being used all across the world and this is due to their user-friendly design that only requires Internet access (Meek, 2014).

For the purpose of this study, any research or reference to cryptocurrencies that are stated as fact are in reference to bitcoins. This is because, as of right now, out of all the cryptocurrencies out there, bitcoin is the most popular and well known of them all; thus, the most research has been conducted on bitcoins. "Since 2009, over 75 virtual currencies have been created and are traded globally, representing about $11 billion in state market value, [where] of these, Bitcoin is the leader, representing about $10 billion or 90% of the total market" (Meek, 2014). While things may have changed marginally since 2014, bitcoin still appears to be the leader when it comes to cryptocurrencies. However, that is not to say that bitcoin itself is here to stay. Bitcoin technology is really the innovation, where banking could occur without banks and without political interference through the use of cryptocurrencies. With that being said, another note must be made where cryptocurrency, virtual currency, digital currency, and digital cash will all be used interchangeably through this paper to describe cryptocurrencies.

The way in which bitcoins work is that it first operates on a peer-to-peer network, meaning the users are the ones who develop and maintain the system and the transaction process. In order to keep track of all the transactions occurring, there is a publicly shared record of all bitcoin transactions, similar to that of a ledger, called the blockchain. This is where users of

bitcoin can verify each transaction made by other users. This allows the bitcoin process to have the ability to run without any entity overseeing it, as will be further explained in the reliability feature of cryptocurrencies. The blockchain can be viewed by anyone, from bitcoin users to law enforcement. Because of this, the identity of bitcoin users is not fully anonymous, but rather pseudo-anonymous, as will also be explained further in the following section as well (Lee, Long, McRae, Steiner, & Handler, 2015).

Bitcoins can be exchanged the same way the American dollar can be exchanged for European euros. Each bitcoin user, when they first purchase bitcoins, is issued a bitcoin wallet. This wallet has two keys in order to get into it: a public key, given out to receiving wallets, and a private key, which is solely meant for the owner of the bitcoins for security purposes. The way in which sending and receiving bitcoins works is similar to sharing files, except the only catch is that once a file is shared, the sender no longer has possession of the file and the receiver now has possession of that file until they decides to send it. This set up makes sure that the sender cannot "double spend" their bitcoins. Once an individual sends bitcoins to another person, they lose those bitcoins for good; there is no way to get those bitcoins back. After a transaction is made, the bitcoin community then verifies that the transaction is legitimate, where the sender has enough coins to send to the receiver. If the transaction checks out, a new block is published on the blockchain, where everyone can now view this newly verified transaction (Lee, Long, McRae, Steiner, & Handler, 2015).

There are three ways of obtaining bitcoins: (1) "mining," (2) purchasing bitcoins with another form of currency, or (3) receiving bitcoins in exchange for something else, like a product or service. "Mining" is an interesting process through which bitcoins are generated. At the most basic level, it is a complex process that requires computer power in order to solve difficult

algorithmic equations. It is solely through this process that new bitcoins are made. The anonymous creators of bitcoin created it to be a currency with a cap amount of 21 million bitcoins (Lee, Long, McRae, Steiner, & Handler, 2015). After this cap is reached, "mining" will cease and bitcoins will become rarer considering all bitcoins ever to be created will have already been created. The creators made bitcoin this way to give it some sort of value and to combat inflation and deflation (Plassaras, 2013). "A Bitcoin could be considered intrinsically and intuitively valuable given how difficult it is to produce" (Plassaras, 2013). If there is a finite amount of bitcoins in circulation, their rarity increases, but so does their value, very similar to that of gold, hence the term "mining" for bitcoins. Bitcoins can also easily be "cashed out" for any currency through online bitcoin exchanges. These exchanges sometimes charge a small fee for transaction; however, it is very low considering how high transaction fees can be for banks, as will be explained in the following section (Plassaras, 2013).

## Features of Cryptocurrencies

***Transactional Costs.*** Cryptocurrencies have many features that are both attractive and costly to its users. First, cryptocurrencies have little to no transactional costs, depending on the specific currency. This means that cryptocurrencies provide a cheaper way of sending money to anywhere in the world because transactions are not monitored by financial institutions, such as banks. This means that banks cannot charge fees for verifying that the money being sent from one customer to another is legitimate (Ammous, 2015). "It is equivalent of Google developing Gmail so that people could email for free and not have to pay for email services from companies such as AOL" (Meek, 2014). What is even better about the low transaction fees is that transactions will also go through almost immediately and in real time. With the blockchain

technology, other users who agree to partake in verifying transactions will authenticate that the sender has enough currency to send to the receiving party. This elimination of a trusted third party, such as banks, to authenticate these transactions also eliminates the transaction fees associated with it (Ammous, 2015).

***Reliability.*** Second, cryptocurrency technology is created to be reliable. Reliability is something that is questioned a lot in literature, but at the theoretical level, cryptocurrencies are built upon a system of verification. What this means is that this is a system that does not require trust in any transaction because multiple other users check every transaction that is ever made, which is important especially to states whose domestic banking systems are corrupt (Ammous, 2015). This idea goes back to the concept of a peer-to-peer network in that the users, not the government or various corporations, are the ones who control the currency market.

> Issuers of electronic currency would have a strong economic incentive to keep their currencies stable: the more stable the currency, the better a store of value it becomes and more likely others are to invest in it as a result" (Plassaras, 2013).

Legitimacy is built up through mass usage, not through the legitimacy of a single government and its monetary system. This means that once more users get onboard with the currency, it increases its consumer base; with an increased consumer base, reputation of the currency increases; as reputation increases, more users would be willing to try the currency. This creates a snowball effect in gaining traction in creating a sort of "trust among the masses" (Ammous, 2015).

To increase reliability, bitcoin creators have taken an extra step to make sure that all transactions are transparent. They created an online, public ledger that anyone with or without

the currency can view at any time. This eliminates the risk of "double spending," where once bitcoins leave one wallet, they are transferred to the receiving wallet; transactions are irreversible. There are two reasons why people believe the blockchain is reliable: trust among the masses, as well as trust in the code. The blockchain is not run by a single individual or organization, but rather the community using the currency. There is no point in failure for the blockchain due to the code that was written for it. It is fair and transparent, lending to the trust in the code. The code cannot be manipulated. The blockchain also lists all of the transactions ever made, while never revealing the true identity of any of its users. The idea of anonymity has been heatedly debated within the past couple of years, but in general, cryptocurrencies do not require personal identifiers in order to make transactions. All that is needed is access to the Internet, and the purchase of some cryptocurrencies, which has posed its own sorts of challenges to law enforcement and government policymakers (Ammous, 2015).

***Anonymity.*** Anonymity, the third feature of cryptocurrencies, is a feature enjoyed by all and not just criminals. Cryptocurrencies offer anonymity where the sender does not have to meet the receiver face-to-face, thus the only identifying feature of either party is their public keys. While the anonymity of cryptocurrencies has been most cited as a feature for criminals, anonymity could be enjoyed by all. Take cash, for example. Cash is also a relatively anonymous form of currency, yet it is widely accepted in most states. People often use cash out of convenience or distrust of banks; however, criminals also use cash, and a lot of it. Cryptocurrency is the digital form of cash, where transactions do not have to be made face-to-face. Cryptocurrencies have taken cash-only transactions and moved them online out of convenience and efficiency; it just so happens to also allow criminals to operate undetected.

However, the literature makes it a point to notice that cryptocurrencies are only pseudo-anonymous, where every transaction ever made using the cryptocurrency is public knowledge, available for anyone to see on the blockchain. By closely following the chain, it becomes apparent which wallet has been sending money to another wallet, and then what that wallet does with the money received. Thus, cryptocurrencies are not completely anonymous, yet they are anonymous enough that people feel safe using the currency without any sort of repercussion (Reynolds & Irwin, 2017).

With pseudo-anonymity, Koshy, Koshy, & McDaniel (2014) conducted a study that examined the blockchain to see whether transactions could be tracked to an individual through their IP address. What the researchers found was that they could actually trace bitcoin addresses back to a single IP address. While one individual may be the owner of many bitcoin wallets, what the researchers found was that by tracking IP addresses instead, law enforcement can actually trace back transactions published on the blockchain to specific people based on their IP address. This may not work for catching all criminals who use cryptocurrency; however, it could be a start to learning effective ways of managing the harms of cryptocurrencies (Koshy, Koshy, & McDaniel, 2014).

***Financial Inclusion.*** Fourth, cryptocurrencies offer a unique alternative to people who are "unbanked," meaning people who do not have access to financial systems in their home country, or choose not to open an account with domestic banks for various reasons, such as government corruption. Chaia, Dala, Goland, Gonzalez, Morduch, & Schiff (2009) state that "2.5 billion adults, just over half of the world's adult population, do not use formal financial services to save or borrow." These people tend to live in areas where banking may be risky if state

financial institutions are deemed as untrustworthy or state currencies are plagued with inflation. So rather than trusting the state to circulate currency, people will simply refrain from using state financial institutions or even state currency. The researchers emphasize the need for policies to give these unbanked populations access to affordable and reliable means for participating in the global financial arena; yet they do not have a concrete solution (Chaia et al., 2009). However, Clegg (2014) has the answer. Clegg (2014) defines financial inclusion as "the delivery of banking services at an affordable cost to the vast sections of disadvantaged and low-income groups" and describes how bitcoin could be the answer to Chaia et al.'s (2009) problem. With its increasing popularity, bitcoin can be both affordable and reliable for unbanked populations. It is simple enough for laypersons to understand and only requires access to the Internet (Clegg, 2014). Clegg (2014) does recognize that there needs to be an increase in Internet connection among developing states, however, he believes bitcoin to be the solution to financial inclusion across the globe. Overall, cryptocurrencies, should they prove to be reliable, offer an alternative way to bank that is detached from any political, social, or economic context, which allows a truly global free economy.

Financial inclusion is a huge driver for bitcoin technology. It offers people in developing nations a unique opportunity to engage in financial endeavors outside of their own state. Interestingly, Popper (2015) states "Bitcoin (a type of virtual currency) proponents like to say that the currency first became popular in the places that needed it least, like Europe and the United States, given how smoothly the currencies and financial services work there." With this experiment starting with computer fanatics, it has evolved into something that could actually be a practical solution for people in developing nations. Several research studies have been conducted on the idea that cryptocurrencies can thrive in states with poor financial systems (Aluko &

Bagheri, 2012; Clegg, 2014; Chaia et al., 2009; & Scott, 2016). Findings conclude that due to limited banking options, the desire for financial inclusion, and the embracement of neocapitalism, large populations of these states are willing to forgo state-backed currency for this new digital currency experiment. This desire for financial inclusion as a driving force to use cryptocurrencies has been referenced frequently in literature.

***Price Volatility.*** However, some academics would argue that cryptocurrencies are not reliable currencies in that their prices fluctuate rapidly. This fifth feature, price volatility, has been an issue for many users. What this means is that cryptocurrencies are prone to rapidly change in value. For example, after the fall of Mt Gox, a popular bitcoin exchange, bitcoin took a severe hit, where before one bitcoin was worth over $1,000 USD but fell to around $500 USD days directly after the fall, where users have now lost half the money they put into bitcoin. This left consumers questioning the reliability of the currency (Trautman, 2014). Because of this, some governments have chosen to view cryptocurrencies as commodities or stocks, rather than a viable currency because there currently is no stable exchange rate (Dostov & Shust, 2014).

This is a hotly debated topic, given the commodity versus currency debate across literature and legal standards. It is essential to address this ongoing debate as to whether cryptocurrencies are in fact considered currencies. While this study will abide by the definition of cryptocurrencies that the FATF released in 2014, where cryptocurrencies are defined as currency, every jurisdiction currently has a different way in viewing these digital currencies. The argument that has been made is whether cryptocurrencies act more like traditional currencies in the sense that they "[are] in circulation as a medium of exchange" (currency, 2017); or rather act more like a commodity in the sense that it is "an economic good" (commodity, 2017). There has

been great debate over this issue (Lee, Long, McRae, Steiner, & Handler, 2015; Tu & Meredith, 2015); however, it is still important to make this distinction, especially when money laundering will be discussed in relation to cryptocurrencies. If cryptocurrencies are not seen as a medium for exchange, or rather are not seen as an accepted currency, then money laundering with cryptocurrencies would not be considered money laundering; it would merely be illegal trading of goods. This implies that if cryptocurrencies are classified as commodities, they cannot be regulated by AML policies, or even the FATF for that matter. With such uncertainty regarding the medium of exchange that cryptocurrencies can hold, for the purposes of this study it will be assumed that virtual currencies are considered currencies and a valid medium of exchange, whether legal or not.

As a currency, the prices of bitcoin fluctuate so much because the "value of bitcoin is only based on the shared perception of value" (Dostov & Shust, 2014). In other words, the price of bitcoin is based on supply and demand. This means that the more people who adopt bitcoin and recognize its value, the more stable the currency will become. However, as mentioned before, bad media coverage, such as the bankruptcy of a bitcoin exchange or hacking attacks on bitcoin wallets, will definitely make the price of bitcoins sway negatively. Bitcoin is only as valuable as its users believe it to be; it is based on consensus. It is this rapid price change reliant upon perception that leads people to believe cryptocurrencies to be similar to commodities or investment stocks, and to ultimately not believe cryptocurrencies to be reliable currencies (Dostov & Shust, 2014).

***Lack of Oversight.*** Sixth, there is a lack of oversight when it comes to cryptocurrencies. As stated before, cryptocurrencies are decentralized, meaning there is no overall ownership of

the currency, which creates its own sets of problems for regulation. It is clear that cryptocurrencies are not universally handled the same way. States have chosen to respond differently to these cryptocurrencies. These reactions include: (1) taking no action, meaning states have no regulations about virtual currencies; (2) treating virtual currencies as commodities, regulating them with taxes; (3) completely banning virtual currencies, especially considering some states do not allow for currencies other than the national currency to be used; (4) treating virtual currencies as any other foreign currency, with the same regulations; and (5) taking a "wait-and-see" approach, where a state currently does not have regulations but may choose to regulate later should it believe this currency to be a threat (Tu & Meredith, 2015). However, these reactions only make the situation even more complex, considering cryptocurrencies transcend all boundaries, where a lack of systematization of financial regulations and jurisdictional borders serve as further obstacles that must be overcome. No individual, corporation, nor government can control these currencies, thus there are no protections for consumers from the various consequences of using these currencies (Dostov & Shust, 2014). Theft of bitcoins from hacking or malware is not uncommon; however, consumers cannot go to local authorities for help because they have no jurisdiction nor the tools or resources to investigate (FBI, 2012). As stated before, states have all taken different stances on how they choose to regulate cryptocurrencies; however, that is not enough. International organizations such as FATF and the International Monetary Fund (IMF) have also taken steps to see whether cryptocurrencies can fall within their jurisdictions; however, this too is not enough (Plassaras, 2013). In order to remedy this issue of oversight and jurisdiction, there needs to be a global, unified response to protect consumers from the lack of oversight with these currencies.

***Crime Association.*** Finally, cryptocurrencies are often associated with crime, which is another deterrent for many potential users. This feature has been a particular deterrent for laypersons to adopt cryptocurrencies because the currencies have been connected to all sorts of crimes. The literature goes back and forth on whether scholars believe cryptocurrencies to be strongly connected to crime. For example, Brown (2016) found that while cryptocurrencies have been used to purchase illicit items online, law enforcement at this point has not found cryptocurrencies to be that much of a threat. On the other hand, the FBI (2012) has found that there have been many criminal schemes that have occurred with the use of cryptocurrencies. In its 2012 report, the FBI (2012) mentions the different types of schemes they have come into contact with. The report ends with implications of how cryptocurrencies can be considered attractive to criminals.

## Cryptocurrencies and Transnational Crimes

**Money Laundering.** Money laundering is the primary crime that is often connected to cryptocurrencies in literature. It is a new way of concealing the true identity of illegal proceeds, but also a way of concealing the true identity of the user, to a certain extent. There have been a few studies that have made connections between money laundering and cryptocurrencies, based on the advantages they offers to criminals (Jacquez, 2016; Maras, 2016; Ritchet, 2017; Sat, Krylov, Evgenyevich. Bezverbnyi, Kasatkin & Kornev 2016; Stuhlmiller, 2013; Virga, 2015). Ritchet (2017) concluded that with the growing use of the Internet, it is likely that more money laundering will be seen to be taking place online than in person as technology advances and anonymity is reinforced. Agreeing with this conclusion, Sat et al. (2016) discussed that as technology advances, so do criminals. These researchers have emphasized that money launderers

are rational beings who take advantage of crime opportunities to remain undetected and are able to continue with their illicit operations. The researchers discuss the different reasons as to why money launderers are drawn to cryptocurrency as the new way to launder money, with the top reason being the anonymity offered. Stuhlmiller (2013) even stresses the harms to financial institutions that cryptocurrencies can have when they are associated with money laundering. The virtual environment through which cryptocurrencies are used allows criminals to thrive without fear of being caught. However, Irwin, Slay, Choo, & Liu (2014) emphasize that while cryptocurrencies offer money launderers an easy and anonymous experience, often times it takes more effort to make sure that the process of laundering the money runs smoothly by setting up the accounts needed and routing them accordingly. However, the researchers do note that more money can be laundered faster via cryptocurrencies than traditional means.

***Cryptolaundering Process.*** Traditionally, money laundering is a process that takes "dirty" money received from illicit activity and "cleaning" it in a way where criminals can use the money without fear of law enforcement tracing back where the money came from. This process consists of three stages: placement, layering, and integration. Placement is where criminals deposit their money into the legal financial system, which could be done in a variety of different ways. Criminals could exchange their cash for foreign currency, which allows them to mask the identity of their proceeds by mixing domestic and foreign banking systems. Criminals could also create front companies that are cash-intensive, making it easy for them to evade detection with large sums of cash. Or, criminals could split up their proceeds into smaller amounts and have multiple individuals deposit these cash amounts into a variety of accounts, which they can later transfer back into a personal account after the money is "cleaned". This is

called smurfing and structuring. Because these cash amounts are smaller, this avoids detection from banking systems in place to detect money laundering. The criminals only need to keep track of the accounts and layer the money in such a way that will reconcile all the money back into their personal accounts (Irwin, Choo, & Liu, 2012a).

Layering is the second stage of this money laundering process. In this stage, criminals seek to conceal the illicit origins of his money. In other words, once the money is placed in some sort of legal financial system, criminals can then move the money around in order to further mask where they actually obtained the money. They could do this by depositing money in multiple accounts both offshore and domestic, and constantly move the money around so it is unclear where the original money actually came from. This is especially challenging for law enforcement to track, especially if criminals used smurfing and structuring in the placement stage. Criminals could also falsify documents, such as invoices of fictitious sales or purchases that would justify large cash amounts or deposits. Sometimes during this stage, corruption comes into play, where criminals will take advantage of financial system employees, or even law enforcement, by paying them off to allow their transactions to go through. Finally, criminals could also begin layering their cash into a legal cash-intensive business, by slowly moving the money through the business. By doing this, criminals can incorporate their illegal proceeds into their legal proceeds from the legal front company they have created (Irwin, Choo, & Liu, 2012a).

The final stage in the money laundering process is integration. Here, the goal is for criminals to walk away with all the cash they started with, but now they can freely use this cash without worrying if the money could be traced back to their illicit activity. This is the stage where criminals often times put their money into real estate or buy luxurious items that are considered normal to purchase with cash. Integration is all about criminals being able to use their

"cleaned" money as if it were legally obtained. However, even with the precautions they took to layer their transactions to conceal the illicit origin, criminals should still spend wisely. This means they should not draw attention to themselves or their cash purchases because it may still alert law enforcement. With the banking system, it is also easier to track which accounts have transacted with other accounts because of the need for personal identification when opening bank accounts (Irwin, Choo, & Liu, 2012a).

In the same way that traditional money laundering goes through a three-step process of concealing origins and legitimizing illicit proceeds, so too does cryptolaundering. This time, however, it is easier and faster for criminals to go through the stages using cryptocurrencies. With the pseudo-anonymity bitcoin offers its users, criminals could take advantage of this system and use it to launder their criminal proceeds without having to worry about raising red flags at banks. While it is difficult to find bitcoin exchanges that will trade large sums of cash for bitcoin, it is not impossible. Typically, criminals wishing to launder their cash to bitcoin and back will look for bitcoin exchanges they trust to do such transactions. This sometimes requires a face-to-face meeting where the cash is exchanged and bitcoins will be transferred to the criminals' wallets. However, it is more common now for criminals to begin conducting their illicit business using bitcoin to save themselves the headache of having to convert the cash to bitcoin in the first place (Christopher, 2014).

In the placement stage for cryptolaundering, criminals would either deposit cash into bitcoin using local bitcoin exchanges that will accept large amounts of cash. Criminals could also have been making illicit business transactions using bitcoin in the first place, where their consumers would pay them in bitcoin for services or goods. For example, drug traffickers could sell their drugs on the darknet, which already requires the use of bitcoins to conceal all parties'

identities. By using currency exchanges and storing money in the form of bitcoin, this satisfies the placement stage of money laundering. It is similar to traditional money laundering where criminals exchange their money for foreign currency. In the layering stage, criminals could create several bitcoin accounts. Because bitcoin is fairly anonymous, it does not ask its users for personal identifiers, allowing them to hold as many bitcoin accounts as they would like. Criminals could use this to their advantage when layering the money. Seeing as bitcoin is only pseudo-anonymous because the blockchain publishes every transaction ever made between any and all bitcoin wallets, it would be wise to still participate in the layering stage of money laundering. Smart criminals would still take precautions to layer their transactions by having several accounts communicating with each other, to conceal their true origins. Finally, for the integration stage, criminals could either keep their illicit gains in bitcoin to make future transactions, or they could "cash out". What this means is that criminals would return to their local bitcoin exchanges where they originally submitted their cash, and would now exchange their bitcoins for whatever fiat currency they would like. Bitcoins can effectively reduce the amount of time it takes to "clean" the "dirty" money obtained from illicit activity (Christopher, 2014).

***Follow the Money*.** During the 1960s, drug usage dramatically increased among teens and young adults, which led conservative politicians in the United States to begin taking action by implementing drug control policies. In 1971 President Nixon formally declared a "war on drugs," which later spurred the international community to declare the same sort of war globally. This led to intense drug crackdowns and increases in incarceration rates worldwide; however, despite increased efforts by law enforcement in targeting drug offenses, drug crime was still on

the rise. Due to the seemingly failure of a globalized war on drugs, an alternative approach was adopted. This approach was dedicated to targeting the proceeds of drug crime in addition to continuing to target drug offenders. This led to money laundering formally being classified as a criminal offense in 1986 within the United States as per the Money Laundering Control Act, and in 1988 within the international community as per the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Jakubiec, Kilcer, & Sager, 2009).

Drug traffickers always need some way to integrate illegally obtained money back into the legal financial sector, and thus formed specific methods of money laundering, using the three stages of layering, placement, and integration. By adopting the "Follow the Money" approach to drug trafficking, policies began targeting the illegal proceeds of illicit activities as just another angle to cut off the flow of drugs internationally (Tang & Ai, 2010). The international community collectively created the Financial Action Task Force (FATF) to establish a global anti-money laundering (AML) policy that would regulate any member-state's financial sector to actively combat money laundering. The FATF describes money laundering as "the processing of…criminal proceeds to disguise their illegal origin" (FATF, 2014) and while its original purpose was to target drug trafficking specifically, the FATF has since began targeting the financing of terrorism, as a majority of terrorists organizations have been known to obtain their money through money laundering (Irwin, Choo, & Liu, 2012a).

However, the AML policy created by the FATF has not proven to be effective because one policy does not fit all states' needs. This failed attempt that the FATF had made in creating a global policy is what prompted researchers to address this issue of AML effectiveness, as well as to make suggestions for how the policy could be modified to improve effectiveness. Research studies has found that in order to increase AML policy effectiveness, AML laws need to be

created specifically towards each member-state[1] party to the FATF guidance because some states tend to be more vulnerable to money laundering than other states, given differences in political, social, and economic contexts. (Tang & Ai, 2010). Developing countries in particular tend to have a harder time enforcing AML policies or adjusting the laws to make them more effective within their own state. This suggests that money laundering tends to happen in places that have an inability to enforce the laws against it.

Developing countries tend to have "a vast size of informal economy…with the cash- and commodity-based nature of the economy" (Aluko & Bagheri, 2012). This informal economy poses a problem for the "one-size-fits-all" AML policies that are recommended by the FATF because the policies were geared toward formal economies that have complete control over their banking and financial sectors. With the informal economies that are common in developing states, a majority of financial transactions are happening outside of the realm of government oversight, which defeats the purpose of AML laws in the first place (Aluko & Bagheri, 2012). Based on the logic of Ferwerda (2008) in that it is more expensive for criminals to launder money in a state with more effective AML policies, it can be concluded that developing states, then, are more susceptible to money laundering because it would be less expensive for criminals to launder their money in these states. However, this could expand to more than just money laundering. Money laundering is only one aspect of the predicate crimes that precede it. By focusing on AML policies, it is a catchall way of combating all sorts of transnational crimes.

[1] The 35 FATF member states include: Argentina, Australia, Austria, Belgium, Brazil, Canada, China, Denmark, Finland, France, Germany, Greece, Hong Kong, Iceland, India, Ireland, Italy, Japan, Republic of Korea, Luxembourg, Malaysia, Mexico, Netherlands, New Zealand, Norway, Portugal, Russian Federation, Singapore, South Africa, Spain, Sweden, Switzerland, Turkey, United Kingdom, & the United States. (http://www.fatf-gafi.org/about/membersandobservers/)

It is important to stress that money laundering is more than its association to drug trafficking. Money laundering is a crime that covers the tracks of its predicate crimes. Without an initial crime being committed, there is no need to launder money. By targeting money laundering specifically, law enforcers can actually target the crimes that precede the stage of legitimizing of the money. Transnational crimes such as drug, human, arms, and wildlife trafficking all require their illegal proceeds to be legitimized. However, this process of legitimizing illegal proceeds is harmful to the global economy. Most importantly, criminals who get away with money laundering demonstrate that crime does pay, and it pays well. With success in money laundering, criminal enterprises will also find success in expanding their businesses. This expansion undermines legitimate businesses, making it more costly to stay within the bounds set out by specific governments. If it is more costly to remain a legal business, business owners may look to criminal activities to make up for the costs (Aluko & Bagheri, 2012).

With money laundering, there is always a certain degree of corruption attached; for example financial institutions turning a blind eye to suspicious activity. The use of financial institutions as a way to clean money for criminals undermines the entire financial sector of the state itself. Money laundering destabilizes economic policies

> …In different forms such as policy mistakes, due to measurement errors in national account statistics; volatility in exchange and interest rates due to unanticipated cross border transfers of funds; the threat of monetary instability due to unsound asset structures; effects on tax collection and public expenditure allocation due to misreporting of income; misallocation of resources due to distortions in asset and commodity prices; and contamination effects on legal transactions due to the perceived possibility of being associated with crime (Aluko & Bagheri, 2012).

Money laundering is not a victimless crime, but a crime that can actually raise national security risks with unstable financial institutions that have been used and abused by criminals to launder their money (Aluko & Bagheri, 2012).

Money laundering also has been known to have links with terrorism financing. The FATF (2008) describes terrorism financing as having two distinct requirements: "(1) funding specific terrorist operations, such as direct costs associated with specific operations and (2) broader organizational costs to develop and maintain an infrastructure of organizational support and to promote the ideology of a terrorist organization." The financing of terrorism can come either directly from the illegal proceeds of transnational crimes or from sponsors of these terrorist groups who can go one step further and actually launder the money for them. With this link between money laundering and terrorism financing comes a great need to disrupt this sort of funding. By cutting off these funds, terrorists cannot operate; if terrorists cannot operate, their groups will eventually disbanded (FATF, 2008).

These are only three of the major reasons why money laundering is harmful to the global economy and security. Fighting money laundering and watching criminal enterprise spending is crucial to learning how to dismantle their operations. Without the flow of money, no enterprise, armed group, nor organization can operate. This is why this research is imperative. However, this is not a traditional money laundering research study. Instead, it urges the evaluation of new technology being used to launder money and conduct criminal business, particularly the use of cryptocurrencies. AML policies, which have worked hard at trying to contain criminal exploitation of the financial sector, have been rendered futile when it comes to these currencies. No one individual, group, or government owns these currencies and they operate outside of all known regulatory bounds. They have complicated the job of AML policies and have only added

a new avenue for criminals to exploit in order to continue receiving the revenue from their illicit activities. This study looked at how criminals are using these cryptocurrencies and evaluated to what extent these cryptocurrencies were facilitating the execution of transnational crimes.

**Drug Trafficking.** Cryptocurrencies have been connected to darknet markets for several years now, where these marketplaces serve as the "Amazon" for all sorts of contraband, from various drugs to weapons to assassins to sexual services. It has been found that the most popular item on these illegal online marketplaces are illicit drugs, with a majority of these drugs being shipped from the United States (Maras, 2016). "English-speaking countries…and Western European countries…dominate the trafficking of illicit drugs on cryptomarkets while cannabis, stimulants (cocaine and amphetamines), ecstasy (MDMA) and psychedelics (NPS, LSD) are the main drugs offered" (Broseus, Rhumorbarbe, Morelato, Staehli, & Rossy, 2017). These marketplaces most likely require cryptocurrencies to be used on these sites to keep parties anonymous when purchasing these illegal products or services. The hardest part about these online marketplaces where people can buy illicit drugs is that the crime is two-fold. First, by operating on the darknet, law enforcers already have a difficult time locating these markets. Second, using cryptocurrencies offers even more protection to them because of the anonymity factor. The problem with these types of marketplaces is that even though law enforcement can take action to shut the site down, many more may open up afterward. This crime displacement poses a lot of problems for law enforcement, much like traditional drug trafficking. However, in the case of drug trafficking on these darknet markets, while they tend to represent traditional drug markets, cryptocurrencies can play a large role in lowering the costs of drug trafficking by hiding their transactions (Maras, 2016).

**Terrorism Financing.** Cryptocurrencies have also been tied to instances of terrorism financing. The FATF (2015) issued a report discussing the risks and threats of terrorism financing. It added a section specifically for virtual currencies and their connection with the financing of terrorism, noting the different aspects of virtual currencies that could be appealing to terrorists. Specifically, the report discusses that terrorists are funded through private donations, non-profit organizations, criminal activity, extorting local populations, kidnappings for ransom, commercial enterprises, and state sponsorship. Each method has its own set of challenges; however, the revenue generated from these activities must ultimately go to the terrorist organization. The report concludes that terrorists are using both physical, meaning personal couriers, and virtual, meaning cryptocurrencies, methods as means of obtaining the funds themselves (FATF, 2015). This money then has two purposes: "direct operational support," referring to specific terrorist operations that take planning and money to execute, and "broader organizational requirements," referring to such things as recruiting, paying recruits, support preexisting infrastructure, and market propaganda (FATF, 2008).

Salami (2017) notes that terrorists often commit other crimes to raise funds for their operations, such as kidnappings, drug trafficking, and bank heists. Traditionally, terrorists have been known to use the hawala system of laundering money, where it is the physical transfer of cash between sender, receiver, and many middlemen. After they commit these side crimes, the terrorists have to launder the money somehow; however, the hawala system has been known to be time consuming and risky when trying to move large sums of money quickly. With better access to the Internet, especially to promote propaganda, terrorists have been using cryptocurrencies to both launder the money they receive from the side crimes, but also as a way

for foreign donors to support them financially without repercussions from their home country government (Salami, 2017). Similarly, Irwin and Milad (2016) discuss the ways in which cash is very important to terrorist operations, where a digital form of cash is a more efficient way of sending and receiving money as a clandestine group. The researchers discuss the ways in which terrorists can utilize the virtual environment, whether through virtual worlds or virtual currency, to their advantage to conceal their identities, their crimes, and their donors. By operating outside of traditional law enforcement, terrorists can, to a certain extent, outsmart law enforcers by constantly breaking through borders via the Internet. Law enforcement has yet to figure out a way to cooperate effectively and share resources on the criminals that enter and leave their jurisdictions (Irwin & Milad, 2016).

On a different note, Irwin, Choo, & Liu (2012a) began a research initiative into creating typologies for money laundering and terrorism financing. Their research was directed at whether these crimes could work in virtual environments, particularly in Second Life and World of Warcraft, where users can actually use fiat money within these games. While this is not necessarily connected to cryptocurrencies, this research is relevant to understanding that money laundering and financing of terrorism has in fact moved online due to the ease of use and anonymity offered. The first part of their research outlines the different typologies and schemes that criminals can use to conceal their illicit proceeds from crime. The researchers find similarities and differences between money launderers and terrorist financers when using virtual worlds to transfer funds, noting that money launderers generally take more precaution when laundering the money through different online transactions (Irwin, Choo, & Liu, 2012a). The second part of their research discusses how their research is applicable to practitioners. They discuss the importance of the research and how it could be used as a way to call for the

international community to take a proactive stance on both crimes, seeing as they have both moved online. This practical application article is helpful for policymakers when looking at AML and counter-terrorism financing policies (Irwin, Choo, & Liu, 2012b). It is interesting, however, to see the differences in approaches that money launderers and terrorism financers have used in virtual worlds. This is perhaps because they have two different agendas: money laundering to conceal the proceeds from a predicate crime, and terrorism financing to fund terrorist operations through a number of avenues, not caring too much about remaining completely anonymous (Irwin, Choo, & Liu, 2012a).

While cryptocurrencies have their benefits and drawbacks, critics argue that the innovation of bitcoin technology that promotes a global free market and connects the globe financially is worth the risk because it helps a lot more people than it harms. However, it is hard to balance the fostering of an innovative piece of technology, while deterring the crime that unsurprisingly is attached to it. If there was a way to mitigate the harms from crime association, then cryptocurrencies would be a lot safer for its users. However, there is a gap in the literature that this study sought to fill in order to move ahead with mitigating the harms. It is the analysis of the role that cryptocurrencies play in facilitating transnational crimes, which is exactly what this research study aimed to do.

In sum, the review of literature suggests that (1) the type of cryptocurrencies, (2) the type of market for cryptocurrencies, (3) the opportunities they provide for disguising large amounts of money to be exchanged without identification, (4) the characteristic features of transactions, (5) individual or team networking operations, all are very important features in understanding the role of cryptocurrencies in facilitating transnational crime operations.

## The Present Study

This study sought to examine the role that cryptocurrencies play in relation to transnational crimes, particularly money laundering, drug trafficking, and terrorism financing. As mentioned before, there is a gap in the literature when it comes to studying cryptocurrencies. Many descriptive studies have been undertaken to show the process and describe the nature of cryptocurrencies; however, there is a need for a more detailed understanding of the role these currencies have in fueling transnational crimes. Currently, there is no empirical analysis of the cases and situations in which cryptocurrencies have been used to facilitate transnational crimes. Many studies already in literature focus on the most notable cases that involve cryptocurrencies with transnational crimes. However, this study went beyond that to study a variety of different cases, not just the handful that have been discussed in previous literature.

The purpose of this study was to examine a larger number of cryptocurrency cases that have been reported, both in the form of court cases and newspaper articles. One hundred cases were collected using secondary data means from around the world to develop trends and patterns among the cases. This study offers a new look at cryptocurrencies' relationship to transnational crimes specifically by analyzing a variety of cases of criminals either arrested or prosecuted on the grounds of transnational crime, with the use of cryptocurrencies during some part of the execution of the crime. This study looked past isolated and glamorized cases that are often cited in the literature and instead analyzed the role these currencies play particularly in the execution of these crimes against a variety of cases. This study aimed to:

1. Compile reported instances of cryptocurrencies being used in crimes of money laundering, terrorism financing, and drug trafficking.

2. Analyze qualitative data for the nature and patterns of the role of cryptocurrencies in money laundering, terrorism financing, and drug trafficking.
3. Quantify the qualitative data to examine similarities and differences between compiled cases.
4. Produce a publishable article or book chapter to submit to a peer-reviewed journal.

This research was designed to fill the current gap in literature in quantifying the qualitative data on reported cases of money laundering, drug trafficking, and terrorism financing, all with a cryptocurrency component. This design contributes to current literature because it offers an empirical base that goes beyond the current case studies in literature. Transnational criminals are rational beings who weigh the costs and benefits of committing the crime. With the benefits of efficiency and anonymity, criminals have deemed cryptocurrencies as a viable option to launder their illegal proceeds, or to even conduct their entire business with. Because criminals are exploiting this technological innovation to further their own schemes, it is imperative to find a solution to make it difficult, riskier, and less rewarding for criminals in using cryptocurrencies. However, this cannot be done without knowing the extent to which criminals are using these currencies.

With the improvement in technology comes the sophistication of criminals in making themselves harder to identify, much less find. This study has contributed recommendations towards the process of implementing effective strategies to take preventive measures as an international community in stopping transnational crimes to be facilitated by cryptocurrencies. Cryptocurrencies offer criminals easy access to launder money obtained illegally, as well as a way to remain under the radar of money laundering investigators who focus their energy solely on domestic financial institutions. The crimes that they commit and are able to get away with

when using cryptocurrencies have serious global impact that needs to be addressed. By understanding and establishing the role that cryptocurrencies have in fueling transnational crimes, it could then lead to further research on how to relieve crime association from cryptocurrencies. The results of this study further illustrate this phenomenon to draw attention to this nexus between cryptocurrencies and various transnational crimes.

## Theoretical Framework

The logic behind this study stems from environmental criminological theories. Today's ecology is heavily reliant on technology and the Internet because of its ease of use and speed. It seems that most of the world is connected via the Internet, and it would be naïve to assume that criminals were not taking advantage of the Internet in the same ways as law-abiding citizens. Crime has always been a part of the social ecology, which over the last several years, has had a larger presence over the Internet. Environmental crime does not study the criminal who commits crime, but rather the crime itself. It does not answer the question of "why" criminals commit crime, but rather "how" they commit crime. Environmental criminology assumes that the offender's immediate environment plays a primary role in the facilitation of crime. In other words, crime is generated by criminal opportunities, which present themselves in the immediate environment of offenders; the offender need only decide to commit the crime (Wortley & Mazerolle, 2008). However, this decision is a complex decision made up of cost-benefit calculations, as described by Rational Choice Theory.

Rational Choice Theory suggests that every person is a rational being, with the equal likelihood of committing crime. What this means is that crime is always a choice that is determined through hedonistic calculations by potential offenders. If the perceived costs of committing the crime are too high, the potential offender will refrain from offending. If the

perceived rewards are greater than the perceived costs, the potential offender will commit the crime presented. For every potential crime, individuals will calculate the benefits and risks of what could happen if the crime is committed. However, this calculation is different for every individual; some are more closely tied to the law, while others are more closely tied to selfish gain. In sum, when a crime opportunity presents itself, individuals will calculate the costs and benefits of committing the crime. The individual will always choose whichever option they believe is most likely to fall in their favor (Clarke & Cornish, 1985). In their research, Clarke & Cornish (1985) suggest that offenders' decision-making process in committing crime is a result of "rational and obvious responses to the pressures and opportunities of their particular circumstances." When crime presents itself, potential offenders are left with a life-changing decision to make. Clarke & Cornish (1985) make it clear too that this hedonistic calculation not only applies to the initial decision to commit a crime, but also to the decision to continue to commit the crime. They also found that by modelling offenders' decisions, policymakers can find better ways of controlling crime.

Clarke & Cornish (1985) also point out that there are different incentives and deterrents for specific crimes. The more specific crimes are operationalized, the better crime prevention policies will be at handling that particular crime. Criminals will use cryptocurrencies for different purposes dependent on the specific type of crime. For example, Irwin, Choo, & Liu (2012a) suggest that both money launderers and terrorism financers take different approaches to the crime, even though they essentially have the same goal: legitimatize and obtain large sums of money. However, what the researchers find is that money launderers tend to be more careful in taking precaution to make sure the origins of the funds are completely covered, whereas

financers of terrorists are less concerned with covering their tracks than they are with getting the funds to their destination quickly (Irwin, Choo, & Liu, 2012a).

When weighing the costs and benefits of committing a crime using cryptocurrencies, the currency can be useful for minimizing the costs and maximizing the benefits of committing the crime presented. This is what Rational Choice Theory suggests: that any individual seeks to gain pleasure and dispose of pain. Cryptocurrencies allow offenders to partake in traditionally riskier operations due to anonymity and decentralization, and leave with high monetary gains. Traditionally, there are many points of intervention where law enforcement can track transnational crime operations; however, with the use of cryptocurrencies, this crime trail has become more concealed in nature. This makes it harder for law enforcement to investigate and easier for criminals to get away with their actions, making the costs of being caught very low. This allows criminals to move large sums of money over the Internet almost anonymously. Anonymity coupled with a decentralized system makes for a nearly perfect crime situation where criminals can take advantage of the fact that law enforcement jurisdictions do not collaborate well. These features lower the costs of committing crimes using cryptocurrencies because offenders could potentially move all the money they want in one shot, without having to break up transactions to avoid detection. Offenders would need to learn how to cover their tracks on the blockchain by creating a situation where many accounts are involved in the transaction, making it harder for law enforcement to follow. Cryptocurrencies are also supposed to be easy enough to use for people with little computer knowledge, which helps because not all offenders are highly trained in computer science. With greater exposure to cryptocurrencies and other criminals who have used cryptocurrencies in their crimes, potential offenders may be more likely

to offend because of the environment they find themselves in and exposure to new techniques of evading detection.

Routine Activities Theory (Cohen & Felson, 1979) nicely complements Clarke & Cornish's (1985) work on Rational Choice Theory because it describes the environment where crime thrives. Cohen & Felson (1979) suggest that there are three main components to any given crime opportunity: (1) a likely offender, (2) a suitable target, and (3) the absence of a capable guardian. This theory assumes that crime happens when all three of these components converge. By understanding the routines of offenders and the convergence of the three components, Cohen & Felson (1979) believe this will help policymakers and law enforcement find points of intervention to better control crime.

With cryptocurrencies, a likely offender could be anyone with a need to launder or move money, the suitable target is using cryptocurrencies because of the anonymity it offers and its decentralized nature, and the absence of a capable guardian is the lack of oversight that any government has over these currencies. With this convergence, crime is more than likely happening on online environments that offenders frequent. Online environments, including chats, games, forums, markets, and the darknet in general, offer even more "offender convergence settings" which is different than what it had been from places like the local bar or restaurant, because offenders can meet up at any time over the Internet (Wortley & Mazerolle, 2008). Here criminals can share their techniques and operations with a much larger crowd, which allows for social learning to thrive. With the Internet "the world becomes smaller, and it's much easier for 'rare' offenders to find suitable co-offenders" (Kleemans, Soudijn, & Weenink, 2012). Criminals are learning from one another, and by seeing the rise in popularity of cryptocurrencies and the media releases about how criminals have been getting away with their crimes using

cryptocurrencies, more potential offenders are becoming interested in how they could utilize the currency for their own gain. This is especially alarming considering these online environments can create subcultures of offenders who work together to carry out their crimes, yet they may not actually know who the other is. The lack of capable guardians on these online environments only allow criminality to thrive and be seen as a norm. With this growing norm of criminality online, criminals will more likely commit crimes in a manner they trust and are comfortable with, considering not every criminal has a degree in computer science. With more exposure to cryptocurrencies whether from the media or other criminals on online environments, potential criminals will begin to see the worth that cryptocurrencies offer, especially considering criminals are always trying to find new ways to launder or move their illicit proceeds undetected (Maras, 2016).

However, it is not enough to simply study the rational choices and routines of offenders in preventing crime. Cornish's (1994) Crime Script Analysis focuses on specifically understanding the procedural aspects and requirements for any given crime. He uses this step-by-step script to analyze the trends and routines of offenders in order to pinpoint exactly where law enforcement can intervene to make the crimes more costly to commit. For example, with drug trafficking, by using the Follow the Money technique, law enforcement were able to attack traffickers' illicit proceeds, making it costlier for the traffickers to sell drugs and profit from it. By using these crime scripts, law enforcement can not only intervene, but they can also proactively plan for interventions, where they can make it more costly to commit crimes before the crimes are even committed. Cornish's (1994) idea on Crime Script Analysis added to the development of Clarke's (1995) Situational Crime Prevention techniques. The purpose of these techniques is to increase costs and reduce rewards of crime. Clarke (1995) emphasizes the

importance of not merely displacing crime, but preventing it altogether. In order for this to occur, Situational Crime Prevention techniques need to be crime specific to increase the effectiveness of deterring particular modus operandi among offenders. These techniques are aimed at reducing crime opportunities and hardening targets, removing the vulnerability of targets and incentives for potential offenders.

Building off these ideas, Cornish & Clarke (2002) came together in applying their theories to organized crime and how policies can be preventative. They found organized crime to be "highly planned and organized" and directed by determined offenders, making them prime examples of Rational Choice Theory. With organized crime come great economic motivations. Cornish & Clarke (2002) looked at the opportunity structures for various organized crime situations and developed 25 techniques for Situational Crime Prevention. Within these 25 techniques are five themes of: (1) increasing effort, (2) increasing risks, (3) reducing rewards, (4) reducing provocation, and (5) removing excuses. These themes are targeting aspects of crime environments making it more costly to commit crime, and eliminating the need for understanding "why" criminals commit crime in creating policy. According to Cornish & Clarke (2002) these are the ways in which policies can effectively control behavior.

Because specific crimes have specific crime patterns, by understanding these crime patterns, it will help identify points of intervention in order to reduce that particular crime. As Cornish (1994) points out, this is particularly helpful when crime script analysis is used to target areas that may reduce crime. "With crime scripts, knowledge is ascertained about specific procedural aspects and procedural requirements of a crime by overcoming presumed routinization around certain criminal acts" (Gilmour, 2014). With learning specific procedures criminals use in order to carry out their crimes, points of intervention can be identified allowing

for more effective prevention tactics to be used. This is important to study because even though typologies for money laundering, drug trafficking, and terrorism financing have been published and are useful for policymakers, Crime Script Analysis allows for a more in-depth analysis of the particular tactics criminals are using in order to carry out their crimes. It maps out every decision offenders have when committing the crime and ways in which they choose to remain undetected in order for them to continue committing crime (Clarke, 1994). In his research, Gilmour (2014) stresses the attractiveness of cash intensive businesses for criminals to launder their money. This is because the business could be both legitimate and illegitimate, and is an easy way for criminals to launder their money by layering their illicit funds with the legitimate cash received at the legitimate cash intensive business (Gilmour, 2014). With cryptocurrencies, seeing as they operate very similar to cash, this is particularly attractive for criminals. If criminals are already choosing to operate heavily in cash intensive areas, why not use a digitalized version of cash and reach an even wider consumer base that does not have to be restricted by geography. By analyzing the procedures through which criminals launder or move money via cryptocurrencies, it makes Situational Crime Prevention an ideal option for policy makers when trying to prevent cryptocurrencies from being used to facilitate crimes. By targeting the abuses of cryptocurrencies for specific crimes, it will hopefully reduce the crime associated with them and give credibility back to them, to allow them to thrive as currency particularly in the places that need it the most (Clarke & Cornish, 1985).

The policy implications for environmental criminological theories would be to employ Situational Crime Prevention measures, aiming to make crime more difficult, risker, and less rewarding for offenders. This means that in order to reduce crime, there has to be a reduction in criminal opportunities. In order to accomplish this, there needs to be a change in the environment

of individual offenders to make crime more unattractive. However, there is the issue of the transnationality of cryptocurrencies, where Situational Crime Prevention tactics have to be uniform across the globe in order to make using cryptocurrencies as costly as possible for potential offenders. Traditionally Situational Crime Prevention with financial crimes tended towards strengthening AML policies or closely monitoring financial institutions to make sure they are identifying suspicious activity. However, with the transnationality of cryptocurrencies, it is not as simple considering each state has their own way of conducting their financial sectors as well as defining cryptocurrencies. Even with these challenges, it does not make Situational Crime Prevention obsolete. In fact, it is just the opposite. What the international community needs to focus on is making these crimes costlier; however this will require coordination and cooperation between states.

Overall, the Situational Crime Prevention approach is essential for coming up with immediate and practical solutions that will target cryptocurrencies by making them costlier to potential offenders to use to facilitate their crimes. An in-depth understanding of how crime was committed for specific crimes will help finding points of intervention, which is what this study aimed to accomplish (Clarke, 1995). By analyzing the different roles of cryptocurrencies, trends and patterns were pulled out to help understand how the criminals are using the currency. With this in mind, research can be done in trying to take preventive measures to make cryptocurrencies less attractive options for criminals to take. This would allow for a decrease in the crime association connected to cryptocurrencies, which could help stabilize the price volatility, making it a currency that can compete in the global financial arena.

# Methods

## Research Design

This descriptive, exploratory research gathered 100 court cases and newspaper articles, examining the different ways in which cryptocurrencies facilitate transnational crimes, particularly four crimes: money laundering, drug trafficking, money laundering and drug trafficking together, and terrorism financing. Using both qualitative and quantitative data, this study examined the nature and patterns between and among the cases. This mixed methods strategy is to answer the research questions (see below) and assess the extent cryptocurrencies could facilitate transnational crimes.

While the quantitative analysis will help compare specific variables including the demographics of operators, the type of cryptocurrencies used, the type of markets utilized, the amount received from operations, the qualitative analysis has developed many themes for understanding the nature and patterns of transnational cryptolaundering and illicit drug sales operations.

## Research Question

The research question for this research study is: Do cryptocurrencies facilitate transnational crimes? If so, in what ways? What are the criminal opportunities that exist in the cyber world promoting illegal operations via cryptocurrencies and what can we do to prevent and control these transnational activities? Answering these questions will help contribute to the growing knowledge about the relation between cryptocurrencies and money laundering, drug trafficking, and terrorism financing. This is an imperative research study in understanding this relationship and how cryptocurrencies are being used to further crime. No research study has

before looked at a large number of cases like this, so this study complements current literature in understanding the criminality associated with cryptocurrencies. This research study could also help develop hypotheses for further research into this phenomenon.

**Data Collection Methods**

Using secondary data sources, data were collected by compiling relevant court cases and newspaper articles. Because a few prominent cases are touched upon in literature, the literature is lacking in examining a variety of cases. Data were gathered and systematically organized to 100 cases of reported instances of cryptocurrencies being used to facilitate transnational crimes. The cases collected ranged from 2004 to 2018. While any language was included in the search criteria, all cases were either in English, or had English translations. It was a convenience sample of cases where all the instances of transnational crime using cryptocurrencies researched were recorded and capped at 100, meaning the first 100 cases to be found were the ones that were used. It is also important to note that if there were cases with sufficient information about co-offenders, each co-offender counted as its own case. For example, a father-son duo participating in drug trafficking, they would count as two separate cases. With every case, there is only one offender, however there may be multiple offenders involved in the same crime, yet they were treated as separate cases in this study. Due to the variety of data sources, relative newness of the topic, and the inability to collect standardized forms of information, it is important to have some form of compilation and standardization of the secondary data that was used. In addition, as this is an exploratory research study, conducting an experiment would be premature and conducting interviews to collect primary data would be difficult. This method of collecting, compiling, and

quantifying the qualitative data found in the court cases and newspaper articles was the best way of creating an empirical study from the qualitative data.

In order to compile relevant court cases and newspaper articles, the databases used in the search included: Lexis Nexis, John Jay OneSearch library search engine, and Google. Search terms used included: virtual currency, digital currency, digital cash, electronic cash, electronic money, cryptocurrency, bitcoin, money laundering, online money laundering, cryptolaundering, terrorism, terrorism financing, terrorism funding, drug trafficking, drug trade, drug markets, and darknet drugs. This compilation is all publicly available and accessible, which does not require data management because confidentiality and anonymity of participant information are not issues with this study. No human subjects were used in the collection of this data; only secondary sources were used.

**Data Analysis**

An in-depth analysis of 100 cases on cryptocurrencies and money laundering, drug trafficking, and terrorism financing was undertaken. By quantifying the qualitative data, it has also enhance the systematic selection of identifying the patterns and features across all collected cases. This will allow the researcher to compare and contrast the trends and characteristics for further implications. The unit of analysis will be court cases and newspaper articles regarding transnational crimes, such as money laundering, drug trafficking, and terrorism financing, with a cryptocurrency component to the crime itself.

***Quantitative Data.*** First the qualitative data was transferred to quantitative data by coding information for the newspaper articles and court cases. Data were then entered into SPSS for a

descriptive statistical analysis. First, a univariate analysis was undertaken to examine the frequency distribution of variables. Percentages were calculated and analyzed. Then a bivariate analysis was undertaken to examine and explain the significant relationship between the cryptocurrency use and transnational crime variables. Detailed analysis is discussed in the Data Analyses and Findings Section. Variables were coded using a codebook, which can be found in Appendix B. It is important to note that since cases involving bitcoin are more plentiful than other cryptocurrencies, the study focused on bitcoin cases for detailed analysis. In cases where multiple cryptocurrencies were used in facilitation of the crime, if bitcoin was listed as one of them, the case was coded as a bitcoin case, even though there might have been other cryptocurrencies involved. This was relevant for only two cases.

***Qualitative Data.*** Since the newspaper articles and court cases are qualitative in nature, a content analysis was performed in identifying specific themes in understanding the cryptocurrencies use in transnational crime activities. Qualitative data analysis was aimed at developing hypotheses about cryptocurrencies and their role in transnational crime activities.

This study heavily relied on the qualitative data compiled from a variety of secondary sources. NVIVO, a qualitative software was used to organize, systematize, and draw connections among the cases. After reading through all the cases, themes were identified. Twenty pointers were derived and were grouped under six major themes. In the Data Analyses and Findings Section, these themes are discussed in detail with relevant cases to provide examples.

**Ethical Concerns**

No ethical concerns are prevalent because data is publicly available and accessible, meaning there is no need for anonymity. There was no usage of human subjects for this proposed study. Nevertheless, the researcher has cited all data sources used to protect the ownership of the secondary data collected.

**Limitations**

Limitations with this study are primarily regarding the generalizations of the findings of this study. The cases are not random. The convience sampling does not allow the findings to be generalized. However, this is an exploratory study to learn about the recent development in the cyber world that has implications for illegal transnational activities. There is a limitation of information, where some cases may have more information readily available than others, which creates issues for quantitative analysis. The qualitative analysis nicely complements the quantitative analysis in an attempt to correct these issues.

Secondly, obtaining 100 cases themselves was a challenge. There are not very many sources that report transnational crimes with the use of cryptocurrencies. This could be due to the vagueness in laws around the world relating to cryptocurrencies. States may either be hesitant to charge criminals who use these currencies or many not even have the resources to investigate such crimes committed. However, even though these crimes may not be reported, it does not indicate that these crimes committed using cryptocurrencies are not occurring. These crimes are not exempt from the dark figure of crime, where reported crime is only a minority of all crimes committed. It even becomes a smaller percentage when cases go to trial. Because of this dark figure, it can only be assumed that these crimes may be occurring at a higher rate than this study

is reporting. Regardless, this study offers insight into how criminals are using these currencies to carry out their transnational crimes.

Thirdly, much along the same lines, different states view cryptocurrencies differently, which may cause problems in identifying cases. It may be considered money laundering in one state, but it may be considered tax evasion in another. As with all transnational crime data, this presents cross-country data systematization challenges. Adapting search terms to locate all available cases reporting individuals using cryptocurrencies to carry out crimes was used to help mitigate the issues of cross-country data systematization. Further, currency amounts were all converted to American dollars to have stated currency amounts standardized as well.

However, despite these challenges, this exploratory research will complement previous literature nicely by adding an empirical component to studying the relationship between cryptocurrencies and money laundering, terrorism, and drug trafficking. Transnational crimes in general are difficult to study because their illicit activities, and perhaps criminal partners, transcend borders where law enforcement cannot as easily cross these same borders. Yet, this does not make studying these crimes and how they are committed any less important. This research is imperative to understanding the role that cryptocurrencies play in facilitating transnational crimes.

## Data Analyses and Findings

Using data collected through secondary sources, this study examines the role of cryptocurrencies in transnational crime activities. Quantitative data analysis describes the characteristic features of the cases and the relationship between the variables. These variables include: (1) year of arrest; (2) type of market, meaning the type of services being offered, for example money laundering services through currency exchanges or drug sales through multiple

drug markets; (3) gender of offender; (4) age of offender; (5) individual or team, meaning how many coconspirators were involved in the scheme; (6) nationality, (7) region of arrest, meaning the continent the offender was arrested; (8) type of court, whether American or foreign; (9) cryptocurrency type; (10) how the crypto currencies were used, for example used in exchange for cash or in exchange for drugs; (11) operation amount, meaning how much was made in the duration of the scheme; and (12) the type of crime, whether money laundering, drug trafficking, money laundering and drug trafficking combined, and terrorism financing. These variables are listed in the Code Book in Appendix B. Both qualitative and quantitative analyses were performed and the results are described below.

**Quantitative Analyses**

The quantitative data describes the characteristic features of the cases. In order to describe the scenario of these cases, a frequency was run on all variables (see Table 1). Of the offenders included in this study, a majority of them were males, making up 92% of cases, and were between the ages of 20 and 39, making up 67% of cases. The most common type of crime linked with cryptocurrencies was found to be drug trafficking at 45% of cases, followed by money laundering at 29% of cases, money laundering and drug trafficking combined at 20% of cases, and terrorism financing at 6% of cases. With drug trafficking being the largest percentage of cases for crime type, it was also found that single drug markets were used 36% of the time, followed by multiple drug markets at 30% and currency exchanges at 25%. Finally, 86% of offenders used bitcoins and the other 14% were made up of a variety of different cryptocurrencies, including PayPal, OneCoin, ZufloCoin, e-gold, Web Money, Liberty Reserve,

and other unspecified alt coins. Table 1 provides a description of the cases by age, gender, type of transnational crime, cryptocurrency type, type of market, and operation amount.

**Table 1. Description of Cases (N=100)**

| Variables | N | % |
|---|---|---|
| **Age** | | |
| 15 to 19 | 2 | 2 |
| 20 to 29 | 32 | 32 |
| 30 to 39 | 35 | 35 |
| 40 to 39 | 17 | 17 |
| 50 to 59 | 8 | 8 |
| Age Unknown | 6 | 6 |
| **Gender** | | |
| Male | 92 | 92 |
| Female | 8 | 8 |
| **Individual or Team Network** | | |
| Individual | 35 | 35 |
| Team | 65 | 65 |
| **Type of Transnational Crime** | | |
| Money Laundering | 29 | 29 |
| Drug Trafficking | 45 | 45 |
| Money Laundering & Drug Trafficking | 20 | 20 |
| Terrorism Financing | 6 | 6 |
| **Type of Cryptocurrency** | | |
| Bitcoin | 86 | 86 |
| Other | 14 | 14 |
| **Type of Market** | | |
| Single Drug Market | 36 | 36 |
| Multiple Drug Markets | 30 | 30 |
| Currency Exchange | 25 | 25 |
| Other | 9 | 9 |
| **Operation Amount** | | |
| Less than $100,000 | 13 | 13 |
| $100,000 to $999,999 | 33 | 33 |
| $1 million to $999 million | 40 | 40 |
| $1 billion or greater | 9 | 9 |
| Operation Amount Unknown | 5 | 5 |

## Bivariate Analyses

Bivariate analyses were undertaken to examine if there are significant differences between the type of transnational crime, the cryptocurrency use variables, and demographic

characteristics of those transnational crime operations. Since all the variables are nominal, a Chi-Square test was used; this is a nonparametric test used to compare data.

Chi-Square analyses were undertaken to test for significant relationships between the transnational crime type variable including money laundering and drug trafficking cases only. Because money laundering cases and drug trafficking cases make up a majority of cases at 94%, a Chi-Square analysis was only performed on these 94 cases. For the purposes of this analysis, money laundering used by drug trafficking networks and other illegal operations were combined and recoded to form one category of money laundering. This variable was then compared to drug trafficking sales, meaning the exchange of buying and selling drugs using cryptocurrencies. Essentially, one category involves money laundering (N=49) and the other does not (N=45). Terrorism financing cases were not used for this analysis. It was found that relationship to the variables for year of arrest, age, and court type were insignificant when tested against crime type. This suggests crimes facilitated by cryptocurrencies are happening all over the world and across all age groups, consistently over the years. Relationships to the variables for gender and whether the crime was committed with a team or as an individual were also found to be insignificant, indicating that these crimes are being committed by groups of people as well as individuals, both male and female. However, variables for market affiliation type [$\chi^2(3)=48.17$, $p<.01$], nationality [$\chi^2(3)=8.92$, $p>.05$], arrest region [$\chi^2(3)=8.84$, $p<.05$], cryptocurrency type [$\chi^2(1)=11.44$, $p<.01$], cryptocurrency use [$\chi^2(3)=63.95$, $p<.01$], and operation amount [$\chi^2(3)=15.86$, $p<.01$] were all found to have significant relationships with the crime types of money laundering and drug trafficking. What this indicates is that market affiliations, nationality, arrest region, cryptocurrency type, cryptocurrency use, and operation amounts are all significantly different depending on the crime committed.

The three variables of cryptocurrency type, cryptocurrency use, and operation amount were further looked at in how they operate differently depending on the crime. Because these three variables had a significant Chi-Square, this indicates there are significant differences in the way criminals use the three variables in money laundering and illicit drug sales. For both crimes, offenders tend to rely on bitcoin than other cryptocurrencies, most likely due to its popularity. However, depending on whether an offender is committing money laundering or drug trafficking will determine how they use the cryptocurrency to facilitate their crimes. With money laundering, often times their transactions will be exchanging cash for cryptocurrencies and later will "cash out" their clients. For drug sales, offenders will exchange cryptocurrencies as transactions for services or products.

It has also been found that money laundering lends to more crime opportunities, thus higher dollar amount schemes. Operation amounts were found to be higher in money laundering cases than with drug trafficking cases, yet bitcoins were the favored currency in both crimes. With this analysis, money laundering seems to be the most feasible crime to be committed with cryptocurrencies because of its ability to evade detection and to gain high commissions off of this type of business. This makes sense considering money laundering will use more money in transactions, so operation amounts will already be higher than that of drug trafficking. There is also less contact with average people, where money launderers do not have to worry about the collateral damage of overdoses, as do drug traffickers. All Chi-Square findings be found below in Table 2.

**Table 2. Bivariate Analyses**

| | Drug Trafficking ONLY (N=45) | | Money Laundering & Money Laundering/Drug Trafficking (N=49) | |
|---|---|---|---|---|
| **Variable** | **N** | **%** | **N** | **%** |
| **Cryptocurrency Use **** | 45 | 47.9 | 49 | 52.1 |
| Cryptocurrencies for cash; vice versa | 0 | 0.0 | 15 | 16.0 |
| Transactions made using cryptocurrencies | 45 | 47.9 | 9 | 9.6 |
| Cryptocurrencies for cash; Transactions made using cryptocurrencies | 0 | 0.0 | 12 | 12.8 |
| Theft of cryptocurrencies with the potential to launder | 0 | 0.0 | 3 | 13.8 |
| **Operation Amount **** | 43 | 47.8 | 47 | 52.2 |
| Less than $100,000 | 10 | 11.1 | 1 | 1.1 |
| $100,000 to $999,999 | 16 | 17.8 | 15 | 16.7 |
| $1 million to $999 million | 16 | 17.8 | 23 | 25.6 |
| $1 billion or greater | 1 | 1.1 | 8 | 8.9 |
| **Year** | 45 | 47.9 | 49 | 52.1 |
| 2012 or prior | 0 | 0.0 | 6 | 6.4 |
| 2013 | 5 | 5.3 | 2 | 2.1 |
| 2014 | 7 | 7.4 | 5 | 5.3 |
| 2015 | 6 | 6.4 | 9 | 9.6 |
| 2016 | 7 | 7.4 | 5 | 5.3 |
| 2017 | 18 | 19.1 | 21 | 22.3 |
| 2018 | 2 | 2.1 | 1 | 1.1 |
| **Company Affiliation **** | 45 | 47.9 | 49 | 52.1 |
| Single drug market | 10 | 27.7 | 26 | 10.6 |
| Multiple drug markets | 11 | 20.2 | 19 | 11.7 |
| Currency exchanges | 25 | 0.0 | 0 | 26.6 |
| Other | 3 | 0.0 | 0 | 3.2 |
| **Gender** | 45 | 47.9 | 49 | 52.1 |
| Male | 40 | 42.6 | 48 | 51.1 |
| Female | 5 | 5.3 | 1 | 1.1 |
| **Age** | 45 | 47.9 | 49 | 52.1 |
| 15 to 19 | 1 | 1.1 | 0 | 0.0 |
| 20 to 29 | 16 | 17.0 | 15 | 16.0 |
| 30 to 39 | 16 | 17.0 | 17 | 18.1 |
| 40 to 49 | 7 | 7.4 | 9 | 9.6 |
| 50 to 59 | 3 | 3.2 | 5 | 5.3 |
| Age Unknown | 2 | 2.1 | 3 | 3.2 |
| **Co-Conspirators** | 45 | 47.9 | 49 | 52.1 |
| Individual | 17 | 18.1 | 14 | 14.9 |
| Team | 28 | 29.8 | 35 | 37.2 |
| **Nationality **** | 45 | 47.9 | 49 | 52.1 |
| North American | 24 | 25.5 | 31 | 33.0 |
| European | 10 | 10.6 | 15 | 16.0 |
| Asian | 7 | 7.4 | 3 | 3.2 |
| Australian | 4 | 4.3 | 0 | 0.0 |
| **Arrest Region **** | 45 | 47.9 | 49 | 52.1 |
| North America | 27 | 28.7 | 36 | 38.3 |
| Europe | 7 | 7.4 | 10 | 10.6 |
| Australia | 7 | 7.4 | 3 | 3.2 |
| Asia | 4 | 4.3 | 0 | 0.0 |
| **Court** | 45 | 47.9 | 49 | 52.1 |

| | | | | |
|---|---|---|---|---|
| U.S. courts | 26 | 27.7 | 37 | 39.4 |
| Foreign court | 19 | 20.2 | 12 | 12.8 |
| **Type of Cryptocurrency **** | 45 | 47.9 | 49 | 52.1 |
| Bitcoin | 45 | 47.9 | 38 | 40.4 |
| Other | 0 | 0.0 | 11 | 11.7 |

** Chi Square values significant at .05 level

In sum, the bivariate results indicate that the use of cryptocurrencies differs depending on the type of crime potential offenders are trying to undertake. With the crime opportunities cryptocurrencies offer to money laundering, these offenders will benefit more than offenders who are simply drug trafficking on the darknet, without any connection to money laundering. This is an important finding of this study because it demonstrates that crime using cryptocurrencies does pay when it is in connection to money laundering. It was also clear that between money laundering and drug trafficking, bitcoin seemed to be the preferred cryptocurrency. This could be for a number of different reasons, for example, law enforcement could be focusing on stopping bitcoin-related crimes and not focusing so much on other alt coins. Another reason could be that criminals do not want to use lesser known cryptocurrencies out of fear that they could be Ponzi schemes, whereas bitcoin has been known to be reliable in terms of its algorithm, drawing criminals to bitcoin. Either way, the quantitative results indicates that these crimes are happening, where criminals are gaining lots of money and have a safe way to launder that money.

## Content Analysis of Qualitative Data

While the quantitative analysis helped compare the transnational crimes and the use of cryptocurrencies, the content analysis of the cases interpreted the quantitative analysis and also to identified concepts that emerged for developing and testing hypotheses on the use of cryptocurrencies. The content analysis of cases rendered six common themes with 20 specific

pointers. These themes justify the hypotheses about cryptocurrencies and their role in assisting transnational crime, which are significant elements in grounded theory. Listed below are the themes developed along with cases that describe each of the 20 pointers.

**Theme 1: Criminals use the darknet to buy and sell drugs**

Since drug trafficking cases were the most plentiful out of the 100 cases compiled, it was clear to see that the darknet is where many of these drug transactions were happening. The reason cryptocurrencies are connected to the darknet in this way is because many of these darknet marketplaces that sell drugs will require all users, both consumers and vendors, to use bitcoin, or another form of cryptocurrency, to make all transactions. This is to protect both buyer and seller from being personally identified.

***Types of Darknet Marketplaces Used.*** When compiling the data, there were a variety of darknet marketplaces and websites connected with using bitcoin as its primary form of currency for any transaction. These sites included: the Silk Road, AlphaBay, the Silk Road 2.0, Sheep Marketplace, Agora, Hansa, Nucleus, Pandora, Abraxas, Shiny Flakes, Black Bank, and Evolution. Out of these sites, administrators for five sites were included in this study as arrested and/or prosecuted for their involvement in allowing such transactions under their supervision. While each site is unique, their general purpose is the same: to facilitate the trafficking of illegal goods particularly, for the purposes of this study, illegal drugs. These darknet marketplaces and sites allow drug vendors to have a broader consumer base than if they were to sell drugs locally. With the darknet, vendors can ship their illegal drugs both domestically and internationally,

reaching people all over the world. The darknet also allows these vendors to evade detection, especially with the requirement of the use of bitcoin to make any and all transactions.

***Evolving Nature of Darknet Marketplaces.*** With activities occurring on the darknet, law enforcement has a hard time identifying who these darknet site administrators are. Even when law enforcement can finally make an arrest on one of these administrators, it is very easy for another individual to start his own darknet marketplace. It would merely replace the one that law enforcement had just shut down. The cases below, in Boxes 1, 2, and 3, describe how regardless of how popular a darknet drug market is, there will always be a replacement should law enforcement find a way to shut one down. These marketplaces evolve and are becoming more and more resilient to law enforcement efforts in taking them down.

**Box 1: Case Study: Ross Ulbricht**. In 2011, Ross Ulbricht started his infamous darknet marketplace known as the Silk Road. This marketplace was the "Amazon" for criminals, where they could shop for drugs, weapons, and hitman services all in the same place. Ulbricht made it clear that bitcoins must be used in order to make any sale or purchase to conceal the identity of all Silk Road users. However, in 2013, Ulbricht's crimes caught up with him and he was sentenced to life in prison in 2015. By this time, another popular marketplace surfaced called AlphaBay, ran by Alexandre Cazes. Similar to the Silk Road, AlphaBay sold nearly identical merchandise and also required users to use bitcoins in order to continue evading detection.

**Box 2: Case Study: Alexandre Cazes**. Like Ulbricht, Cazes was arrested in 2017 for allowing illegal transactions to happen on his darknet marketplace site. However, Cazes was not even

sentenced, but was found to have committed suicide while in custody in Thailand after seeing the harsh sentence Ulbricht went through.

**Box 3: Case Study: Blake Benthall**. Still, regardless of law enforcement efforts to contain the issue of these two darknet marketplaces, Blake Benthall started his own darknet marketplace which he called the Silk Road 2.0. Again, this marketplace operated in a nearly identical manner as Silk Road and AlphaBay, offering the same sorts of services and also requiring bitcoins to be used for all transactions. Eventually Benthall was arrested and could be serving a similar sentence to that of Ulbricht.

***Use of Darknet and Bitcoin to Evade Detection***. These examples suggest that law enforcement will always be one step behind when it comes to darknet marketplaces that promote the usage of bitcoin. However, this could also suggest that law enforcement does have their ways in finding the administrators of such sites. While their work takes time and resources, this idea demonstrates that even criminals using the darknet in combination with bitcoin are not above the law. One thing is very clear from these examples, however. Darknet marketplaces, along with bitcoin, are constantly evolving in nature to better evade detection from law enforcement. They are becoming more and more resilient to law enforcement efforts, hence why law enforcement has caught so few of these site administrators. Once they catch one administrator, five more will just emerge in their place due to the supply and demand of the vendors and consumers that take advantage of these sites. So, yes, the efforts of law enforcement are not futile because they are actually catching some of these bitcoin using criminals. However, their efforts can only go so far if the supply and demand of illegal drugs on the darknet is still there.

***Diversification.*** With this idea of supply and demand, vendors will resist the urge to put all their eggs in one basket. They will choose to diversify their sales, meaning they will sell drugs on multiple darknet sites, which was reflected in the quantitative data, where nearly half of all market affiliated vendors were engaged in multiple markets. This allows their businesses to survive when law enforcement takes down the site administrators because then they could simply manage their other sales on other illicit platforms. This diversification allows vendors to float from one darknet marketplace to another, especially considering each marketplace that sells illegal contraband is set up in nearly identical ways. With the support of quantitative data, it would seem unlikely that these criminals are only using one site to sell their drugs, instead of furthering their consumer base and securing their own businesses by engaging sales on multiple platforms. The case below, in Box 4, describes how drug vendors can "set up shop" on multiple marketplaces, allowing them a better chance of survival if one marketplace closes down.

**Box 4:** **Case Study: Bryan Lemons & William Farber.** After the Silk Road was shut down in 2013, Bryan Lemons and William Farber started selling their drugs on AlphaBay, accruing nearly $7 million in drug sales. They specialized in nine different drugs: marijuana, cocaine, oxycodone, hydrocodone, psilocybin, MDMA, LSD, Xanax, and ketamine, and had a drug lab located in Massachusetts. Authorities were able to link Lemons and Farber to their drug store on the Silk Road, and also were able to document their operations on AlphBay.

***Types of drugs sold.*** The most common types of drugs trafficked on these darknet sites seemed to be synthetic drugs. Among the 100 cases, fentanyl was the most commonly trafficked drug, with 19 instances, followed by cocaine, MDMA, heroin, LSD, methampthetamine,

cannabis, ecstasy, oxycodone, and others. It also is not a coincidence that these top drugs sold on these sites are also linked to various overdose cases around the world. It is through these overdoses that law enforcement was able to get a lead on tracking down these synthetic drug vendors. The danger with these drugs are that they are not regulated in anyway, so vendors could be putting poison in these drugs and no one would know, except for the mass of corpses that are left in their wake. By attacking these overdose cases, law enforcement can narrow their search and track down where the shipments were coming from, and ultimately who was selling the drugs. The case below, in Box 5, describes how overdosing led law enforcement to the direct supplier of the drugs sold online.

**Box 5:** **Case Study: Xiaobing Yan & Jian Zhang**. In the case of Xiaobing Yan and Jian Zhang, these two Chinese nationals were fentanyl producers selling the fentanyl to American suppliers. However, their mass produced fentanyl contained lethal levels, which led to at least four deaths in the United States. It was the investigation into these deaths that led authorities to Yan and Zhang, where they now have to answer to U.S. courts on charges on illegal dealing of fentanyl.

With other top drugs as cocaine and MDMA, it is also no surprise that these darknet drugs have also been linked to local nightclubs. These drugs could be purchased easily online and then easily distributed locally in the club scene. This is not very different from traditional drug trafficking. However, in this context where drugs are bought on the darknet with bitcoins, dealer identities are concealed and it allows for easy transactions, where anyone could potentially become a drug dealer in this way. The case below, in Box 6, describes how offenders can buy drugs online and distribute them locally through the nightclub scene.

**Box 6:** **Case Study: Kamal Kalara & Mahesh Goyal**. Kamal Kalara was a local DJ in Delhi and would often work at raves and nightclubs for a living. After meeting Mahesh Goyal, an ecstasy supplier, Kalara began a business with Goyal to purchase drugs off of the darknet and sell them at raves they would work together in order to liven up the party. However, interestingly, the Delhi police do not believe Kalara and Goyal met coincidentally. Instead they have a hunch that there is a larger figure at large connecting drug suppliers to the local nightclub scene to push drugs through the raves to make a profit all across India.

***Summary***. While not a surprising finding, this theme is what makes up a majority of all cases studied in this research study. Drug trafficking and cryptocurrencies were highly connected to evade detection from the police. They were the ideal currency to exchange because anyone can obtain cryptocurrencies and their identities were pretty much concealed from outsiders. Drug trafficking is a large business on the darknet and is only increasing in size with the presence of cryptocurrencies. Like traditional drug trafficking, displacement is an issue law enforcement is currently facing, where when one site administrator is taken down, others will rise up to take his place. It is a tedious game of cat and mouse, where law enforcement seems to always be on a defensive, rather on an offensive, against these drug trafficking cybercriminals.

**Theme 2: Networking and the division of labor**

Another theme that emerged in the qualitative analysis of the 100 cases was the theme of networking the division of labor. In traditional crime, division of labor is often a necessity to be efficient as a business. Cybercrime is no different, but it requires particular skill sets in order to

maintain a place within the group. These skill sets are important because if an individual does a job well, they are likely to land another job by word-of-mouth.

***Division of Labor.*** With traditional crime syndicates, there is always a division of labor in order for the syndicate to be efficient at the crimes they commit. This suggests each individual working as part of the operation has a particular role to play. What this means is there is no dead weight; everyone is pulling their share of the operation and will be compensated for such work. The same goes for cybercrime syndicates. The cases below, in Boxes 7 and 8, describe how cybercrime syndicates have specialized operators to help them carry out their schemes and are using cryptocurrencies in order to further these crime operations.

**Box 7:** **Case Study: Sergei Kirin**. In the case of Sergei Kirin, Vadim Polyakov set up a cybercrime operation that stole over $1 million worth of StubHub tickets from victims who actually purchased the tickets. His main goal was to steal these tickets and resell them online at a higher price. However, in order to reap the rewards of this scam, Polyakov needed a money laundering specialist. Due to his reputation, Kirin was a good addition to the operation based on his money laundering abilities. Kirin had very little to do with the operation in general outside of his specialty.

**Box 8:** **Case Study: Omar Dhanani**. Similarly, Omar Dhanani, was part of a cybercrime syndicate known as the Shadowcrew. This cybercrime syndicate was known for operating the trafficking of stolen credit card and bank account numbers on their online website. However, similar to Polyakov, Shadowcrew needed a money laundering specialist to “clean” their illicit

proceeds. That is where Omar Dhanani came into play. He was in charge of making wire transfers and exchanges of fiat currency to cryptocurrencies in order to thoroughly layer the money through several accounts to evade detection by law enforcement. Dhanani had very little to do with the stolen account and credit card numbers, yet was still an important asset to the operation.

***Familial Ties.*** Interestingly, family ties seemed to have been used in a good portion of the cases analyzed. Like the cybercrime syndicates, the family ties also have a division of labor, even though it may be more informal. Familial ties were probably utilized out of convenience and to avoid issues with trust. The cases below, in Boxes 9, 10, and 11, describe how families have bonded over their crime operations, where their accomplices are actually related to them.

**Box 9:** **Case Study: Michael & Philip Luciano**. In the case of Michael and Philip Luciano, a father-son duo, Michael, the father, would run the overall business of selling and distributing drugs on AlphaBay. Philip, on the other hand, probably more tech savvy than his father, would handle the transactions made over AlphaBay. He would manage the bitcoin wallet and see to it that his father prepares the packages to be delivered.

**Box 10:** **Case Study: Michael & Anthony Murgio**. In another case, Anthony Murgio and his father, Michael Murgio, ran a bitcoin exchange that would knowingly allowed criminals to launder their money through the exchange. Anthony was in charge of the bitcoin end of the business, while Michael Murgio was in charge of obtaining control over a credit union, where they would funnel money through and not report the transactions to the government. In the end,

Michael Murgio was sentenced to one-year probation for his supporting role in the operation, where his son was sentenced to five and a half years in prison for his lead role in the operation.

**Box 11: Case Study: Ramiz & Sedina Hodzic**. In addition, Ramiz and Sedina Hodzic are a Bosnian-American couple who helped funnel money through cryptocurrencies to then donate to terror groups. The couple would either send the money directly or would accept the money and they would then make purchases on behalf of these terror groups. The couple was working with a larger Bosnian terror-supporting group, and they were in charge of obtaining resources and money for the terror group. While these are only three examples of familial ties, there are other father-son duos, significant other duos, brother-brother duos, and even a mother-son duo involving a minor in illicit business transactions.

***Commissions.*** While quantitative results did not find a significant relationship between crime types and whether crimes were committed individually or with a team, a majority of the cases involved crimes committed as a team, at 65% of all cases. Regardless, these crimes are committed because with the use of the Internet, crimes have become easier to commit. When added with the use of bitcoins as well, it becomes less risky as well, which is attractive to potential criminals, considering the money operations at stake. With bitcoins, criminals can commit the same crimes they would traditionally, but now they have extra protection from being discovered by law enforcement, and they have a potential to make even more money. As described in the literature review, when criminals use bitcoins they can evade detection, easily move money, and even have a chance of making money, considering the price volatility in value for bitcoin, which is currently on the rise. The high commissions that are received from engaging

in various illegal operations are a huge attraction for criminals. The high commissions added with the security of evading detection all goes into the cost-benefit analysis these criminals engage in to determine if the crime is worth the costs. And in the case of bitcoin, these crimes are worth it when their commissions start rolling in. The case below, in Box 12, describes how crime does pay, and it pays well.

**Box 12: Case Study: Alexander Vinnik**. One of the highest operation amounts recorded amongst the cases was in the Alexander Vinnik case where he handled over $4 billion worth of bitcoin in transactions. Vinnik was the operator of a bitcoin exchange known as BTC-e. This exchange was known for its money laundering services and was advertised in such a way to gain criminal clientele, mostly because criminal clientele often will pay more for silence and loyalty. Vinnik was operating between 2011 and 2016, and was arrested in 2017. He had clientele from all over the world wanting to use his money laundering services by layering the money through several accounts. There were only a handful of cases that broke $1 billion, but these cases are most likely due to services they offer criminals, whether it is allowing them to buy and sell drugs at their convenience or offering money laundering services where they can get their money "cleaned" for a high a commission.

***Use of Middlemen.*** While cryptocurrencies allow perpetrators to work alone, there are certain times when middlemen are still used in cryptocurrency-facilitated crimes. Bitcoin exchanges serve as these middlemen that will convert cash into bitcoin or back into cash again. These exchanges assist vendors and money launderers by providing the cash needed for illicit businesses for them to "cash out," or for them to purchase more bitcoins. They are also

particularly useful to criminals when the exchanges would launder the illicit proceeds for them criminals. Bitcoin exchanges also assist consumers by allowing them to exchange their currency for bitcoin in order to make purchases on darknet marketplaces that only accept bitcoin. It is through these bitcoin exchange middlemen that crimes committed with bitcoin can be successful. The case below, in Box 13, describes how middlemen are essential in committing transnational crimes with cryptocurrencies.

**Box 13: Case Study: Charlie Shrem & Robert Faiella.** In Charlie Shrem's case, he ran a bitcoin exchange company, called BitIntant, that was linked to the Silk Road, which allowed anyone wanting to purchase or sell items on the Silk Road to exchange their money for bitcoin. Shrem also allowed people to exchange their bitcoins back for cash, which is exactly what Robert Faiella used him for. Shrem and Faiella had a working relationship, where Faiella would sell drugs on the Silk Road and return to Shrem to "cash out". Shrem knew where Faiella had gotten his money from, yet proceeded to cash him out regardless, without reporting such transaction. Shrem would even give Faiella discounts on the owed commission because his business was recurring. In this scenario, Shrem is the middleman, bridging the gap between darknet marketplace users and "cashing out."

***Summary***. When it comes to transnational crimes and working in a network, it was found that 65% of all cases involved offenders having at least one other person helping them with their schemes. With the Internet, criminals can easily meet each other online and have marketable skills that are needed for certain operations. However, with this new way of meeting people comes its own risks, where there may be a lack of loyalty because these individuals are not

connected in any other way than their operations. This could be the explaining factor as to why familial ties are so prevalent among the 100 cases. However, this could create issues because familial bonds may not have the specializations needed for a particular operation; they are simply the convenient choice for a partner. On the other hand, meeting people with specialized skills comes in handy when these skills are hard to come by. This online criminal networking has turned into its own subculture, where crime thrives, and criminals learn from each other; especially from each other's mistakes. These criminals continue with the risks involved with networking because of the high rewards to be gained.

**Theme 3: One crime provides opportunities for other crimes**

This was not an unexpected finding of this study, where one crime was found to provide opportunities for other crimes. It is clear that all crimes provide opportunities for money laundering because there needs to be a way to "clean" illicit proceeds; it does not, however, always indicate that other crimes may be linked as well. These crimes range beyond the crimes studied in this research, from identity theft to corruption to hacking. They covers a wide variety of crimes that would be interesting to look into: which crimes offer opportunities for other crimes.

***Corruption.*** Just as with traditional transnational crimes, transnational crimes committed using cryptocurrencies are not immune to corruption, even though it probably happens at lower rates. Because cryptocurrencies eliminate the intrusion of banks in personal transactions, there is no need for banks or law enforcement to turn the other way because there is no system that is raising red flags. However, what is revealed in these cases is that corruption happens in pursuit

of greed. As discussed earlier, there are extremely high commissions for people engaging in crimes using cryptocurrencies. Even law enforcement is not immune to the feeling of wanting more. The case below, in Box 14, describes how even law enforcers themselves can be sucked into the high reward operations cryptocurrencies allow.

**Box 14: Case Study: Shaun Bridges & Carl Force**. In the cases of Shaun Bridges and Carl Force, these are good examples of dirty law enforcement officers who recognized the value of bitcoin in facilitating crimes, especially the perception of anonymity it provides. Bridges, former Secret Service, and Force, former DEA, were working a joint case looking into the crimes of Ross Ulbricht, the creator of the Silk Road darknet marketplace. While doing their jobs, these two agents were swept up into the attractiveness of bitcoin and the high commissions that come from transacting with them. They found themselves apart of Ulbricht's scheme and were in it for the quick and easy paycheck. In the end, both made hundreds of thousands of dollars, but shortly after, were arrested and sentenced to several years in prison. It was the way in which Ulbricht conducted business, so easily, through the use of bitcoins that attracted Bridges and Force in the first place. Their judgments were clouded by greed, and they are paying for their missteps.

***Misappropriation of Client Money.*** With the rising popularity of bitcoin and its overall success in being an experimental currency, more have become drawn to using cryptocurrencies. Even though bitcoin is the most popular form, other users have been experimenting with other lesser-known cryptocurrencies. However, with these currencies comes their own set of risks. There are currencies that mimic the algorithm of bitcoin, but do not have all the features set in place, which then traps all users into thinking the cryptocurrency has a value, when in fact it operates almost like a front company for money. Because bitcoin, as of now, operates similar to

that of a stock, new cryptocurrency founders will also look for clients to invest in their coins, but will be defrauding these clients with a plot to close the currency exchange and walk away with all of the investors' money. The cases below, in Box 15 and 16, describe how offenders are deceiving clients into investing in a currency that is not legitimate, but rather a scheme to steal money from clients.

**Box 15: Case Study: Homero Joshua Garza**. Homero Joshua Garza designed his currency of "hashlets," which are dispensed by his companies GAW Miners and ZenMiner. These hashlets operate very similar to bitcoin, yet the only problem is not all the hashlets sold were supported by computer power. What this means is that Garza was selling hashlets with nothing to back them up, rendering them useless. With this he created a sort of Ponzi scheme where new clients buying hashlets were used to exchange hashlets back to fiat currency. Eventually his operation was uncovered by authorities and was prosecuted. So while there are some legitimate cryptocurrencies like bitcoin, there are others that were set up to defraud clients into believing the "currency" can operate as a currency.

**Box 16: Case Study: Ruja Ignatova**. Ruja Ignatova founded the cryptocurrency OneCoin and set it up to operate like an investment scheme. The first set of investors would give money to Ignatova and her team, and the next set of investors' money would be used to pay back the first set of investors. With her entire operation, nearly three million people were affected by this Ponzi scheme. With these two examples of Garza and Ignatova, should criminals decide cryptocurrencies are less costly to commit crimes than traditionally, they should beware of fraudulent currencies that may actually steal their money instead of conceal their money.

***Other Crimes.*** Because bitcoin and its similar cryptocurrencies operate in a decentralized way, there is no regulating or enforcing body to keep crime from happening. With such freedom, criminals have exploited cryptocurrencies to aid in their crime operations. While this study focused mainly on money laundering, drug trafficking, and terrorism financing, other crimes would appear through the narratives of the cases. The case below, in Box 17, describes how it is easy for offenders to float from one crime to another using cryptocurrencies to hide their tracks.

**Box 17:** **Case Study: Alexander Vinnik**. Alexander Vinnik hacked Mt Gox, a very popular bitcoin exchange before it went bankrupt as a result of Vinnik's hack. From the hacking of Mt Gox, Vinnik was able to walk away with hundreds of thousands of dollars. Even before this hack, Vinnik set up his own bitcoin exchange, as mentioned before, which he called BTC-e, through which he funneled criminal money from his own endeavors and endeavors from other criminals. He was able to launder over $4 billion in bitcoin between his money laundering services offered with BTC-e and his hacking skills. With the crime opportunity to serve as a bitcoin exchange, Vinnik used this to his advantage by laundering his own illicit proceeds from hacking through his own exchange.

As discussed before even crime syndicates are looking to take advantage of cryptocurrencies to fulfill their own self-interested goals. The examples of Kirin and Dhanani both show that money laundering was not the main goal; it was just a side project for them to "clean" their money. With Kirin, reselling the stolen tickets was a priority for the cybercrime syndicate. However, as the operation grew, so did the need for money laundering, which is

where Kirin came into play. With Dhanani, the main goal was to sell credit card and bank account information. As their business grew too, they needed Dhanani to handle all transactions and wire transfers to all members of the Shadowcrew. With cybercrime it seems lots of different crimes can bleed into each other because of the ease the Internet allows.

Even loan sharking effects can be seen among crimes used with the help of cryptocurrencies. The case below, in Box 18, describes how offenders could use crimes associated with cryptocurrencies to make some quick cash, but are eventually sucked into the greed and desire for more that comes with it.

**Box 18: Case Study: Daniel Atkinson**. Daniel Atkinson was a gambling addict and often times would find himself owing loan sharks a lot of money. In order to make that money back, Atkinson started to distribute ecstasy online. From here, Atkinson was not only able to pay back his loan sharks, but to also make hundreds of thousands of dollars for himself to pocket as well. This goes back to the pointer of high commissions. By operating online, criminals can reach a larger consumer base that is not only geographical, but global. Atkinson used this to his advantage by making a lot of cash in a short amount of time to pay back his debts, but to even profit from his new business as well. These are only just a few of the crime opportunities that have presented themselves throughout the compiled cases.

***Summary***. Again, this was not a surprising finding that cryptocurrencies are linked with more than just money laundering, drug trafficking, and terrorism financing. In fact, cryptocurrencies open up doors from criminals to engage in crimes they might not have otherwise thought to commit. With the versatility cryptocurrencies lends in both conducting

business, as well as laundering money, it can be assumed that criminals would be drawn to more than just these types of crimes researched in this study. If given the opportunity to commit more crimes, out of greed and rational choice, these criminals would take the chance if the benefits outweighed the costs. This is an important finding in understanding that cryptocurrencies are not just used for transacting, but also as a bridge between crimes because cryptocurrencies can easily bridge the gap and conceal the tracks.

**Theme 4: Money laundering services**

When it comes to cryptocurrencies, it makes sense that they are often associated with money laundering, especially because they are known for being a digitalized form of cash. For the purposes of this study, they are a currency after all. However, out of all the cases studied, only 29% of cases were strictly money laundering related, with no ties to drug trafficking. As discussed earlier, criminals can take advantage of such currencies by concealing their identities while also laundering their money through.

***Front companies***. Just as with traditional money laundering, cryptolaundering still involves the uses of front companies. The cases below, in Boxes 19 and 20, describe how offenders use front companies to hide their cryptocurrency transactions for extra precaution in trying to evade law enforcement efforts.

**Box 19: Case Study: Anthony Murgio**. In order to hide his operation from the police, Anthony Murgio created an online "Collectibles Club" website that was advertised as a place for collectors to discuss and trade rare collectibles. In reality, this website was a front for his

currency exchange business where he knowingly exchanged cash for bitcoin to criminals involved in illegal online drug distributions. He advertised his exchange, called CoinMx, as a place for anyone to exchange cash for bitcoins, however, a majority of his clientele were of the criminal type. Throughout the duration of his scheme, Murgio was able to make close to $10 million from his business.

**Box 20:** **Case Study: Zoobia Shahnaz**. Similarly, to conceal activities, Zoobia Shahnaz sent bitcoin to several dummy business accounts that were actually operated by ISIS. By using these accounts it would further conceal where the money was going. However, Shahnaz did not take preventative steps in concealing where the money came from, where her bitcoin account was linked to her personal bank account, leading authorities straight to her. From there the police were able to verify that the accounts she deposited bitcoins into were in fact shell companies she funneled money into that were operated by ISIS.

***Money Exchanges***. Out of all the money laundering cases, a majority of them involved currency exchanges. Like Murgio, there were many instances of individuals starting up currency exchanges that were explicitly made for criminals to use as a resource for laundering their illegal proceeds. The case below, in Box 21, describes how offenders use currency exchanges to facilitate their crime operations in "cashing out."

**Box 21:** **Case Study: Vadim Vassilenko**. Vadim Vassilenko was known for his Western Express International currency exchange, where he would exchange cash for what he called e-gold. When his clients would exchange their cash for e-gold, Vassilenko would then launder the

money for his clients through a series of layering transactions between dummy accounts. He would use his site to do these transactions but to also help his clients "cash out" and exchange the e-gold back to cash money. Vassilenko operated as a money laundering middleman, where a majority of his clients were criminals wishing to "clean" their money. However, Vassilenko was apparently not layering his transactions enough because he was detected by authorities that he was an unlicensed money services business, but also that he was moving a lot of money through his currency exchange. Vassilenko's case is only one of the many currency exchanges cases found in the set of 100.

***Bridging the Gap***. By laundering money with cryptocurrencies, it bridges the gap between predicate crimes and the "cash out" in the end. It is a necessary crime that has become a lot easier with the use of cryptocurrencies to both commit crime and launder money. These money exchange middlemen provide services that bridge the gap between the business end and the profit end of the operation. The case below, in Box 22, describes how the ease of money laundering via cryptocurrencies adds to the benefit of committing transnational crimes, where without this ease, these crimes may not be occurring.

**Box 22: Case Study: Charlie Shrem & Robert Faiella**. As mentioned before, Charlie Shrem and Robert Faiella worked together to create the ultimate crime opportunity. Charlie Shrem was the administrator for his currency exchange called BitInstant, while Robert Faiella was a popular drug vendor on the Silk Road. Because the Silk Road only accepted bitcoins to make any sort of transaction, it made for an ideal situation. Faiella could exchange his money with Shrem, who would help launder his money, and Shrem would benefit from Faiella by requesting a high

commission for his money laundering services. This bitcoin exchange service allowed Shrem to bridge the gap between money laundering and drug trafficking, allowing for a smooth operation that was fast and convenient, all while not having to meet together in person. Shrem's exchange was also popular with other criminals because Ulbricht allowed Shrem's bitcoin exchange to be advertised on the Silk Road site, where average people were directed to BitInstant to exchange their money for bitcoins in order to proceed with any transaction. So while Shrem had his regular criminals using his services, he also had a lot of foot traffic from normal people as well, which helped keep his business legitimate. He provided an easy way for people to cash in and cash out easily.

***Summary***. With the quantitative data confirming the notion that money laundering activities actually benefit offenders greatly, even more so than drug trafficking, it is no surprise that money laundering has its own theme that was recurrent throughout the 100 cases. What it comes down to is that currency exchanges are going rogue. While some states have made attempts at regulating currency exchanges, it does not help that other states have taken a more passive stance. These currency exchanges are key to understanding transnational crime operations facilitated by cryptocurrencies. This is because they operate as the middlemen in the situation. They profit from people wanting to convert their cash for cryptocurrency. If they want even more money running through their business, they will go so far as to explicitly offer money laundering services to criminals wanting to launder their illicit proceeds. Money laundering via cryptocurrencies is connected with a myriad of predicate crimes ranging far beyond drug trafficking and terrorism financing. It is a business that allows its operators to evade detection, while also making millions of dollars just on commissions for their services.

**Theme 5: Terror support and cryptocurrencies**

While terror support cases were a clear minority of the 100 cases, at 6% of all cases, these few cases demonstrate that cryptocurrencies are being used to fund terrorism regardless. It may not be happening as drastically as some law enforcement are led to believe, or maybe terror supporters are skilled at concealing their identities. Whatever the reason for the low numbers of reported cases where terror supporters are actively using cryptocurrencies to fund larger terror groups, this sort of money transaction is happening, as demonstrated by six cases included in this study.

***Bitcoins Used to Fund Terrorism.*** While bitcoins were not exclusively used to fund terrorism, they were still used, most likely due to the convenience and anonymity the currency offers. The case below, in Box 23, describes how terror supporters are using cryptocurrencies to fund terrorists overseas in the hopes they can resume operations.

**Box 23:** **Case Study: Zoobia Shahnaz**. Zoobia Shahnaz was almost able to send $85,000 in bitcoins to ISIS, but even before this she was able to send over $150,000 to ISIS to help replenish their cash flow. After making these transactions with her personal bank account, in addition to her booking a flight to Syria, authorities stopped her at the airport where they made the connection that she has been supporting ISIS through the use of bitcoins exclusively. She is the first known terror supporter in the United States to have explicitly sent bitcoins to a known terror group and to be prosecuted. Shahnaz faces up to 50 years in prison for her crimes. While bitcoin seems like the most trusted and most convenient currency to use, other currencies, such as PayPal and other altcoins, were used in addition to bitcoin to fund terrorism.

***A Variety of Cryptocurrencies are Used.*** Other currencies were found to be used in addition to bitcoin, which was probably to diversify the way in which these middlemen supporting terror groups were able to appeal to a larger group of supporters. By allowing people to pay how they pleased, it allowed convenience for greater number of people. The case below, in Box 24, describes how terror supporters are using social media and various types of cryptocurrencies to fund terrorism activities to allow people from all over the world, sympathetic to terrorist causes, to donate money via these cryptocurrencies to remain anonymous and evade detection.

**Box 24: Case Study: Ali Shukri Amin**. In the Ali Shukri Amin case, Amin described on Twitter how supporters of terror groups can contribute to the cause. He detailed exactly how people can purchase cryptocurrencies online and then send money to an account, which would then be forwarded to ISIS. He used various forms of social media, particularly Twitter, to reach younger generations who are willing to support the cause financially, giving them a concealed way of donating. Amin was only 17 years old when police arrested him. By allowing a variety of methods in receiving payments from civilians, Amin could consolidate the transactions and forward them along to ISIS. The use of multiple cryptocurrencies was most likely to reach a greater population as well as diversify their evading law enforcement techniques.

***Middlemen Collect Money.*** With terrorism financing, a few of the cases studied indicated that the perpetrators arrested were actually regional middlemen collecting and compiling resources for terror groups. They might not have been themselves terrorists, but they were the

suppliers and supporters of terrorist actions. The case below, in Box 25, describes how middlemen are used in supporting terrorists, where these middlemen will collect money donating from locals and will either purchase resources for terrorists or send the terrorists all the money they have collected. Cryptocurrencies allow these middlemen to do this in a fairly secure manner.

**Box 25: Case Study: Ramiz & Sedina Hodzic**. Ramiz and Sedina Hodzic were in charge of both transferring funds to terror groups overseas, but also purchasing resources they would then ship to these terror groups. They raised support locally and had people send them money, which they would use at their own discretion. Overall, they were the couple to go to in order to donate money to the terror cause or to donate resources. It is almost as if they were disaster relief for overseas terror groups where they would collect both money and resources to then send along to these groups as needed.

***Summary***. While terrorism-financing cases were a clear minority in this study, what the small number of cases does suggest is that these crimes are still occurring. It seems that these cases are similar in the fact that they are carried out by terror group middlemen, often times average people wanting to be involved in the causes overseas. However this creates a national security risk for not just the United States, where these cases were taken from, but for all over the globe. These people are using cryptocurrencies to funnel money to terror groups that law enforcement are desperately trying to cut funding from. These cases also make it clear that, while the highlight of this study is focused on cryptocurrencies, these middlemen are using these currencies and buying resources, which they will then ship to terror groups. Terror supporters are

using all available avenues to get financial and resource donations to their causes, which is alarming from a national security standpoint.

**Theme 6: Challenges for law enforcement and prosecution**

Returning to the idea of rational choice, where criminals are believed to calculate the costs and benefits of committing any crime, it is important to note that prosecutors do not investigate cryptocurrency cases very frequently. It is always a big deal to have to explain to the jury and judge what exactly cryptocurrencies are and how they operate in order for them to understand the harms they are allowing criminals to commit. However, with such newness of these types of cases, prosecutors have to tread lightly, because what they resolve in these cases may set a precedent for how all cases like these should be solved.

***Precedent.*** Prosecutors have to be careful how they handle their cases. They need to set a precedent for these cases. If these criminals are given light sentences, deterrence is not so much a factor in the cost-benefit analysis for these criminals. However, if sentences are seemingly too harsh for the crimes, deterrence may not be a factor either. The sentence needs to be proportional to the crime in order to deter criminals from engaging in such activity. Prosecutors and judges have to demonstrate that these types of crimes will not be tolerated, and that while it is hard to locate these criminals, law enforcement is trying its best to bring them in in order to serve justice. The cases below, in Boxes 26 and 27, describe how prosecutors are figuring out how to handle these cryptocurrency cases, by offering harsh sentences as punishment for offenders' crimes.

**Box 26: Case Study: Ross Ulbricht**. With Ross Ulbricht, it was one of the biggest cases against criminals using bitcoin and darknet marketplaces all in one. Prosecutors and judges realized the harm of such a combination, and thus declared it suitable to punish Ulbricht with one of the harshest sentences, second to the death penalty: life in prison. However, in theory, this means that Blake Benthall, and all other caught darknet marketplace administrators, should also be sentenced the same way because of the precedent the judge left with Ulbricht's case.

**Box 27: Case Study: Zoobia Shahnaz**. In the case of Zoobia Shahnaz, the woman who sent over $150,000 in bitcoins to ISIS, this is the case that will set precedent for other terror involved bitcoin cases. This is a hard job for prosecutors in understanding the issue and making it come across at sentencing. Shahnaz is not yet sentenced, however, it would be possible to assume she would receive close to the 50 years maximum she was meant to receive.

However, the United States is not the only state that is struggling with this idea of setting a precedent for these crimes. In Japan, Ayumu Teramoto was the first individual caught distributing drugs online throughout Japan in exchange for bitcoins. In Australia, Christopher Owens, was also the first drug distribution case, where he would purchase drugs off of the Silk Road and distribute the drugs locally in Australia. Within the legal system, they are going to have to figure out how they would like to handle this situation. However, it is not so easy. Many states have taken a passive stance on how they view cryptocurrencies, meaning it is in a sort of limbo, legally. This make things difficult when crime presents itself and the courts do not know how to handle such crimes. It makes it even more difficult when many of these crimes are happening across borders, yet every state has their own way of handling the cases. For right now,

the United States has taken the lead role in aggressively prosecuting these individuals for their crimes, but this can only go so far if other states are not on board.

***Brains versus Brawn***. Within these cases, it was found that because prosecutors and judges needed to set a precedent, sentences were harsh. However, they made sure that the harsh sentences were within proportion to the crimes committed. For example, the "brains," or leader, of the operation was punished more harshly than the "brawn," or the subordinates to the leader. The cases below, in Boxes 28 and 29, describe how the main operators behind the schemes are the ones that are punished more heavily because of their rational choice to commit the crime. The supporting operators are the ones listening to these main operators, thus their rational choice is altered by the main operators. However, regardless, it is imperative to punish both types of operators harshly in order to deter the behavior.

**Box 28: Case Study: Ross Ulbricht & Gary Davis**. In this section of setting an example for future criminals, the biggest case that comes is that of Ross Ulbricht and his role as administrator of the Silk Road. Out of all the cases, he had received by far, one of the most harshest sentences for his crimes: life in prison. He was the brains of the operation and was the one with the vision. His right hand man, Gary Davis, was also arrested and tried, however, his sentence will most likely be not nearly as long as Ulbricht's. The reasoning behind this is that Davis was merely following the orders of Ulbricht in daily operations of the Silk Road. It was not Davis' idea to run an online marketplace that mostly sold illegal contraband, but instead it was Ulbricht's idea.

**Box 29: Case Study: Blake Benthall & Brian Farrell**. Similarly, with Blake Benthall, administrator for Silk Road 2.0, Benthall was the brains behind the operation and could potentially receive the same sentence as Ross Ulbricht for his crimes. On the other hand, Brian Farrell was the right hand man of Benthall and would be punished as that: a follower of Benthall. However, mixed with his responsibilities from Benthall, and him actually being a vendor on the Silk Road 2.0, Farrell was still sentenced to 8 years in prison because of the combination of his crimes; a sentence severely less harsh than Ulbricht's.

***Summary***. Prosecutorial examples indicate that these types of crimes are not only challenges for law enforcement, but also challenges for our court systems. The obstacles of having lawyers, judges, and juries to understand, first what cryptocurrencies are, and second, how these cryptocurrencies are facilitating worldwide harm, are no easy tasks. It is a frustrating and grueling process that will have to take time and thought. By focusing well on these cases, which are most likely only the beginning, prosecutors can set themselves up for later when more of these crimes begin appearing. Like other traditional crimes, the person with more stakes in the operations will continue to be punished more harshly than subordinates, but will also be sentenced seemingly more harshly than for their traditional crime equivalents. It is the way that prosecutors and judges react that will ultimately decide if these crimes are too costly for potential criminals to commit. That is why prosecutors are tasked with properly punishing such crimes, without knowing the true extent to which these crimes will occur in the future. What is decided today will generally stand in the future.

## Discussion

From the findings discussed above, it can be inferred that cryptocurrencies have made transnational crimes easier for criminals. Because it is assumed that these transnational offenders are rational beings, in order for them to believe committing the crime is worth the risks, there needs to be some sort of mitigation of costs. With cryptocurrencies, there is a variety of ways to both cut costs and increase benefits, which is the ideal scenario for criminals. Cryptocurrencies offer features like anonymity, convenience, and ease of use, which can be enjoyed by all, but provides excellent crime opportunities exploited by criminals in evading detection and arrest. Convenience provides a way for criminals to conduct all their business, while also evading transaction reporting by banks, considering the decentralized nature of cryptocurrencies. Ease of use also allows criminals of any skill set to reap in the benefits cryptocurrencies present. These characteristics of cryptocurrencies make it harder for law enforcement to investigate these crimes. Cryptocurrencies decrease the costs and increase the rewards of committing the crime in three specific ways. The major themes that are important are discussed below.

### Cash Flow

With cryptocurrencies, it has become harder for law enforcement to employ Follow the Money techniques. With traditional money laundering, law enforcement could review bank records to follow the flow of cash deposits to unravel the layering phase of money laundering. However, with cryptocurrencies, this technique becomes very difficult, considering the multitude of ways criminals can launder money. It is also difficult when law enforcement cannot subpoena transaction records for a particular account holder, whose information is most likely falsified. While the blockchain is a public ledger where law enforcement can go to track transactions;

however, law enforcement then has to have an idea of which public wallet key goes with their subject. From there, tracking becomes even more difficult because account holders could potentially have an infinite amount of accounts to layer their money through. While it is not impossible, as these cases demonstrate, law enforcement will have a hard tracking cash flow of careful criminals who take extra precautions to launder their money using cryptocurrencies.

It is clear from the cases that many of them have exceeded $1 million in total operation amount. This is an interesting finding because this indicates there are high commission for the crimes studied, as well as the fact that bitcoins can facilitate the way in which such large amounts of money can be concealed. It is reasonable to assume that these sorts of schemes are happening more often than the 100 cases studied. It is also reasonable to assume that large amounts of money are being concealed using bitcoins or other cryptocurrencies. Criminals are using cryptocurrencies to facilitate their businesses by making transactions, but also concealing their identity, as well as the identity of their clients. It is a dangerous arena with high money rewards at stake, but at the price of civilians. For example, fentanyl distributors are making enormous amounts of money through counterfeit fentanyl. It is cheap and easy to produce; darknet marketplaces and bitcoins make it easy to distribute and remain undetected; and unsuspecting fentanyl users are expecting FDA approved doses of fentanyl, when in reality they are receiving lethal doses of counterfeit drugs.

Traditionally, in order to stop these criminals from taking advantage of unsuspecting drug users, they would attack from all sides: from monitoring their distribution methods to following the money flow. However, as discussed earlier, it has become harder for law enforcement to keep up with drug distributing criminals since they have moved to the darknet, using a currency that conceals their identities. By moving online, drug kingpins can now reach a larger, worldwide

consumer base, which allows their operation amounts to increase even more. They have also taken to using cryptocurrencies to not only protect themselves from law enforcement, but to also have a way to easily launder the currency by layering several transactions across several bitcoin wallets, making it very challenging for law enforcement to follow. From there these drug lords can then begin cashing out after they are satisfied with how well concealed their transactions are. It has also been found that currency exchanges are often times working with criminals, which further hinders law enforcement efforts because these exchanges are not reporting suspicious activity. Cash flow used to be a very important way in which law enforcement would go after drug-related crimes only; however, this is no longer the case. Law enforcement has been going after so many more crimes by using the Follow the Money techniques.

Terrorism financing and straight money laundering have also become of interest to law enforcement, hence why these crimes were also studied in this research. With terrorism financing and cryptocurrencies, it is now becoming a concern for law enforcement that terror supporters are funneling cash donations through cryptocurrencies and into the accounts of known terrorists. This is particularly concerning considering law enforcement no longer has a way of knowing what accounts terrorists are using, nor which individuals are supporting these groups. Also with the use of multiple types of cryptocurrencies it would be nearly impossible to track down every account they ever make in order to cut funding to the terror groups. This is a real threat to public safety, where people are donating anonymously to terror organizations and are getting away with it. Examples of terror support middlemen were shown through the results of this study, where their primary role is to collect donations from other terror supporters and find a way to get the money to the groups without being detected. They go so far as to publish online how to donate anonymously to groups like ISIS. While only six cases of terrorism financing using

cryptocurrencies were studied, this does not diminish the importance of tracking such criminal behavior. More research is imperative to understanding cryptocurrencies and their use to terror organizations. However, this finding also goes to show that cryptocurrencies can be used by anyone, anywhere, and at any time. People funding terrorism through cryptocurrencies could be average people supporting a cause that is taking place overseas. It is a simple and convenient way of sending and receiving money, and it is easy enough for laypersons to use as well.

Money laundering, on the other hand, is an interesting case because almost always it is connected to some other crime. In this study, the crimes of money laundering only and money laundering and drug trafficking combined were studied. It was important to separate the two because even though money laundering happens most frequently with drug trafficking, it was important to show that other crimes need money laundering as well. This points out the significance of having a Follow the Money technique within law enforcement agencies because of reliance on money laundering in order to access illicit funds received from illicit activities. By eliminating the ease of "cleaning" illicit money, law enforcement can make crime more costly. Money laundering is the key crime to focus on in order to make other crimes more costly. However, this is only possible if law enforcement knows the methods in which criminals are using cryptocurrencies in combination with their crimes. This study identifies the ways in which transnational criminals rely on cryptocurrencies to facilitate their crimes.

**Deal, Launder, and Profit**

Cryptocurrencies are convenient for criminals. It is a way to conduct business, launder money, and utilize resources, all using the same method. Criminals can buy drugs on the darknet with cryptocurrencies. They can then participate on darknet marketplaces as vendors and sell

these drugs to demanding consumers. They can take these proceeds and layer them through several bitcoin accounts that they own in order to layer the transactions. Finally, they can "cash out" the freshly laundered cryptocurrencies into whatever form of fiat currency they would like. Taking it one step further, these criminals could even run their own cryptocurrency exchange, where they will convert cryptocurrency for cash. With this, they can "cash out" whenever they want, without the need to trust a third party cryptocurrency exchange, and they can make business by exchanging other people's cash for cryptocurrency and back, making even more of a profit.

By conducting all business in cryptocurrency, the value of the currency even has a potential to increase, as more demand for it arises. What this means for criminal is that if they leave their criminal proceeds as cryptocurrency, like bitcoin, they could have the potential to make money off of the increasing value. While this is not guaranteed, considering the volatile nature of cryptocurrencies, it is a risk they would have to calculate in their rational choice of using cryptocurrencies to commit crimes. Overall, criminals have a way of dealing drugs or other illicit services, laundering the proceeds from their crimes, and profit even more by investing in the currency. With this in mind, there seem to be greater benefits than costs of using cryptocurrencies to commit crime.

However, this idea only applies to crimes that are not time sensitive. For example, with drug trafficking, as long as the money gets to where it needs to be, meaning from the drug lord down to their subordinates, the money can remain as bitcoin as long as they would like. By leaving the money in bitcoin, there is a potential for the value of bitcoin to increase and for them to make a profit off of their illicit profit. On the other hand, for crimes like terrorism financing, terror groups may benefit from keeping their money in bitcoins because generally that money is

being sent to be used. Terror organizations often need a steady flow of cash to remain afloat. Even with the cases studied, it was found that both cash and resources are needed by terror groups, however, that cash would most likely be used right away to pay for resources or pay their soldiers. Terrorists do not have the luxury of letting their money sit in an account with the hopes to profit even more. With drug trafficking or straight money laundering, it does not necessarily matter if the money is withdrawn right away or not. With them, their businesses rely on them having a store of cryptocurrencies anyway, so if given the option, they could keep their money in bitcoin, as they would keep their money in a stock. This is something that would fall under the benefits category for committing crime: the ability to make money by using bitcoin. However, it could also be considered a cost for committing crime because if the value of bitcoin goes down, their total profit goes down in value as well.

**One Crime Leads to Another**

Because of the anonymity, convenience, and ease of use that cryptocurrencies offer, it is easy to see how cryptocurrencies would allow criminals to be involved in a multitude of crimes. As described above, criminals can be involved in darknet drug dealing, but can also own their own cryptocurrency exchanges that will launder money for other criminals. With cryptocurrencies closely related to money laundering because of the currency aspect, it is easy to assume that these crimes are all predicate crimes to money laundering. However, what is unique about crimes with cryptocurrencies is that they may never have been committed if cryptocurrencies did not ensure them a way of concealing their own identities as well as bypassing the need for banks. It has become easier for criminals to switch and adjust their plans to involve multiple crimes, all using cryptocurrencies as their failsafe or escape plan.

For example, embezzling was found to be popular when using cryptocurrencies. Because of the lack of authority or jurisdiction over cryptocurrencies, it is easy for criminals to plot to steal cryptocurrencies from unsuspecting users. The way in which criminals do this is through setting up their own currency exchanges or even a new cryptocurrency in general. They are able to obtain a solid consumer base and deceive their clients into thinking their money is secure. With currency exchanges, the administrators would empty out all of the accounts into their own personal accounts and declare bankruptcy. This leaves their clients with empty wallets and frustration that they cannot raise complaints against the currency exchange for plotting such a heist. With new cryptocurrencies, the site administrators treat the currency as a stock and will create a sort of Ponzi scheme, where they will take the money of their primary investors and repay them using secondary investors' money, and so forth. Eventually the scheme comes to an end, with the site administrators running away with the money their consumers invested and consumers left with nothing.

It is also possible that criminals can hack the wallets of unsuspecting users, stealing whatever is in their wallets. Because of the way the bitcoin algorithm works, this method is challenging and criminals would need to be technically advanced in somehow obtaining the private key needed to get into the bitcoin wallets of their victims. This is another way criminals can obtain access to cryptocurrencies that are not theirs. Even without hacking someone's wallet, criminals can take the easier route and hack an individual's computer and infecting it with ransomware, where the victim is requested to pay, in bitcoin, the criminals for access to their computer once again. This is a popular method because once the criminals are paid, they can then easily layer the bitcoins through several accounts to launder their money and use in the future.

Cybercrime syndicates have also found ways in which to use cryptocurrencies to their advantage. While the targets of these cybercrime groups are not generally cryptocurrencies themselves, they have found uses for cryptocurrencies to make their operations more efficient. That is all cryptocurrencies offer: efficiency and crime opportunities. Cryptocurrencies make businesses more efficient allowing them to commit all their crimes using the currency and in the end they can launder all the money and "cash out". They also offer crime opportunities because if these currencies were not around, potential criminals would have to recalculate the costs of their crimes as opposed to the benefits. This study has established that cryptocurrencies do play a role in facilitating transnational crimes, making it an area of interest with much needed policy suggestions.

**Theoretical Implications**

In sum, this study has shown that transnational crime actors are rational in nature. They weigh the costs and benefits of any crime to make sure the gains of committing crime always outweigh the consequences. Wortley & Mazerolle (2008) argue that criminals are environmentally aware, meaning they understand their contexts and are always looking for opportunities with crime. With cryptocurrencies, they offer the perfect environment for them to get away with their crimes. Because cryptocurrencies do not ask for personal identifiers, individuals can seemingly get away with their crimes because there is this lack of oversight. Police do not have the authority to regulate cryptocurrencies, thus providing the perfect environment to commit crime: outside the jurisdiction of all police forces. Cryptocurrencies are easy to use and convenient to make multiple transactions without racking up bank fees. They are used for both legitimate and illegitimate purposes, making it easy to claim the money being

"cashed out" is from legitimate businesses. Criminals can also take advantage of police efforts in trying to regulate currency exchanges, meaning criminals take advantage of the fact that police jurisdiction does not transcend borders, even though their crimes do. By transcending borders, police need to collaborate in efforts in tracking these criminals, yet, collaboration between foreign agencies is a challenge in itself. With this transcendence of border, criminals are meeting each other online, making it easier to network, especially when looking for specific qualifications for a particular operation, such as money laundering expertise. This helps them find the best of the best when picking co-offenders. With this environmental approach to rational choice theory, cryptocurrencies provide a viable way for transnational criminals to realistically make over $1 million in commissions and walk away from their crimes, untraced.

With Clarke & Cornish's (1985) idea about offenders' decision-making processes, they argue that criminals are very much driven by the opportunities that present themselves in their lives. Offenders may not actively be seeking out crime, but crime opportunities find them. However, it is up to them whether the crime is worth the risks involved. With cryptocurrencies there are several features to benefit from, from high cash rewards to anonymity to a booming business, and very little risks involved, including losing money off of the devaluing of the cryptocurrency, or the currency exchange that was used is now bankrupt. In committing crime with cryptocurrencies, if the crime presents itself, criminals will most likely commit the crime because of the rewards they can walk away with, especially considering the low chances of being caught. Traditionally, these crimes may be considered risky, with high chances of being caught. However, with the decentralized nature of cryptocurrencies and the built-in feature of anonymity, criminals can now take part in this risky business and still obtain high rewards, without the constant fear of being caught by authorities.

Cohen & Felson (1979) discuss the ways in which routine activities can factor into the rational choice of offenders. With the convergence of a likely offender, suitable target, and absence of a capable guardian, Cohen & Felson (1979) agree that crime will occur. With cryptocurrencies in addition to the darknet marketplaces, crimes will occur. On these sites are all sorts of likely offenders looking to make some quick cash. Their suitable target is doing business with cryptocurrencies to protect their identities and keep their transaction private. Finally, on these sites, there is a lack of guardian period. Law enforcement needs to have a stronger presence on the darknet for criminals to really factor the chances of them getting caught into their cost-benefit analysis. Criminals are connected via the Internet and can socialize with people from all over the world to plot and scheme the best ways in committing crime without even being detected by law enforcement. Online environments and cryptocurrencies allow for such interactions, making it very difficult to investigate and prosecute, hence why prosecutors are not taking their job lightly when actually getting to prosecute a case like this. In sum, if the crime opportunity presents itself, criminals will take it; and with cryptocurrencies, the crime opportunity is always there.

**Prescription for Prevention**

Though this is an exploratory study, this study has extensive policy implications. Following the prescription of prevention from Cornish (1994) and Clarke (1995), policy implications derived from this study are great. In order to discourage the use of cryptocurrencies to facilitate crimes, law enforcement and policymakers need to decide how to make cryptocurrencies more costly for criminals by mapping out the procedural aspects of crimes committing using cryptocurrencies. By making it more costly to use cryptocurrencies potential

offenders will have to look towards other methods of conducting business, or return to their traditional methods. However, with this, law enforcement need to plan to prevent crime, not just displace it. While making cryptocurrencies harder to facilitate crimes, criminals may look to exploit other ways of committing their crimes at a lower cost. In order to make any change, law enforcement and policymakers need to be educated on the implications of this study.

Cryptocurrencies are in fact being used to facilitate transnational crimes and this behavior is having a global impact on civilians. They are being victimized by these transnational criminals, ranging from a loss of money to even death. These are not victimless crimes that do not require immediate action. Instead, these are crimes that are taking lives and protecting the criminals giving the orders. Cryptocurrencies are playing a supporting role in these crimes, as described by this study. It is not enough just to study crime; action needs to be taken in order to prevent it from occurring in the first place. Situational Crime Prevention is only effective when it is crime specific. This study has laid out the ways in which offenders are using cryptocurrencies to facilitate their crimes. While this study only looked at 100 cases, it provides a foundation for tracking the use of cryptocurrencies in facilitating transnational crimes. Even with these 100 cases, law enforcement can be utilizing Situational Crime Prevention techniques in order to prevent crime before it even happens.

Situational Crime Prevention, an opportunity reduction strategy for developing immediate practical measures to deal with the cyber environment and crime is used to prescribe prevention measures. Using the 25 techniques of Situational Crime Prevention methods developed by Clarke (see popcenter.org), some prevention measures are identified in Table 3 that could help in making it difficult, riskier, and less rewarding for criminals to use cryptocurrencies in facilitating illegal transnational operations. The strongest suggestion for prevention tactics

would be increased education for law enforcers who may have to deal with cryptocurrencies in the future; court personnel, including lawyers and judges; and users of cryptocurrencies as well. The most difficult suggestion to implement would be to monitor cryptocurrency exchanges, where not all countries require these exchanges to obtain licenses or report suspicious activities. These are crimes that affect all states, yet there is not one unified response to cryptocurrencies and their facilitation in transnational crimes.

**Table 3. Prescription for Prevention Tactics**

| Increase Effort | Increase Risk | Reduce Rewards | Reduce Provocations | Remove Excuses |
|---|---|---|---|---|
| Harden Targets | Extend Guardianship | Conceal Targets | Reduce Frustrations and Stress | Set Rules |
| Add oversight measures in trying to mitigate effects of cryptocurrencies on state financial institutions.<br><br>Strengthen knowledge of cryptocurrencies to judges and prosecutors to help deter potential offenders. | Advertise that LE will be using undercover operations to take down illegal currency exchanges that offer money laundering services, as well as darknet marketplaces. | Educate the public on how to defend themselves against the dangers and harms of cryptocurrencies to make them less vulnerable. | Develop blockchain technology for banks so that people can enjoy the features of cryptocurrencies, but also enjoy in the protections of bank oversight. | Educate the public that crimes committed on the darknet and/or with cryptocurrencies will still be prosecuted aggressively. |
| Control Access to Facilities | Assist Natural Surveillance | Remove Targets | Avoid Disputes | Post Instructions |
| Continue to take down drug sites on the visible Internet (moving operations to the darknet), which may deter the average user from proceeding with their potential crimes. | Encourage people to bring suspicious activity to the attention of the police to help keep their own money safe. | Educate the public on how to keep their wallets (and computers) safe from hackers. | Law enforcement should fuel disputes among vendor competitors by giving them incentives to turn each other in. | Create an educational website on "what to know before using cryptocurrencies" to help stress what is expected of people who use cryptocurrencies. |
| Screen Exits | Reduce Anonymity | Identify Property | Reduce Emotional Arousal | Alert Conscience |
| On top of requiring currency exchanges to be licensed, have regular audits on these exchanges to keep them accountable on their books. This will force oversight of people "cashing out" in large sums. | Track IP addresses of suspicious accounts and create a software that would track all of the transactions from wallets to wallets. | Require currency exchanges to all be licensed, which will help monitor all the money being "cashed out." | Have banks create their own forms of cryptocurrency that have legitimate oversight and can guarantee help should users need it. This will minimize the temptation for average users getting mixed up in illegal activity. | Require licensed currency exchanges post on their sites laws regarding crimes committed using cryptocurrencies and the potential consequences of such behavior. Make this a requirement for licensure. |
| Deflect Offenders | Utilize Place Managers | Disrupt Markets | Neutralize Peer Pressure | Assist Compliance |
| Continue to take down darknet marketplaces and currency exchanges in order to show offenders that these crimes are not being taken lightly. | Reward those who can give law enforcement a lead on bad actors on darknet marketplaces or misusing cryptocurrencies. | Increase the amount of undercover operations, as well as closely monitor law enforcement efforts to minimize corruption opportunities. | Increase law enforcement oversight over websites and darknet tutorials on things like how to use stolen credit card numbers or ransomware someone's computer. | Create a site for hotline complaints for currency markets and darknet vendors. |

| Control Tools/Weapons | Strengthen Formal Surveillance | Deny Benefits | Discourage Imitation | Control Drugs and Alcohol |
|---|---|---|---|---|
| Develop software that will identify trends and patterns of accounts making a lot of transactions with other accounts using the public information on the blockchain. | Educate the public on the dangers and harms of cryptocurrencies and the darknet. | Continue to take down illegal currency exchanges that facilitate money laundering. Law enforcement can then dedicate money recovered to more resources in tracking these crimes. | Give harsh sentences to those who are caught to send a message to those who have yet to be caught. | Continue to track suppliers of known overdose cases.<br><br>Track suppliers of caught vendors. |

## Conclusion

This study has shown the relationship between cryptocurrencies and transnational crimes, where cryptocurrencies have made it easier to commit crimes. It has found that cryptocurrencies create crime opportunities for criminals because of their attractive features and the convenience they allow. It is also an important addition to current literature already published and emphasizes the need for more research to be conducted to understand more of the issue. This was the first study to ever look at this many cryptocurrency cases of arrested and/or prosecuted individuals in studying the role these currencies have in facilitating transnational crimes such as money laundering, drug trafficking, and terrorism financing. While descriptive in nature, this study has created a foundation for several testable hypotheses that can be helpful for further studying into this area of research. The quantitative data has shown that when compared to drug trafficking, money launderers can benefit from cryptolaundering than dealing drugs online. The benefit that this brings to offenders has been used to serve their own interests, indicating that this crime will be recurring. The qualitative data in this study has helped shape possible theories of crime facilitated by cryptocurrencies, which also provides a strong foundation for potential policy suggestions to effectively mitigate the harms and abuses of cryptocurrencies. Overall, it has

found that cryptocurrencies are indeed attractive to criminals are being used to facilitate transnational crimes.

In sum, cryptocurrency processes have made it easier for criminals to walk away with the gains of their crimes, while making it harder for law enforcement to investigate, and eventually prosecute. As criminals have become smarter and more resourceful, so should law enforcement. With the assumption that criminals are rational actors who weigh the costs and benefits of any given crime, it is important to understand the role in which cryptocurrencies play into this cost-benefit analysis. Cryptocurrencies are fast, convenient, and lack authority and jurisdiction. They allow criminals to conceal their activities from the police and have the potential for them to increase their profits. They also allows criminals to make transactions with anyone around the world, protecting the identity of themselves and their customers. Cryptocurrencies can also open opportunities to committing more crimes than originally intended. On the other hand, the costs to using cryptocurrencies are that criminals cannot get their money back if it is stolen and cryptocurrencies can decrease in value. While these costs are substantial, the benefits of cryptocurrencies as a whole outweigh these costs. Criminals can do business, evade detection, and make a profit.

This research adds to previous literature about cryptocurrencies and crime, and has illustrated the role of cryptocurrencies in facilitating transnational crimes, specifically money laundering, which is an understudied topic by criminologist. The findings from this study fit nicely with previous literature in that it adds an empirical basis for theories surrounding cryptocurrencies. It adds to the confirmation that cryptocurrencies are being used to facilitate crimes, particularly crimes that are transnational in nature. This is consistent with the FBI report released in 2012, but is inconsistent with the findings of Brown (2016), which indicate that

cryptocurrencies at this point are not a threat to law enforcement. This study has also shown that money laundering can reap enormous amounts of rewards for criminals, which has already been theorized by many research studies (Jacquez, 2016; Maras, 2016; Ritchet, 2017; Sat et al., 2016; Stuhlmiller, 2013; Virga, 2015). This is not a surprising finding because it is a logical move from traditional money laundering to cryptolaundering, where the process of money laundering has become faster and easier. With drug trafficking, the findings of this study also are with the consensus of previous literature. Darknet marketplaces breed crime committed with cryptocurrencies. Drug traffickers using cryptocurrencies can make high commissions and have proven to be resilient towards law enforcement efforts. The offenders captured in this study are presumably only a small minority of instances where people are trafficking drugs on darknet marketplaces. While only a minority of cases, this study has also confirmed that terrorism financing is happening with cryptocurrencies as well, where donors from all over the world are sending money undetected to terrorist groups. Finally, this study has also confirmed that bitcoin has been the leader in cryptocurrencies, yet that could change in the future with the rise of other currencies such as Monero. With the law enforcement spotlight on bitcoin, just like with the darknet drug markets, new cryptocurrencies may begin to surface and may be even more resilient to law enforcement than bitcoin. It is the technology itself that is innovative and being exploited by criminals.

It is believed by scholars that these criminals are rational actors seeking to increase pleasure while decreasing costs. Cryptocurrencies help them achieve these goals. While individual law enforcement agencies can do very little at stopping the abuses of cryptocurrencies, an international effort is needed in understanding this issue and learning how to mitigate the effects. The FATF should focus on putting cryptocurrency on their agenda. Bitcoin technology is

innovative and can be used for legitimate purposes; however, it is being outshined by its connection to crime. It has created solutions to current banking issues, yet is being exploited by cybercriminals wishing to make high profits at low costs. It is technology that can be used by everyone and is not likely to go away, thus there is a need to stop the harms committed by those who abuse the technology. More criminological research for tangible prevention measures must be constantly updated since the criminals are acting faster in the cyber world. Cryptocurrencies are the future; they just need to be taken out of the grasp of criminals.

## Appendix A: Article Citations for all Cases (N=100)

| Arrested/Prosecuted | Citations |
|---|---|
| Achey, Jeremy | Aliens, C. (2017, July 17). DEA busted former AlphaBay vendor "ETIKIN." *DeepDotWeb.* Retrieved from https://www.deepdotweb.com/2017/07/07/dea-busted-former-alphabay-vendor-etiking/<br>United States of America v. Jeremy P. Achey a/k/a EtiKing. 6:17-MJ-01512. M.D. Fla. (2017). |
| Amin, Ali Shukri | Coleman, L. (2015, August 31). How Virginia teen used bitcoin to support terrorism; Judge sentences him to more than 11 years. *CCN.* Retrieved from https://www.ccn.com/virginia-teen-used-bitcoin-support-terrorism-judge-sentences-11-years/<br>United States of America v. Ali Shukri Amin. 1:15-CR-000164. E.D.Va. (2015).<br>USAO - Eastern District of Virginia. (2015, August 28). *Virginia man sentenced to more than 11 years in providing material support to ISIL* [Press release]. Retrieved from https://www.justice.gov/opa/pr/virginia-man-sentenced-more-11-years-providing-material-support-isil |
| Atkinson, Daniel Andrew | Vitaris, B. (2015, Sept 5). Darknet vendor sentenced to 8 years, sold drugs in order to pay back a debt. *DeepDotWeb*. Retrieved from https://www.deepdotweb.com/2015/09/05/darknet-vendor-sentenced-to-8-years-sold-drugs-in-order-to-pay-back-a-debt/ |
| Babadjov, Emil Vladimirov | United States of America v. Emil Vladimirov Babdjov. 1:16-CR-00204. E.D. Ca. (2016).<br>USAO – Eastern District of California. (2018, Jan 16). *Dark-web drug traffickers sentenced in separate cases to 80 months and 70 months in prison* [Press Release]. Retrieved from https://www.justice.gov/usao-edca/pr/dark-web-drug-traffickers-sentenced-separate-cases-80-months-and-70-months-prison<br>USAO – Eastern District of California. (2016, Dec 15). *Fentanyl and heroin sold on dark web marketplace* [Press Release]. Retrieved from https://www.justice.gov/usao-edca/pr/fentanyl-and-heroin-sold-dark-web-marketplace |
| Benthall, Blake | Associated Press. (2014, Nov 6). FBI arrests alleged 'Silk Road 2.0' operator Blake Benthall. *NBCNews*. Retrieved from https://www.nbcnews.com/tech/security/fbi-arrests-alleged-silk-road-2-0-operator-blake-benthall-n242751<br>United States of America v. Blake Benthall a/k/a Defcon. 3:14-MJ-71397. N.D. Ca. (2014). |
| Brennan, Ross | BBC News England. (2017, Sept 25). Dark web drug supermarket duo from Huddersfield jailed. *BBCNews*. Retrieved from http://www.bbc.com/news/uk-england-41361137<br>Campbell, S. (2017, Sept 25). 'Arrogant' criminal, 28, who made hundreds of thousands of pounds selling drugs on the dark web with a university friend |

| | |
|---|---|
| | before spending the cash on gold and prostitutes is jailed for 13 years. *DailyMail*. Retrieved from http://www.dailymail.co.uk/news/article-4918624/Arrogant-criminal-sold-drugs-dark-web-jailed.html |
| Bridges, Shaun | Buntinx, J.P. (2016, Aug 20). Corrupt Silk Road investigator Shaun Bridges is grasping at straws. *The Merkle.* Retrieved from https://themerkle.com/corrupt-silk-road-investigator-shaun-bridges-is-grasping-at-straws/<br>Redman, J. (2017, Aug 16). FBI agent admits to stealing Silk Road bitcoins seized by U.S. Marshals. *BitcoinNews*. Retrieved from https://news.bitcoin.com/rogue-silk-road-agent-admits-to-stealing-bitcoins-seized-by-u-s-marshals/<br>USAO – Northern District of California. (2015, Mar 30). *Former federal agent charged with bitcoin money laundering and wire fraud* [Press Release]. Retrieved from https://www.justice.gov/opa/pr/former-federal-agents-charged-bitcoin-money-laundering-and-wire-fraud |
| Budovsky, Arthur (Liberty Reserve) | McCoy, K. (2013, May 28). Alleged $6 billion money-laundering network bust. *USA Today*. Retrieved from https://www.usatoday.com/story/money/business/2013/05/28/ny-indictment-filed-money-laundering-case/2366237/<br>Pagliery, J. (2016, May 6). Creator of online money Liberty Reserve gets 20 years in prison. *CNN*. Retrieved from http://money.cnn.com/2016/05/06/technology/liberty-reserve-prison/index.html<br>United States of America v. Liberty Reserve S.A., Arthur Budovsky, Vladimir Kats, Ahmed Yassine Abdelghani, Allan Esteban Hidalgo Jimenez, Azzedine El Amine, Mark Marmilev, & Maxim Chukharev. 1:13-cr-00368. S.D.N.Y. (2013).<br>USAO – Southern District of New York. (2016, May 6). *Liberty Reserve founder Arthur Budovsky sentenced in Manhattan federal court to 20 years for laundering hundreds of millions of dollars through his global digital currency business* [Press Release]. Retrieved from https://www.justice.gov/usao-sdny/pr/liberty-reserve-founder-arthur-budovsky-sentenced-manhattan-federal-court-20-years |
| Budovsky, Arthur (GoldAge) | Manhattan DA. (2014, Jan 29). *Testimony before the Department of Financial Services: Hearing on digital currency – Remarks as prepared* [Press Release]. Retrieved from https://www.justice.gov/usao-sdny/speech/new-york-state-department-financial-services-hearing-law-enforcement-and-virtual<br>Robert Morgenthaw v. Arthur Budovsky et al. S.C. of NYS. (2006). Retrieved from http://decisions.courts.state.ny.us/fcas/FCAS_docs/2006SEP/30040297020061SCIV.PDF |
| Burchard, David Ryan | USAO – Eastern District of California. (2018, Jan 16). *Dark-web drug traffickers sentenced in separate cases to 80 months and 70 months in prison* [Press Release]. Retrieved from https://www.justice.gov/usao-edca/pr/dark-web-drug-traffickers-sentenced-separate-cases-80-months-and-70-months-prison |

| | |
|---|---|
| Burnett Jr, Pierre | Ryckaert, V. (2017, Aug 9). Feds: Indy club manager sold drugs for bitcoin through the darknet. *IndyStar*. Retrieved from https://www.indystar.com/story/news/crime/2017/08/09/feds-indy-club-manager-drug-kingpin/551863001/<br>USAO – Southern District of Indiana. (2017, Aug 9). *Drug web investigation leads to conviction of Indianapolis drug trafficking* [Press Release]. Retrieved from https://www.justice.gov/usao-sdin/pr/dark-web-investigation-leads-conviction-indianapolis-drug-trafficker |
| Cazes, Alexandre | FBI. (2017, July 20). *Darknet takedown: Authorities shutter online criminal market AlphaBay* [Press release]. Retrieved from https://www.fbi.gov/news/stories/alphabay-takedown<br>USAO - California, Eastern. (2017, July 20). *AlphaBay, the largest online 'dark market,' shut down* [Press release]. Retrieved from https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down<br>United States of America v. Alexandre Cazes. 1:17-cr-00144. E.D. Cal. (2017). |
| Costanzo, Thomas | Stern, R. (2017, June 26). Brain scientist who brought AR-15 to Sky Harbor indicted in Arizona bitcoin probe. *Phoenix New Times*. Retrieved from http://www.phoenixnewtimes.com/news/peter-steinmetz-indicted-bitcoin-probe-brought-ar-15-to-phoenix-airport-9448123<br>United States of America v. Thomas Mario Costanzo. 2:17-cr-0058. D. Ariz. (2017).<br>United States of America v. Thomas Mario Costanzo and Peter Nathan Steinmetz. 2:17-cr-00585. D. Ariz. (2017).<br>Vitaris, B. (2017, May 14). Previously convicted bitcoin trader arrested for the possession of ammunition in the U.S. *DeepDotWeb*. Retrieved from https://www.deepdotweb.com/2017/05/14/previously-convicted-bitcoin-trader-arrested-possession-ammunition-us/ |
| Cottrell, George | Anglen, R. (2016, Dec 22). U.K. right-wing party adviser George Cottrell admits role in 'dark web' scam. *USAToday*. Retrieved from https://www.usatoday.com/story/news/nation-now/2016/12/22/george-cottrell-jailed-phoenix-irs/95772236/<br>Revesz, R. (2017, Mar 1). Nigel Farage's top aide sentenced for wire fraud. *Independent*. Retrieved from https://www.independent.co.uk/news/nigel-farage-ukip-george-cottrell-wire-fraud-sentenced-guilty-dark-web-money-laundering-a7606686.html |
| Crandall, Drew Wilson | Boyd, R. (2016, Nov 22). Cottonwood Heights drug bust one of the largest in Utah history. *Fox 13 Salt Lake City*. Retrieved from http://fox13now.com/2016/11/22/dea-investigating-drug-operation-near-cottonwood-heights-school/<br>Frandsen, T. (2017, June 1). Six charged in connection with Utah-based drug trafficking ring. *The Salt Lake Tribune*. https://www.sltrib.com/news/crime/2017/06/02/six-charged-in-connection-with-utah-based-drug-trafficking-ring/<br>USAO – District of Utah. (2017, May 31). *Drug trafficking organization faces indictment for involvement in manufacturing fake prescriptions drugs with fentanyl* [Press Release]. Retrieved from https://www.justice.gov/usao- |

| | |
|---|---|
| | ut/pr/drug-trafficking-organization-faces-indictment-involvment-manufacturing-fake<br>Whitehurst, L. (2017, Dec 14). U.S. prosecutors move to cash in on $8.5M in bitcoin seized in drug-ring arrest. *Chicago Tribune.* Retrieved from http://www.chicagotribune.com/news/nationworld/ct-drug-ring-bitcoin-seizure-20171214-story.html |
| Cristea, Leonardo | McGhee, T. (2016, Oct 17). Suspected drug dealer extradited from Romania to Colorado. *The Denver Post*. Retrieved from https://www.denverpost.com/2016/10/17/suspected-drug-dealer-extradited-romania-colorado/<br>USAO – District of Colorado. (2016, Oct 17). *Romania extradites alleged leader of "ItalianMafiaBrussels" drug trafficking organization to Colorado for prosecution* [Press Release]. Retrieved from https://www.justice.gov/usao-co/pr/romania-extradites-alleged-leader-italianmafiabrussels-drug-trafficking-organization |
| Davis, Gary | Giblin, R. (2017, Feb 28). Man to be extradited over Silk Road website, has appeal refused. *The Irish Times*. Retrieved from https://www.irishtimes.com/news/crime-and-law/courts/man-to-be-extradited-over-silk-road-website-has-appeal-refused-1.2992214<br>Redman, J. (2016, Jan 5). Silk Road moderator faces extradition to the U.S. *BitcoinNews*. Retrieved from https://news.bitcoin.com/silk-road-moderator-faces-extradition-us/<br>United States of America v. Andrew Michael Jones a/k/a Inigo, Gary Davis a/k/a Libertas, Peter Phillip Nash a/k/a Samesamebutdifferent a/k/a batman73 a/k/a symmetry a/k/a anonymousasshit. 1:13-CR-00950. S.D.N.Y. (2013). |
| Decker, Robert Kenneth | Aliens, C. (2017, May 26). DEA says four recent vendor busts are connected. *DeepDotWeb*. Retrieved from https://www.deepdotweb.com/2017/05/26/dea-says-four-recent-vendor-busts-connected/<br>USAO – Southern District of Florida. (2017, May 11). *Fourth defendant charged with selling controlled substances in exchange for virtual currencies on the dark web* [Press Release]. Retrieved from https://www.justice.gov/usao-sdfl/pr/fourth-defendant-charged-selling-controlled-substances-exchange-virtual-currencies-dark |
| Dhanani, Omar | United States of America v. Andrew Mantovani, David Appleyard, Anatoly Tyukanov, Kenneth J. Flurry, Kim Taylor, Jeremy Stephens, Matthew Johnson, Brandon L. Monchamp, Wesley A. Lanning, Alexander Palacio, Omar Dhanani, Marcelo del Mazo, Paul A. Mendel Jr., Beau Anthony Franks, Jeremy Zielinski, Aleksi Kolarov, Kaspar Kivi, Rogerio Rodrigues, and Karin Andersson. 2:04-cr-00786. D.N.J. (2004).<br>USAO - District of Columbia. (2005, November 18). *Six defendants plead guilty in internet identity theft and credit card fraud conspiracy* [Press release]. Retrieved from https://www.justice.gov/archive/opa/pr/2005/November/05_crm_619.html |
| Downey, Barry | Broache, A. (2007, Apr 30). E-gold charged with money laundering. *CNet*. |

| | |
|---|---|
| | Retrieved from https://www.cnet.com/news/e-gold-charged-with-money-laundering/<br>USAO – District of Columbia. (2008, July 21). *Digital currency business E-gold pleads guilty to money laundering and illegal money transmitting charges* [Press Release]. Retrieved from https://www.justice.gov/archive/criminal/cybercrime/press-releases/2008/egoldPlea.pdf |
| Dundoo, Anish | TNM Staff. (2017, July 13). Hyd drug bust: Former NASA scientist arrested, notices sent to Tollywood personalities. *The News Minute*. Retrieved from https://www.thenewsminute.com/article/hyd-drug-bust-former-nasa-scientist-arrested-notices-sent-tollywood-personalities-65089<br>Vitaris, B. (2017, Aug 1). Ex-NASA scientist arrested in Hyderabad for dealing drugs. *DeepDotWeb*. Retrieved from https://www.deepdotweb.com/2017/08/01/ex-nasa-scientist-arrested-hyderabad-dealing-drugs/ |
| Elshinawy, Mohamed | Knezevich, A. (2017, Aug 15). Edgewood man pleads guilty to aiding ISIS. *BaltimoreSun*. Retrieved from http://www.baltimoresun.com/news/maryland/crime/bs-md-ha-isis-egewood-man-20170815-story.html<br>Solomon, F. (2017, Aug 11). ISIS used eBay to send money to a U.S. operative, investigators say. *Time*. Retrieved from http://time.com/4896684/islamic-state-ebay-paypal/<br>United States of America v. Mohamed Elshinawy. 1:16-CR-00009. D. Md. (2016).<br>USAO – District of Maryland. (2016, Jan 14). *Maryland man indicted for conspiring to provide and for providing material support to ISIL* [Press Release]. Retrieved from https://www.justice.gov/opa/pr/maryland-man-indicted-conspiring-provide-and-providing-material-support-isil |
| Enos, Kyle | BBC News Wales. (2018, Feb 5). Newport man Kyle Enos jailed for dark web fentanyl drug deals. *BBC News*. Retrieved from http://www.bbc.com/news/uk-wales-south-east-wales-42943114<br>Corcoran, K. (2018, Feb 5). This is the dark web advert a drug dealer used to sell fentanyl for bitcoin. *Business Insider*. Retrieved from http://www.businessinsider.com/read-ad-used-by-dark-web-dealer-kyle-enos-to-sell-fentanyl-for-bitcoin-2018-2<br>Deaerden, L. (2018, Feb 5). Fentanyl: Man who posted deadly drug around the world from Welsh flat jailed. *Independent*. Retrieved from https://www.independent.co.uk/news/uk/crime/fentanyl-fentanil-drug-china-white-dark-web-dealer-jailed-wales-kyle-enos-nca-police-investigation-a8195961.html |
| Faiella, Robert | Associated Press (2015, Jan 20). Robert Faiella sentenced to 4 years for enabling Silk Road transactions. *CBC News*. Retrieved from http://www.cbc.ca/news/technology/robert-faiella-sentenced-to-4-years-for-enabling-silk-road-transactions-1.2921103<br>United States of America v. Robert M. Faiella, & Charlie Shrem. 1:14-cr-00243. S.D.N.Y. (2014).<br>United States of America v. Robert M. Faiella, & Charlie Shrem. 1:14-mag-00164. |

| | |
|---|---|
| | S.D.N.Y. (2014).<br>USAO – Southern District of New York. (2014, Jan 27). *Manhattan U.S. Attorney announces charges against bitcoin exchangers, including CEO of bitcoin exchange company, for scheme to sell and launder over $1 million in bitcoins related to Silk Road drug trafficking* [Press Release]. Retrieved from https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-bitcoin-exchangers-including-ceo<br>Zetter, K. (2015, Jan 21). Bitcoin exchange operator sentenced to 4 years for Silk Road transactions. *Wired*. Retrieved from https://www.wired.com/2015/01/bitcoin-exchange-operator-sentenced-4-years-silk-road-transactions/ |
| Farber, William James | CBS Staff. (2017, Aug 18). Feds bust 'dark web' drug ring operating out of Altadena gated community. *CBS Los Angeles.* Retrieved from http://losangeles.cbslocal.com/2017/08/18/feds-bust-dark-web-drug-ring-operating-out-of-altadena-gated-community/<br>Serna, J. (2017, Aug 18). Dark web drug network operated from gated community in Altadena, feds say. *LA Times*. Retrieved from http://www.latimes.com/local/lanow/la-me-ln-dark-web-network-altadena-20170818-story.html<br>USAO – Eastern District of California. (2017, Aug 17). *Six indicted for large-scale drug distribution via the dark web* [Press Release]. Retrieved from https://www.justice.gov/usao-edca/pr/six-indicted-large-scale-drug-distribution-dark-web |
| Farrell, Brian | Raymond, N. (2016, June 4). Silk Road's key player Brian Farrell sentenced to 8 years prison*. Huffington Post*. Retrieved from https://www.huffingtonpost.com/entry/silk-road-brian-farrell_us_57536fe7e4b0c3752dcde515<br>USAO – Western District of Washington. *Key player in Silk Road 2.0 arrested in Bellevue* [FBI Press Release]. Retrieved from https://www.fbi.gov/contact-us/field-offices/seattle/news/press-releases/key-player-in-silk-road-2.0-arrested-in-bellevue |
| Force IV, Carl Mark | Jeong, S. (2015, Oct 20). DEA agent who faked a murder and took bitcoins from Silk Road explains himself. *Motherboard*. Retrieved from https://motherboard.vice.com/en_us/article/8q845p/dea-agent-who-faked-a-murder-and-took-bitcoins-from-silk-road-explains-himself<br>USAO – Northern District of California. (2015, Mar 30). *Former federal agents charged with bitcoin money laundering and wire fraud* [Press Release]. Retrieved from https://www.justice.gov/opa/pr/former-federal-agents-charged-bitcoin-money-laundering-and-wire-fraud |
| Fusco, Kevin | Aliens, C. (2017, May 26). DEA says four recent vendor busts are connected. *DeepDotWeb*. Retrieved from https://www.deepdotweb.com/2017/05/26/dea-says-four-recent-vendor-busts-connected/<br>USAO – Southern District of Florida. (2017, May 11). *Fourth defendant charged with selling controlled substances in exchange for virtual currencies on the dark web* [Press Release]. Retrieved from https://www.justice.gov/usao- |

| | |
|---|---|
| | sdfl/pr/fourth-defendant-charged-selling-controlled-substances-exchange-virtual-currencies-dark |
| Garza, Homero Joshua | Securities and Exchange Commission v. Homero Joshua Garza, Gaw Miners LLC, and Zenminer LLC d/b/a Zen Cloud. 3:15-CV-01760. D. Conn. (2015).<br>Haig, S. (2017, Oct 5). GAW/Paycoin CEO Josh Garza held liable for $9 million USD for wire fraud. *BitcoinNews*. Retrieved from https://news.bitcoin.com/josh-garza-held-liable-9-million-usd-wire-fraud/<br>USAO – District of Connecticut. (2017, July 20). *Former virtual currency CEO pleads guilty to $9 million fraud scheme* [Press Release]. Retrieved from https://www.justice.gov/usao-ct/pr/former-virtual-currency-ceo-pleads-guilty-9-million-fraud-scheme |
| George IV, Jacob Theodore | Duncan, I. (2014, Sept 5). Silk Road drug dealer gets six years prison. *The Baltimore Sun*. Retrieved from http://www.baltimoresun.com/news/maryland/crime/bs-md-silk-road-sentencing-20140905-story.html<br>Sandvik, R.A. (2013, Nov 7). Feds reveal arrest of another Silk Road vendor, did he become an informant? *Forbes*. Retrieved from https://www.forbes.com/sites/runasandvik/2013/11/07/feds-reveal-arrest-of-another-silk-road-vendor-did-he-become-an-informant/#53b6557e2635<br>United States of America v. Jacob Theodore George IV a/k/a digitalink. 1:13-CR-00593. D. Md. (2013). |
| Gledhill, Aaron | BBC News England. (2017, Sept 25). Dark web drug supermarket duo from Huddersfield jailed. *BBCNews*. Retrieved from http://www.bbc.com/news/uk-england-41361137<br>Campbell, S. (2017, Sept 25). 'Arrogant' criminal, 28, who made hundreds of thousands of pounds selling drugs on the dark web with a university friend before spending the cash on gold and prostitutes is jailed for 13 years. *DailyMail*. Retrieved from http://www.dailymail.co.uk/news/article-4918624/Arrogant-criminal-sold-drugs-dark-web-jailed.html |
| Goyal, Mahesh | Anash, K. (2017, Nov 17). Two arrested in Delhi for selling drugs via the dark web. *DeepDotWeb*. Retrieved from https://www.deepdotweb.com/2017/11/17/two-arrested-delhi-selling-drugs-via-dark-web/<br>F.E. Online. (2017, Nov 7). What is deep web? Here is how police bust drug racket involving bitcoins in Delhi. *Financial Express*. Retrieved from https://www.financialexpress.com/india-news/what-is-deep-web-here-is-how-police-bust-drug-racket-involving-bitcoins-in-delhi/922394/<br>Singh, K.P. (2017, Nov 7). 'Dark web' to bitcoin: Delhi cops bust gang that bought drugs for rave parties. *Hindustan Times*. Retrieved from https://www.hindustantimes.com/delhi-news/dark-web-to-bitcon-delhi-cops-bust-gang-that-bought-drugs-for-rave-parties/story-nviB9kYF8wuvaWNUbWc3jJ.html |
| Gray, Lee | Ryckaert, V. (2017, Aug 9). Feds: Indy club manager sold drugs for bitcoin through the darknet. *IndyStar*. Retrieved from https://www.indystar.com/story/news/crime/2017/08/09/feds-indy-club- |

| | |
|---|---|
| | manager-drug-kingpin/551863001/<br>USAO – Southern District of Indiana. (2017, Aug 9). *Drug web investigation leads to conviction of Indianapolis drug trafficking* [Press Release]. Retrieved from https://www.justice.gov/usao-sdin/pr/dark-web-investigation-leads-conviction-indianapolis-drug-trafficker<br>USAO – Souther District of Indiana. (2015, Aug 18). *Camby Indiana man indicted on drug and money laundering charges using underground websites* [Press Release]. Retrieved from https://www.justice.gov/usao-sdin/pr/camby-indiana-man-indicted-drug-and-money-laundering-charges-using-underground-websites |
| Haddow, Renwick | United States of America v. Renwick Haddow. 1:17-MAG-04939. S.D.N.Y. (2017).<br>USAO – Southern District of New York. *Charges unsealed against British citizen for defrauding investors of more than $36 million* [Press Release]. Retrieved from https://www.justice.gov/usao-sdny/pr/charges-unsealed-against-british-citizen-defrauding-investors-more-36-million |
| Hall, Kyle | BBC News. (2015, Sept 4). Two in court over dark web drugs case involving bitcoin. *BBC News*. Retrieved from http://www.bbc.com/news/uk-northern-ireland-foyle-west-34151553<br>Young, J. (2017, Jan 19). Three Irishmen jailed for dark web drug trading, use of cash vital in crackdown. *DeepDotWeb*. Retrieved from https://www.deepdotweb.com/2017/01/19/three-irishmen-jailed-dark-web-drug-trading-use-cash-vital-crackdown/ |
| Hodzic, Ramiz | Hughes, S. & Clifford, B. (2017, May 25). First he became an American – Then he joined ISIS. *The Atlantic*. Retrieved from https://www.theatlantic.com/international/archive/2017/05/first-he-became-an-americanthen-he-joined-isis/527622/<br>Masunaga, S. (2015, Feb 8). 6 Bosnian immigrants indicted in alleged overseas terror financing ring. *Los Angeles Times*. Retrieved from http://www.latimes.com/nation/la-na-terror-arrest-20150208-story.html<br>United States of America v. Ramiz Zijad Hodzic, Sedina Unkick Hodzic, Nihad Rosic, Mediha Medy Salkicevic, Armin Harcevic, and Jasminka Ramic. 4:15-CR-00049. E.D. Mo. (2015).<br>USAO – Eastern District of Missouri. (2015, Feb 6). *Six defendants charged with conspiracy and providing material support to terrorists* [Press Release]. Retrieved from https://www.justice.gov/opa/pr/six-defendants-charged-conspiracy-and-providing-material-support-terrorists |
| Hodzic, Sedina | Hughes, S. & Clifford, B. (2017, May 25). First he became an American – Then he joined ISIS. *The Atlantic*. Retrieved from https://www.theatlantic.com/international/archive/2017/05/first-he-became-an-americanthen-he-joined-isis/527622/<br>Masunaga, S. (2015, Feb 8). 6 Bosnian immigrants indicted in alleged overseas terror financing ring. *Los Angeles Times*. Retrieved from http://www.latimes.com/nation/la-na-terror-arrest-20150208-story.html<br>United States of America v. Ramiz Zijad Hodzic, Sedina Unkick Hodzic, Nihad Rosic, Mediha Medy Salkicevic, Armin Harcevic, and Jasminka Ramic. 4:15-CR-00049. E.D. Mo. (2015). |

| | |
|---|---|
| | USAO – Eastern District of Missouri. (2015, Feb 6). *Six defendants charged with conspiracy and providing material support to terrorists* [Press Release]. Retrieved from https://www.justice.gov/opa/pr/six-defendants-charged-conspiracy-and-providing-material-support-terrorists |
| Ignatova, Ruja | Higgins, S. (2017, Jul 11). Indian police prepare charges against OneCoin founder Ruja Ignatova. *CoinDesk*. Retrieved from https://www.coindesk.com/indian-police-charges-onecoin-founder-ruja-ignatova/<br>Tassev, L. (2018, Jan 20). OneCoin offices raided in Sofia, servers shut down. *BitcoinNews*. Retrieved from https://news.bitcoin.com/onecoin-offices-raided-in-sofia-servers-shut-down/ |
| Jackson, Douglas | Broache, A. (2007, Apr 30). E-gold charged with money laundering. *CNet*. Retrieved from https://www.cnet.com/news/e-gold-charged-with-money-laundering/<br>USAO – District of Columbia. (2008, July 21). *Digital currency business E-gold pleads guilty to money laundering and illegal money transmitting charges* [Press Release]. Retrieved from https://www.justice.gov/archive/criminal/cybercrime/press-releases/2008/egoldPlea.pdf |
| Jackson, Reid | Broache, A. (2007, Apr 30). E-gold charged with money laundering. *CNet*. Retrieved from https://www.cnet.com/news/e-gold-charged-with-money-laundering/<br>USAO – District of Columbia. (2008, July 21). *Digital currency business E-gold pleads guilty to money laundering and illegal money transmitting charges* [Press Release]. Retrieved from https://www.justice.gov/archive/criminal/cybercrime/press-releases/2008/egoldPlea.pdf |
| Jeong, FNU | Korea Herald Staff. (2014, Mar 17). Korean-American caught buying illegal drugs with bitcoin. *Korean Herald*. Retrieved from http://www.koreaherald.com/view.php?ud=20140317001000 |
| Jian, Chirag | India Today Staff. (2017, Mar 29). LSD worth Rs 70 lakh seized, channel associate producer among. *India Today*. Retrieved from https://www.indiatoday.in/pti-feed/story/lsd-worth-rs-70-lakh-seized-channel-associate-producer-among-898988-2017-03-29<br>Naidu, J.S. (2017, May 6). U.S. student visa, bitcoins, darknet: Here's how 5 men fooled airport scanners, smuggled LSD worth 70 lakh into Mumbai. *Hindustan Times*. Retrieved from https://www.hindustantimes.com/mumbai-news/us-student-visa-bitcoins-darknet-here-s-how-5-men-fooled-airport-scanners-smuggled-lsd-worth-70-lakh-into-mumbai/story-EOUqreSsqOjW7EX6p1VVVI.html |
| Jirikovsky, Tomas | Remand, J. (2017, April 5). Darknet market operators who stole 40 thousand BTC face prison time. *BitcoinNews*. Retrieved from https://news.bitcoin.com/darknet-market-operators-who-stole-40-thousand-btc-face-prison-time/ |

| | |
|---|---|
| | The Prague Monitor Staff. (2017, October 10). Czech man sent to prison for stealing bitcoins. *The Prague Daily Monitor*. Retrieved from http://www.praguemonitor.com/2017/10/10/czech-man-sent-prison-stealing-bitcoins |
| Kalra, Kamal | Anash, K. (2017, Nov 17). Two arrested in Delhi for selling drugs via the dark web. *DeepDotWeb*. Retrieved from https://www.deepdotweb.com/2017/11/17/two-arrested-delhi-selling-drugs-via-dark-web/<br>F.E. Online. (2017, Nov 7). What is deep web? Here is how police bust drug racket involving bitcoins in Delhi. *Financial Express*. Retrieved from https://www.financialexpress.com/india-news/what-is-deep-web-here-is-how-police-bust-drug-racket-involving-bitcoins-in-delhi/922394/<br>Singh, K.P. (2017, Nov 7). 'Dark web' to bitcoin: Delhi cops bust gang that bought drugs for rave parties. *Hindustan Times*. Retrieved from https://www.hindustantimes.com/delhi-news/dark-web-to-bitcon-delhi-cops-bust-gang-that-bought-drugs-for-rave-parties/story-nviB9kYF8wuvaWNUbWc3jJ.html |
| Karpeles, Mark | Popper, N. (2017, July 27). Bitcoin exchange was a nexus of crime, indictment says. *The New York Times*. Retrieved from https://www.nytimes.com/2017/07/27/business/dealbook/bitcoin-exchange-was-a-nexus-of-crime-indictment-says.html?mtrref=undefined&gwh=7C95D89296EA01EC9EFC98B77D25C3FD&gwt=pay<br>Shares, D. (2016, July 14). Former Mt. Gox exchange CEO Mark Karpeles has been released from prison. *Bitcoin News*. Retrieved from https://news.bitcoin.com/former-mt-gox-exchange-ceo-mark-karpeles-released-prison/ |
| Kelly, Joshua | Aliens, C. (2017, May 26). DEA says four recent vendor busts are connected. *DeepDotWeb*. Retrieved from https://www.deepdotweb.com/2017/05/26/dea-says-four-recent-vendor-busts-connected/<br>USAO – Southern District of Florida. (2017, May 11). *Fourth defendant charged with selling controlled substances in exchange for virtual currencies on the dark web* [Press Release]. Retrieved from https://www.justice.gov/usao-sdfl/pr/fourth-defendant-charged-selling-controlled-substances-exchange-virtual-currencies-dark |
| Kennedy, Ryan | Redman, J. (2017, Oct 20). UK police force investigate the defunct Mintpal Exchange and owner. *BitcoinNews*. Retrieved from https://news.bitcoin.com/uk-police-force-investigates-the-defunct-mintpal-exchange-and-owner/<br>Wilmoth, J. (2017, Sept 19). Alleged 'Moolah' bitcoin thief Ryan Kennedy faces first court hearing. *CCN*. Retrieved from https://www.ccn.com/alleged-moolah-fraudster-ryan-kennedy-faces-first-court-hearing/ |
| Khan, Arbaz | India Today Staff. (2017, Mar 29). LSD worth Rs 70 lakh seized, channel associate producer among. *India Today*. Retrieved from |

| | |
|---|---|
| | https://www.indiatoday.in/pti-feed/story/lsd-worth-rs-70-lakh-seized-channel-associate-producer-among-898988-2017-03-29<br>Naidu, J.S. (2017, May 6). U.S. student visa, bitcoins, darknet: Here's how 5 men fooled airport scanners, smuggled LSD worth 70 lakh into Mumbai. *Hindustan Times*. Retrieved from https://www.hindustantimes.com/mumbai-news/us-student-visa-bitcoins-darknet-here-s-how-5-men-fooled-airport-scanners-smuggled-lsd-worth-70-lakh-into-mumbai/story-EOUqreSsqOjW7EX6p1VVVI.html |
| Kirin, Sergei | Alcindor, Y. (2014, July 23). Arrests made in global, $1.6M StubHub cybertheft case. *USA Today*. Retrieved from https://www.usatoday.com/story/tech/2014/07/23/cyberthieves-stubhub-fraud/13036243/ |
| Koffie, Henry | USAO – Western District of Pennsylvania (2017, Aug 3). *Darby man charged for distributing fentanyl* [Press Release]. Retrieved from https://www.justice.gov/usao-wdpa/pr/darby-man-charged-distributing-fentanyl<br>USAO – Western District of Pennsylvania. (2017, July 12). *Alleged Philadelphia fentanyl distributor arraigned on federal drug trafficking charges* [ICE Press Release]. Retrieved from https://www.ice.gov/news/releases/alleged-philadelphia-fentanyl-distributor-arraigned-federal-drug-trafficking-charges<br>Wood, S. (2017, July 15). AlphaBay, one-stop shop for criminals, is shut down; alleged mastermind dead. *The Inquirer Daily News*. Retrieved from http://www.philly.com/philly/business/alphabay-one-stop-shop-for-criminals-shuts-down-alleged-mastermind-dead-20170715.html |
| Koleski, Victoria | United States of America v. Brian Parker & Victoria Koleski. 1:17-MAG-04123. D.N.J. (2017).<br>USAO – District of New Jersey. (2017, Aug 29). *Two individuals charged in synthetic opioid drug conspiracy following overdose death* [Press Release]. Retrieved from https://www.justice.gov/usao-nj/pr/two-individuals-charged-synthetic-opioid-drug-conspiracy-following-overdose-death<br>Vitaris, B. (2017, Sept 13). Police busted NYC synthetic drug dealer. *DeepDotWeb*. Retrieved from https://www.deepdotweb.com/2017/09/13/police-busted-nyc-synthetic-drug-dealer/ |
| Lailan, Kurt | BBC News England. (2017, Dec 20). Portsmouth dark net drug dealer jailed for 16 years. *BBC News*. Retrieved from http://www.bbc.com/news/uk-england-hampshire-42424358<br>Fishwick, B. (2017, Dec 19). Portsmouth drug dealer who used the dark web to sell thousands of ecstasy tablets is jailed for 16 years. *Portsmouth News*. Retrieved from https://www.portsmouth.co.uk/news/crime/portsmouth-drug-dealer-who-used-the-dark-web-to-sell-thousands-of-ecstasy-tablets-is-jailed-for-16-years-1-8298129 |
| Lemons, Bryan Anthony | CBS Staff. (2017, Aug 18). Feds bust 'dark web' drug ring operating out of Altadena gated community. *CBS Los Angeles.* Retrieved from http://losangeles.cbslocal.com/2017/08/18/feds-bust-dark-web-drug-ring-operating-out-of-altadena-gated-community/ |

| | |
|---|---|
| | Serna, J. (2017, Aug 18). Dark web drug network operated from gated community in Altadena, feds say. *LA Times*. Retrieved from http://www.latimes.com/local/lanow/la-me-ln-dark-web-network-altadena-20170818-story.html<br>USAO – Eastern District of California. (2017, Aug 17). *Six indicted for large-scale drug distribution via the dark web* [Press Release]. Retrieved from https://www.justice.gov/usao-edca/pr/six-indicted-large-scale-drug-distribution-dark-web |
| Leslie, Chrissano | Aliens, C. (2017, May 26). DEA says four recent vendor busts are connected. *DeepDotWeb*. Retrieved from https://www.deepdotweb.com/2017/05/26/dea-says-four-recent-vendor-busts-connected/<br>USAO – Southern District of Florida. (2017, May 11). *Fourth defendant charged with selling controlled substances in exchange for virtual currencies on the dark web* [Press Release]. Retrieved from https://www.justice.gov/usao-sdfl/pr/fourth-defendant-charged-selling-controlled-substances-exchange-virtual-currencies-dark |
| Leslie, Dana Marie | Dellinger, A.J. (2018, Jan 23). Opioid crisis: Veterinarian bought fentanyl with bitcoin on the dark web. *International Business Times.* Retrieved from http://www.ibtimes.com/opioid-crisis-veterinarian-bought-fentanyl-bitcoin-dark-web-2644289<br>Gilmour, J. (2018, Jan 23). Alabama man arrested for buying overseas fentanyl shipped in teddy bear, police say. *Miami Herald*. Retrieved from http://www.miamiherald.com/news/nation-world/national/article196224384.html |
| Lord, Michael | Aliens, C. (2017, June 12). Prison time for father and son caught selling bitcoin. *DeepDotWeb*. Retrieved from https://www.deepdotweb.com/2017/06/12/prison-time-for-father-and-son-caught-selling-bitcoin/<br>USAO – Western District of Louisiana (2017, May 25). *Former Shreveport chiropractor, son sentenced for operating illegal bitcoin exchange business* [Press Release]. Retrieved from https://www.justice.gov/usao-wdla/pr/former-shreveport-chiropractor-son-sentenced-operating-illegal-bitcoin-exchange<br>USAO – Western District of Louisiana. (2016, Apr 20). *Former Shreveport chiropractor, son plead guilty to operating illegal bitcoin exchange business* [Press Release]. Retrieved from https://www.justice.gov/usao-wdla/pr/former-shreveport-chiropractor-son-plead-guilty-operating-illegal-bitcoin-exchange |
| Lord, Randall | Aliens, C. (2017, June 12). Prison time for father and son caught selling bitcoin. *DeepDotWeb*. Retrieved from https://www.deepdotweb.com/2017/06/12/prison-time-for-father-and-son-caught-selling-bitcoin/<br>USAO – Western District of Louisiana (2017, May 25). *Former Shreveport chiropractor, son sentenced for operating illegal bitcoin exchange business* [Press Release]. Retrieved from https://www.justice.gov/usao- |

| | |
|---|---|
| | wdla/pr/former-shreveport-chiropractor-son-sentenced-operating-illegal-bitcoin-exchange<br>USAO – Western District of Louisiana. (2016, Apr 20). *Former Shreveport chiropractor, son plead guilty to operating illegal bitcoin exchange business* [Press Release]. Retrieved from https://www.justice.gov/usao-wdla/pr/former-shreveport-chiropractor-son-plead-guilty-operating-illegal-bitcoin-exchange |
| Luciano, Michael | United States of America v. Michael Luciano & Phillip Luciano. 1:17-MAG-06344. S.D.N.Y. (2017).<br>USAO – Southern District of New York. (2017, Aug 23). *Father and son charged with selling fentanyl and oxycodone on the dark web* [Press Release]. Retrieved from https://www.justice.gov/usao-sdny/pr/father-and-son-charged-selling-fentanyl-and-oxycodone-dark-web<br>Winter, T. & Siemaszko, C. (2017, Aug 23). NYC father and son busted for alleged opioid dealing on the darknet. *NBC News*. Retrieved from https://www.nbcnews.com/storyline/americas-heroin-epidemic/new-york-dad-son-busted-darknet-opioid-dealing-n795206 |
| Luciano, Philip | United States of America v. Michael Luciano & Phillip Luciano. 1:17-MAG-06344. S.D.N.Y. (2017).<br>USAO – Southern District of New York. (2017, Aug 23). *Father and son charged with selling fentanyl and oxycodone on the dark web* [Press Release]. Retrieved from https://www.justice.gov/usao-sdny/pr/father-and-son-charged-selling-fentanyl-and-oxycodone-dark-web<br>Winter, T. & Siemaszko, C. (2017, Aug 23). NYC father and son busted for alleged opioid dealing on the darknet. *NBC News*. Retrieved from https://www.nbcnews.com/storyline/americas-heroin-epidemic/new-york-dad-son-busted-darknet-opioid-dealing-n795206 |
| M., Joey | Cox, J. (2016, January 20). Dutch police bust multi-million dollar bitcoin laundering ring. *Motherboard.* Retrieved from https://motherboard.vice.com/en_us/article/ezpnze/dutch-police-bust-multi-million-dollar-bitcoin-laundering-ring<br>Sterling, T. (2016, January 20). Dutch arrest 10 men suspected of using bitcoin to launder money. *Reuters.* Retrieved from https://www.reuters.com/article/us-netherlands-crime-bitcoin/dutch-arrest-10-men-suspected-of-using-bitcoin-to-launder-money-idUSKCN0UY0V8<br>The Guardian Staff (2016, January 20). Ten arrested in Netherlands over bitcoin money-laundering allegations. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2016/jan/20/bitcoin-netherlands-arrests-cars-cash-ecstasy<br>The Sun Daily Staff (2017, October 25). Six in Dutch court over 'bitcoin drug money laundering'. *The Sun Daily*. Retrieved from http://www.thesundaily.my/news/2017/10/25/six-dutch-court-over-bitcoin-drug-money-laundering |
| Mannion, Neil | Breen, S. (2015, Dec 21). 'Mastermind' of pills, L.S.D. and pot website gets 6 ½ years. *The Irish Sun*. Retrieved from https://www.thesun.ie/archives/irish-news/119822/mastermind-of-pills-l-s-d-and-pot-website-gets-6-%C2%BD- |

| | |
|---|---|
| | years/<br>Roberts, B. (2016, Nov 3). Dublin pair sentenced over 'dark net' drug selling operation. *The Irish Times*. Retrieved from https://www.irishtimes.com/news/crime-and-law/dark-net-drug-dealer-loses-appeal-over-jail-sentence-1.2853540 |
| Moffitt, Nicholas C. | Lehman, D. (2013, Aug 23). Police: Queensbury shop owner bought drugs on Silk Road website. *The Post Star*. Retrieved from https://poststar.com/news/local/police-queensbury-shop-owner-bought-drugs-on-silk-road-website/article_8f45d126-0c1f-11e3-a590-001a4bcf887a.html |
| Murgio, Anthony | Goldstein, M. (2015, Aug 10). Man charged in bitcoin scheme appears in New York court. *The New York Times*. Retrieved from https://www.nytimes.com/2015/08/11/business/man-charged-in-bitcoin-scheme-appears-in-new-york-court.html<br>Stempel, J. (2017, June 27). Bitcoin exchange operator tied to hacks gets five-and-a-half years U.S. prison. *Reuters*. Retrieved from https://www.reuters.com/article/us-cyber-jpmorgan-murgio/bitcoin-exchange-operator-tied-to-hacks-gets-five-and-a-half-years-u-s-prison-idUSKBN19I2JM<br>United States of America v. Anthony Murgio. 1:17-cr-00769. (2017).<br>USAO – Southern District of New York. (2017, June 27). *Operator of unlawful bitcoin exchange sentenced to more than 5 years in prison for leading multimillion dollar money laundering and fraud scheme* [Press Release]. Retrieved from https://www.justice.gov/usao-sdny/pr/operator-unlawful-bitcoin-exchange-sentenced-more-5-years-prison-leading-multimillion |
| Naim, Bahrun | Chan, F. (2017, Dec 4). Efforts under way to verify chatter about death of Indonesian ISIS leader linked to Marina Bay plot. *Straits Times*. Retrieved from https://www.straitstimes.com/asia/se-asia/efforts-underway-to-verify-chatter-about-the-death-of-indonesian-isis-leader-linked-to<br>Soeriaatmadja, W. (2017, Jan 10). Indonesian militant used PayPal to fund terror acts. *Straits Times*. Retrieved from https://www.straitstimes.com/asia/se-asia/indonesian-militant-used-paypal-to-fund-terror-acts |
| O'Connor, Richard | Breen, S. (2015, Dec 21). 'Mastermind' of pills, L.S.D. and pot website gets 6 ½ years. *The Irish Sun*. Retrieved from https://www.thesun.ie/archives/irish-news/119822/mastermind-of-pills-l-s-d-and-pot-website-gets-6-%C2%BD-years/<br>Roberts, B. (2016, Nov 3). Dublin pair sentenced over 'dark net' drug selling operation. *The Irish Times*. Retrieved from https://www.irishtimes.com/news/crime-and-law/dark-net-drug-dealer-loses-appeal-over-jail-sentence-1.2853540 |
| Okparaeke, Chukwuemeka | Ashok, I. (2017, Mar 21). AlphaBay drug lord arrested after he was spotted wearing latex gloves while dropping off packages. *YahooNews*. Retrieved from https://sg.news.yahoo.com/alphabay-drug-lord-arrested-spotted-115542179.html<br>United States of America v. Chukwuemeka Okparaeke a/k/a Emeka. 1:17-MAG- |

| | |
|---|---|
| | 01972. S.D.N.Y. (2017).<br>USAO – Southern District of New York. (2017, Mar 20). *Acting Manhattan U.S. Attorney announces the arrest of Chukwuemeka Okparaeke for conspiracy to distribute analogues of fentanyl on the darknet* [Press Release]. Retrieved from https://www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-arrest-chukwuemeka-okparaeke-conspiracy |
| Owen, Christopher | Illawarra Mercury Staff. (2013, May 17). Jail time for Figtree web trafficker. *Illawarra Mercury News*. Retrieved from https://www.illawarramercury.com.au/story/1507381/jail-time-for-figtree-web-trafficker/ |
| Panzeca, Amy | Budd, L. (2018, Jan 17). Springboro teacher's criminal case headed back to trial. *Dayton Daily News*. Retrieved from https://www.daytondailynews.com/news/crime--law/springboro-teacher-criminal-case-headed-back-trial/tQLSnJqETTOMEQOcOaFoUO/ |
| Panzeca's Son, Amy | Budd, L. (2018, Jan 17). Springboro teacher's criminal case headed back to trial. *Dayton Daily News*. Retrieved from https://www.daytondailynews.com/news/crime--law/springboro-teacher-criminal-case-headed-back-trial/tQLSnJqETTOMEQOcOaFoUO/ |
| Parker, Brian | United States of America v. Brian Parker & Victoria Koleski. 1:17-MAG-04123. D.N.J. (2017).<br>USAO – District of New Jersey. (2017, Aug 29). *Two individuals charged in synthetic opioid drug conspiracy following overdose death* [Press Release]. Retrieved from https://www.justice.gov/usao-nj/pr/two-individuals-charged-synthetic-opioid-drug-conspiracy-following-overdose-death<br>Vitaris, B. (2017, Sept 13). Police busted NYC synthetic drug dealer. *DeepDotWeb*. Retrieved from https://www.deepdotweb.com/2017/09/13/police-busted-nyc-synthetic-drug-dealer/ |
| Pollard, Richard | Associated Press. (2016, May 31). Australian police to auction $13m in confiscated bitcoins. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2016/may/31/australian-police-to-auction-13m-in-confiscated-bitcoins<br>Redman, J. (2016, May 30). Ernst & Young to auction 24,000 confiscated bitcoins in Australia. *BitcoinNews*. Retrieved from https://news.bitcoin.com/ernst-young-auction-24-thousand-btc/ |
| Price, Theodore | Associated Press. (2017, July 20). Man tells federal officials he stole $40 million in bitcoin. *U.S. News*. Retrieved from https://www.usnews.com/news/best-states/pennsylvania/articles/2017-07-20/man-tells-federal-officials-he-stole-40-million-in-bitcoin<br>Swenson, K. (2017, July 24). Pennsylvania police, hunting for stolen laptops, say they stumbled on $40 million bitcoin scam. *Washington Post*. Retrieved from https://www.washingtonpost.com/news/morning-mix/wp/2017/07/24/pennsylvania-police-hunting-for-stolen-laptops-say-they-stumbled-on-40-million-bitcoin-scam/?utm_term=.511503eb502f |

| | |
|---|---|
| Prime, Joel Paul | Aliens, C. (2018, Jan 16). Australian drug trafficker caught using his own PO box. *DeepDotWeb*. Retrieved from https://www.deepdotweb.com/2018/01/16/australian-drug-trafficker-caught-using-po-box/<br>M.C. (2018, Feb 9). Dark web seller pleads guilty to 10+ counts of drug trafficking. *DarkWebNews*. Retrieved from https://darkwebnews.com/drugs/guilty-plea-for-darknet-drug-seller/ |
| Reid, Edward James Montague | Times of News Staff. (2017, Sept 29). Tokyo cops nab British national in bitcoin sales of cocaine in Roppongi. *Times of News Japan*. Retrieved from http://japan.timesofnews.com/tokyo-cops-nab-british-national-in-bitcoin-sales-of-cocaine-in-roppongi.html |
| S., Maximillian | Dunn, M. (2015, Nov 7). Teen sentenced to seven years jail for running $6.7 million darknet drug trade from his mother's home. *AU News*. Retrieved from http://www.news.com.au/technology/online/teen-sentenced-to-seven-years-jail-for-running-67-million-darknet-drug-trade-from-his-mothers-home/news-story/885fd12852346a5a307750768ccbd6fc<br>Locker. T. (20105, Nov 3). Germany's most notorious darknet drug dealer sentenced to only 7 years. *Motherboard*. Retrieved from https://motherboard.vice.com/en_us/article/d7yzjy/germanys-most-notorious-darknet-drug-dealer-sentenced-to-only-7-years<br>Vitaris, B. (2015, Nov 7). Shiny Flakes sentenced to 7 years. *DeepDotWeb*. Retrieved from https://www.deepdotweb.com/2015/11/07/shiny-flakes-sentenced-to-7-years/ |
| Sadler, Steven Lloyd | Associated Press. (2015, Mar 19). Bellevue man gets 5 years for selling drugs on 'Silk Road' Internet site. *The Seattle Times*. Retrieved from https://www.seattletimes.com/seattle-news/crime/bellevue-man-gets-5-years-for-selling-drugs-on-silk-road-internet-site/<br>United States of America v. Steven Lloyd Sadler & Jenna M. White. 2:13-MJ-00487. W.D. Wash. (2013). |
| Schell, David | DeepDotWeb Staff. (2014, Nov 21). Onymous: Durham couple indicted. *DeepDotWeb*. Retrieved from https://www.deepdotweb.com/2014/11/21/onymous-durham-couple-indicted/<br>USAO – Eastern District of California. (2014, Nov 20). *Butte County couple indicted for drug trafficking as part of Silk Road 2.0 takedown* [Press Release]. Retrieved from https://www.justice.gov/usao-edca/pr/butte-county-couple-indicted-drug-trafficking-part-silk-road-20-takedown |
| Schell, Teri | DeepDotWeb Staff. (2014, Nov 21). Onymous: Durham couple indicted. *DeepDotWeb*. Retrieved from https://www.deepdotweb.com/2014/11/21/onymous-durham-couple-indicted/<br>USAO – Eastern District of California. (2014, Nov 20). *Butte County couple indicted for drug trafficking as part of Silk Road 2.0 takedown* [Press Release]. Retrieved from https://www.justice.gov/usao-edca/pr/butte-county-couple-indicted-drug-trafficking-part-silk-road-20-takedown |

| | |
|---|---|
| Shahnaz, Zoobia | Peaster, W. (2017, December 14). U.S. woman indicted in first bitcoin terrorism laundering case. *BitsOnline*. Retrieved from https://www.bitsonline.com/woman-indicted-bitcoin-terrorism/<br>United States of America v. Zoobia Shahnaz. 1:17-CR-00690. E.D.N.Y. (2017).<br>USAO – Eastern District of New York. (2017, Dec 14). *Long Island woman indicted for bank fraud and money laundering to support terrorists* [Press Release]. Retrieved from https://www.justice.gov/usao-edny/pr/long-island-woman-indicted-bank-fraud-and-money-laundering-support-terrorists |
| Shamo, Aaron | Boyd, R. (2016, Nov 22). Cottonwood Heights drug bust one of the largest in Utah history. *Fox 13 Salt Lake City*. Retrieved from http://fox13now.com/2016/11/22/dea-investigating-drug-operation-near-cottonwood-heights-school/<br>Frandsen, T. (2017, June 1). Six charged in connection with Utah-based drug trafficking ring. *The Salt Lake Tribune*. https://www.sltrib.com/news/crime/2017/06/02/six-charged-in-connection-with-utah-based-drug-trafficking-ring/<br>USAO – District of Utah. (2017, May 31). *Drug trafficking organization faces indictment for involvement in manufacturing fake prescriptions drugs with fentanyl* [Press Release]. Retrieved from https://www.justice.gov/usao-ut/pr/drug-trafficking-organization-faces-indictment-involvment-manufacturing-fake<br>Whitehurst, L. (2017, Dec 14). U.S. prosecutors move to cash in on $8.5M in bitcoin seized in drug-ring arrest. *Chicago Tribune.* Retrieved from http://www.chicagotribune.com/news/nationworld/ct-drug-ring-bitcoin-seizure-20171214-story.html |
| Shrem, Charlie | Spaven, E. (2015, May 14). Bitcoin's 'first felon' Charlie Shrem begins 2-year sentence. *CoinDesk*. Retrieved from https://www.coindesk.com/bitcoins-first-felon-charlie-shrem-begins-2-year-sentence/<br>United States of America v. Robert M. Faiella, & Charlie Shrem. 1:14-cr-00243. S.D.N.Y. (2014).<br>United States of America v. Robert M. Faiella, & Charlie Shrem. 1:14-mag-00164. S.D.N.Y. (2014).<br>USAO – Southern District of New York. (2014, Jan 27). *Manhattan U.S. Attorney announces charges against bitcoin exchangers, including CEO of bitcoin exchange company, for scheme to sell and launder over $1 million in bitcoins related to Silk Road drug trafficking* [Press Release]. Retrieved from https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-bitcoin-exchangers-including-ceo |
| Simion, Filiip Lucian | McGhee, T. (2016, Oct 17). Suspected drug dealer extradited from Romania to Colorado. *The Denver Post*. Retrieved from https://www.denverpost.com/2016/10/17/suspected-drug-dealer-extradited-romania-colorado/<br>USAO – District of Colorado. (2016, Oct 17) *Romania extradites alleged leader of 'ItalianMafiaBrussels' drug trafficking organization to Colorado for prosecution* [Press Release]. Retrieved from https://www.justice.gov/usao-co/pr/romania-extradites-alleged-leader-italianmafiabrussels-drug-trafficking-organization |

| | |
|---|---|
| Sinclair, Richard | BBC News. (2015, Sept 4). Two in court over dark web drugs case involving bitcoin. *BBC News*. Retrieved from http://www.bbc.com/news/uk-northern-ireland-foyle-west-34151553<br>Erwin, A. (2016, Mar 19). Man ran $200k drugs empire from his bedroom. *Belfast Telegraph*. Retrieved from https://www.belfasttelegraph.co.uk/news/northern-ireland/man-ran-200k-drugs-empire-from-his-bedroom-34553802.html<br>Young, J. (2017, Jan 19). Three Irishmen jailed for dark web drug trading, use of cash vital in crackdown. *DeepDotWeb*. Retrieved from https://www.deepdotweb.com/2017/01/19/three-irishmen-jailed-dark-web-drug-trading-use-cash-vital-crackdown/ |
| Singh, Jagit | Singh, J. (2016, Dec 26). Six more arrested in Crown chit fund scam. *Tribune India*. Retrieved from http://www.tribuneindia.com/news/punjab/six-more-arrested-in-crown-chit-fund-scam/518969.html |
| Smith, Gregory | Clancy, A. (2017, Aug 16). Seattle man suspected of importing fentanyl from China through mail. *Kiro 7*. Retrieved from https://www.kiro7.com/news/local/seattle-man-suspected-of-importing-fentanyl-from-china-through-mail/592809819<br>Pulkkinen, L. (2017, Aug 15). Feds: Bitcoin drug dealer trafficked China-sourced fentanyl. *Seattle Pi.* Retrieved from https://www.seattlepi.com/local/crime/article/Feds-Bitcoin-drug-dealer-trafficked-11821946.php<br>Q13 News Staff (2017, Aug 16). King County man bought pounds of fentanyl through mail prosecutors say. *Fox Q13.* Retrieved from http://q13fox.com/2017/08/16/king-county-man-bought-pounds-of-fentanyl-through-mail-prosecutors-say/ |
| Steinmetz, Peter | United States of America v. Thomas Mario Costanzo and Peter Nathan Steinmetz. 2:17-cr-00585. D. Ariz. (2017).<br>White, K. (2017, July 7). Neurologist who once carried AR-15 at Phoenix airport charged with illegal bitcoin trading. *AZ Central*. Retrieved from https://www.azcentral.com/story/news/local/phoenix/2017/07/08/man-rifle-phoenix-airport-indicted-arizona-bitcoin-investigation/460752001/ |
| Teramoto, Ayumu | Japan Today Staff. (2014, May 10). Police make bitcoin-linked drug arrest. *Japan Today*. Retrieved from https://japantoday.com/category/crime/police-make-bitcoin-linked-drug-arrest<br>Mathew, J. (2014, May 9). Japan makes first arrest over alleged drug trafficking using bitcoin. *International Business Times*. Retrieved from https://www.ibtimes.co.uk/japan-makes-first-arrest-over-alleged-drug-trafficking-using-bitcoin-1447857 |
| Ulbricht, Ross | Greenberg, A. (2017, May 31). Silk Road creator Ross Ulbricht loses his life sentence appeal. *Wired*. Retrieved from https://www.wired.com/2017/05/silk-road-creator-ross-ulbricht-loses-life-sentence-appeal/<br>Greenberg, A. (2015, Jan 13). Why the Silk Road trial matters. *Slate*. Retrieved from |

| | |
|---|---|
| | http://www.slate.com/articles/technology/future_tense/2015/01/ross_ulbricht_and_silk_road_the_trial_everyone_should_watch.html<br>United States of America v. Ross Ulbricht. 1:14-cr-00068. S.D.N.Y. (2014).<br>USAO – Southern District of New York. (2015, May 29). *Ross Ulbricht, a/k/a "Dread Pirate Roberts", sentenced in Manhattan federal court to life in prison* [Press Release]. Retrieved from https://www.justice.gov/usao-sdny/pr/ross-ulbricht-aka-dread-pirate-roberts-sentenced-manhattan-federal-court-life-prison |
| V., Tommie | Aliens, C. (2017, Aug 16). Belgian police raiding houses in BTC money laundering bust. *DeepDotWeb*. Retrieved from https://www.deepdotweb.com/2017/08/16/belgian-police-raiding-houses-btc-money-laundering-bust/<br>Pieters, J. (2017, July 31). Dutch man arrested in Belgian money laundering investigation. *NLTimes*. Retrieved from https://nltimes.nl/2017/07/31/dutch-man-arrested-belgian-money-laundering-investigation |
| Vallerius, Gal | Solon, O. (2017, Sept 28). Trip to world beard competition ends in arrest for alleged dark web drug dealer. *The Guardian*. Retrieved from https://www.theguardian.com/us-news/2017/sep/28/world-beard-moustache-competition-drug-dealer<br>Swenson, K. (2017, Oct 10). He came to the U.S. for a beard competition – Law enforcement was waiting. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/morning-mix/wp/2017/10/05/he-came-to-the-u-s-for-a-beard-competition-law-enforcement-was-waiting/?utm_term=.2c60d8113b55 |
| Vassilenko, Vadim | Pohlman, J. & Day, A. (2013, September 12). Busted! Inside one massive cybercrime ring. *CNBC*. Retrieved from https://www.cnbc.com/id/101029866<br>Zetter, K. (2013, August 8). Ukrainian carder in $5 million ring sentenced to 14-plus years in prison. *Wired.* Retrieved from https://www.wired.com/2013/08/carder-eskalibur-sentenced/ |
| Vinnik, Alexander | Mizrahi, A. (2017, December 13). Greek Supreme Court rejects extradition appeal by BTC-e's Alexander Vinnick. *BitcoinNews*. Retrieved from https://news.bitcoin.com/greek-supreme-court-rejects-extradition-appeal-by-btc-es-alexander-vinnik/<br>United States of America v. BTC-E, A/K/A Canton Business Corporation and Alexander Vinnick. CR-16-00227. N.D. Cal. (2016).<br>USAO - Northern District of California (2017, July 26). *Russian national and bitcoin exchange charged in 21-count indictment for operating alleged international money laundering scheme and allegecdly laundering funds from hack of Mt. Gox* [Press release]. Retrieved from https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged |
| Wallace, David Ray | Dellinger, A.J. (2018, Jan 23). Opioid crisis: Veterinarian bought fentanyl with bitcoin on the dark web. *International Business Times.* Retrieved from http://www.ibtimes.com/opioid-crisis-veterinarian-bought-fentanyl-bitcoin- |

| | |
|---|---|
| | dark-web-2644289<br>Gilmour, J. (2018, Jan 23). Alabama man arrested for buying overseas fentanyl shipped in teddy bear, police say. *Miami Herald*. Retrieved from http://www.miamiherald.com/news/nation-world/national/article196224384.html |
| White, Jenna M. | Associated Press. (2015, Mar 19). Bellevue man gets 5 years for selling drugs on 'Silk Road' Internet site. *The Seattle Times*. Retrieved from https://www.seattletimes.com/seattle-news/crime/bellevue-man-gets-5-years-for-selling-drugs-on-silk-road-internet-site/<br>United States of America v. Steven Lloyd Sadler & Jenna M. White. 2:13-MJ-00487. W.D. Wash. (2013). |
| Willner, Joseph | D., R. (2017, November 1). Bitcoin used in SEC market manipulation case. *NewsBTC*. Retrieved from http://www.newsbtc.com/2017/11/01/bitcoin-used-sec-market-manipulation-case/<br>Moyer, L. (2017, October 30). Day trader made $700,000 in a scheme targeting hacked online brokerage accounts, prosecutors say. *CNBC.* Retrieved from https://www.cnbc.com/2017/10/30/day-trader-made-700000-in-a-scheme-targeting-hacked-online-brokerage-accounts-prosecutors-say.html<br>SEC. (2017, October 30). *Day trader charged in brokerage account takeover scheme* [Press release]. Retrieved from https://www.sec.gov/news/press-release/2017-202<br>United States of America v. Joseph Willner. 17-cr-620. E.D.N.Y. (2017). |
| Yan, Xiaobing | Fox 9 Staff (2017, Oct 17). Fentanyl distribution ring busted, Chinese factory bosses among 21 indicted. *Fox 9*. Retrieved from http://www.fox9.com/news/fentanyl-bust-charges-north-dakota-china<br>Williams, P. (2017, Oct 17). Two Chinese nationals charged with selling fentanyl to U.S. suppliers. *NBC News*. Retrieved from https://www.nbcnews.com/storyline/americas-heroin-epidemic/two-chinese-nationals-charged-selling-fentanyl-u-s-suppliers-n811506<br>USAO – District of Columbia. (2017, Oct 17). *Deputy Attorney General Rod J. Rosenstein delivers remarks enforcement actions stop deadly* [Press Release]. Retrieved from https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-enforcement-actions-stop-deadly |
| Yensan, Matthew Lee | M.E. (2017, Dec 2). Drug dealer made Xanax and sold it on the dark web. *DeepDotWeb*. Retrieved from https://www.deepdotweb.com/2017/12/02/drug-dealer-made-xanax-sold-dark-web/<br>McDonald, T. (2017, Nov 21). Homemade Xanax: Federal agents say Raleigh man sold drugs on dark net. *The News Observer.* Retrieved from http://www.newsobserver.com/news/local/crime/article185862823.html |
| Zhang, Jian | Fox 9 Staff (2017, Oct 17). Fentanyl distribution ring busted, Chinese factory bosses among 21 indicted. *Fox 9*. Retrieved from http://www.fox9.com/news/fentanyl-bust-charges-north-dakota-china<br>Williams, P. (2017, Oct 17). Two Chinese nationals charged with selling fentanyl to |

| | |
|---|---|
| | U.S. suppliers. *NBC News*. Retrieved from https://www.nbcnews.com/storyline/americas-heroin-epidemic/two-chinese-nationals-charged-selling-fentanyl-u-s-suppliers-n811506<br>USAO – District of Columbia. (2017, Oct 17). *Deputy Attorney General Rod J. Rosenstein delivers remarks enforcement actions stop deadly* [Press Release]. Retrieved from https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-enforcement-actions-stop-deadly |
| Zhao Dong, Brother 1 | Aliens, C. (2017, Aug 16). Belgian police raiding houses in BTC money laundering bust. *DeepDotWeb*. Retrieved from https://www.deepdotweb.com/2017/08/16/belgian-police-raiding-houses-btc-money-laundering-bust/<br>Pieters, J. (2017, July 31). Dutch man arrested in Belgian money laundering investigation. *NLTimes*. Retrieved from https://nltimes.nl/2017/07/31/dutch-man-arrested-belgian-money-laundering-investigation |
| Zhao Dong, Brother 2 | Aliens, C. (2017, Aug 16). Belgian police raiding houses in BTC money laundering bust. *DeepDotWeb*. Retrieved from https://www.deepdotweb.com/2017/08/16/belgian-police-raiding-houses-btc-money-laundering-bust/<br>Pieters, J. (2017, July 31). Dutch man arrested in Belgian money laundering investigation. *NLTimes*. Retrieved from https://nltimes.nl/2017/07/31/dutch-man-arrested-belgian-money-laundering-investigation |

## Appendix B: Code Book

| Year | Age of Offender | Gender of Offender |
|---|---|---|
| 1 = 2012 or prior<br>2 = 2013<br>3 = 2014<br>4 = 2015<br>5 = 2016<br>6 = 2017<br>7 = 2018 | 1 = 15 to 19<br>2 = 20 to 29<br>3 = 30 to 39<br>4 = 40 to 49<br>5 = 50 to 59 | 1 = male<br>2 = female |
| **Crime Type** | **Affiliation** | **Individual or Team** |
| 1 = money laundering (ML)<br>2 = drug trafficking (DT)<br>3 = ML + DT<br>4 = terrorism financing | 1 = single drug market<br>2 = multiple drug markets<br>3 = currency exchanges<br>4 = other | 1 = individual<br>2 = team |
| **Operation Amount** | **Cryptocurrency Use** | **Cryptocurrency Type** |
| 1 = less than $100,000<br>2 = $100,000 to $999,999<br>3 = $1 million to $999 million<br>4 = $1 billion or greater<br>5 = unknown amount | 1 = cryptocurrencies for cash<br>2 = transactions made using cryptocurrencies<br>3 = cryptocurrencies for cash AND for transactions<br>4 = theft of cryptocurrencies with the potential to launder | 1 = bitcoin<br>2 = other |
| **Nationality** | **Arrest Region** | **Court** |
| 1 = North American<br>2 = European<br>3 = Asian<br>4 = Australian | 1 = North America<br>2 = Europe<br>3 = Asia<br>4 = Australia | 1 = U.S. courts<br>2 = foreign courts |

**References**

Aluko, A. & Bagheri, M. (2012). The impact of money laundering on economic and financial stability and on political developing in developing countries: The case of Nigeria. *Journal of Money Laundering Control, 15*(4), 442-457.

Ammous, S. (2015). Economics beyond financial intermediation: Digital currencies' possibilities for growth, poverty alleviation, and international development. *The Journal of Private Enterprise, 30*(3), 19-50.

Broseus, J., Rhumorbarbe, D., Morelato, M., Staehli, L., & Rossy, Q. (2017). A geographical analysis of trafficking on a popular darknet market. *Forensic Science International, 277*, 88-102.

Brown, S.D. (2016). Cryptocurrency and criminality: The Bitcoin opportunity. *The Police Journal: Theory, Practice, and Principles, 89*(4), 327-339.

Chaia, A., Dala, A., Goland, T., Gonzalez, M.J., Morduch, J., & Schiff, R. (2009). Half the world is unbanked. *Financial Access Initiative Framing Note*. Retrieved from http://ww.desi.gsma.com/mobilefordevelopment/wp-content/uploads/2012/06/110109halfunbanked_0_4.pdf

Christopher, C.M. (2014). Wack-a-mole: Why prosecuting digital currency exchanges won't stop online money laundering. *Lewis and Clarke Review, 18*(1).

Clarke, R.V. (1995). Situational crime prevention. *Crime and Justice, 19*, 91-150.

Clarke, R.V. & Cornish, D.B. (1985). Modeling offenders' decisions: A framework for research and policy. *Crime and Justice – An Annual Review of Research, 6,* 147-185.

Clegg, A. G. (2014). Could Bitcoin be a financial solution for developing economies? Applying Austrian economics to currency network models and evaluating Bitcoin as a financial

solution for low-tech environments. *University of Birmingham*. Retrieved from http://www.cs.bham.ac.uk/~rjh/courses/ResearchTopicsInHCI/2013-14/Papers/Alastair.pdf

Cohen, L.E. & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588-608.

commodity. (2017) *Merriam-Webster.com*. Merriam-Webster, Retrieved December 2017 from http://www.merriam-webster.com/dictionary/commodity

currency. (2017) *Merriam-Webster.com*. Merriam-Webster, Retrieved December 2017 from http://www.merriam-webster.com/dictionary/currency

Cornish, D. B. (1994). The procedural analysis of offending and its relevance for situational prevention. In R. V. Clarke (ed.) *Crime Prevention Studies* (Vol. 3). Monsey: Criminal Justice Press.

Cornish, D.B. & Clarke. R.V. (2002). Analyzing organized crimes. In A. Piquero & S.G. Tibbetts (Eds.), *Rational Choice and Criminal Behavior: Recent Research and Future Challenges*. New York: Routledge.

Dostov, V. & Shust, P. (2014). Cyrptocurrencies: An unconventional challenge to the AML/CFT regulators. *Journal of Financial Crime, 21*(3), 249-263.

Driffill, J. (2012). Currency conflicts on the international scene. *ECSSR (Abu Dhabi) - Emirates Lecture Series, 94*, 1-59.

FBI (2012). Bitcoin virtual currency: Unique features present distinct challenges for deterring illicit activity. *Federal Bureau of Investigation – Intelligence Assessment*. Retrieved from https://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf

Ferwerda, J. (2008). The economics of crime and money laundering: Does anti-money laundering policy reduce crime? *Review of Law and Economics, 5*(2), 903-929.

FATF (2015). *FATF Report.* Emerging Terrorist Financing Risks. Retrieved from http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf

FATF (2014). *FATF Report* Virtual currencies: Key definitions and potential AML/CFT risk. Retrieved from http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

FATF (2008). *FATF Report.* Terrorist financing. Retrieved from http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf

Fratianni, M. (2012). The future international monetary system: Dominant currencies or supranational money? An introduction. *Open Economies Review, 23*(1), 1-12.

Gilmour, N. (2014). Understanding money laundering: A crime script approach. *The European Review of Organized Crime, 1*(2), 35-56.

Irwin, A.S.M. & Milad, G. (2016). The use of crypto-currencies in funding violent jihad. *Journal of Money Laundering Control, 19*, 407-425.

Irwin, A.S.M., Slay, J., Choo, K.K.R., & Liu, L. (2014). Money laundering and terrorism financing in virtual environments: a feasibility study. *Journal of Money Laundering Control, 17*(1), 50-75.

Irwin, A.S.M., Choo, K.K.R., & Liu, L. (2012a). An analysis of money laundering and terrorism financing typologies. *Journal of Money Laundering Control, 15*(1), 85-111.

Irwin, A.S.M., Choo, K.K.R., & Liu, L (2012b). Modelling of money laundering and terrorism financing typologies. *Journal of Money Laundering Control, 15*(3), 316-335.

Jacquez, T. (2016). Cryptocurrency: The new money laundering problem for banking, law enforcement, and the legal system. *Utica College – Proquest Dissertations Publishing*.

Jakubiec, D., Kilcer, A., & Sager, W. (2009). The war on drugs. *Rochester Institute of Technology RIT Scholar Works.* Retrieved from http://scholarworks.rit.edu/cgi/viewcontent.cgi?article=2664&context=article

Kleemans, E.R., Soudijn, M.R.J., & Weenink, A.W. (2012). Organized crime, situational crime prevention and routine activity theory. *Trends in Organized Crime, 15*, 87-92.

Koshy, P., Koshy, D., & McDaniel, P. (2014). An analysis of anonymity in Bitcoin using P2P network traffic. *Financial Cryptography and Data Security,* 469-485.

Lavorgna, A. (2015). Organised crime goes online: Realities and challenges. *Journal of Money Laundering Control, 18*(2), 153-168.

Lee, J., Long, A., McRae, M., Steiner, J., & Handler, S. (2015). Bitcoin basics: A primer on virtual currencies. *Business Law International, 16*(1), 21-48.

Maras, M-H. (2016). *Cybercriminology*. New York: Oxford University Press.

Meek, J. (2014). Bitcoin regulation challenges and complexities. *Operational Risk & Regulation*. Retrieved from http://www.risk.net/operational-risk-and-regulation/feature/2328022/bitcoin-regulation-challenges-and-complexities

Plassaras, N.A. (2013). Regulating digital currencies: Bringing Bitcoin within the reach of the IMF. *Chicago Journal of International Law, 14*(1), 377-407.

Popper, N. (2015, April 29). Can Bitcoin conquer Argentina? With its volatile currency and dysfunctional banks, the country is the perfect place to experiment with a new digital

currency. *The New York Times*. Retrieved from http://www.nytimes.com/2015/05/03/magazine/how-bitcoin-is-disrupting-argentinas-economy.html?_r=0

Reda, H.A. (2017). Terrorist financing: Are current anti-money laundering regulations easily applied to virtual currencies? *Colorado Technical University - ProQuest Dissertations Publishing*.

Reynolds, P. & Irwin, A. (2017). Tracking digital footprints: Anonymity within the bitcoin system. *Journal of Money Laundering Control, 20*(2), 172-189.

Ritchet, J.L. (2013). Laundering money online: a review of cybercriminals' methods. *Tools and Resources for Anti-Corruption Knowledge – UNODC.* Retrieved from https://arxiv.org/abs/1310.2368

Salami, I. (2017). Terrorism financing with virtual currencies: Can regulatory technology solutions combat this? *Studies in Conflict & Terrorism*.

Sat, D.M., Krylov, G.O., Evgenyevich, K., Bezverbnyi, Kasatkin, A.B., & Kornev, I.A. (2016). Investigation of money laundering methods through cryptocurrency. *Journal of Theoretical and Applied Information Technology, 83*(2), 244-254.

Scott, B. (2016). How can cryptocurrency and blockchain technology play a role in building social and solidarity finance? *UNRISD: United Nations Research Institute for Social Development,* Working Paper 2016-1. Retrieved from http://www.unrisd.org/brett-scott

Stuhlmiller, L. (2013). Mitigating virtual money laundering: An analysis of virtual worlds and virtual currencies. *ProQuest Dissertations Publishing*.

Tang, J. & Ai, L. (2010). Combating money laundering in transition countries: The inherent limitations and practical issues. *Journal of Money Laundering Control, 13*(3), 215-225.

Trautman, L. (2014). Virtual currencies: Bitcoin & what now after Liberty Reserve, Silk Road, and Mt. Gox? *Richmond Journal of Law & Technology, 20* (4).

Tu, K.V. & Meredith, M.W. (2015). Rethinking virtual currency regulation in the Bitcoin age. *Washington Law Review, 90*(1), 271-347.

Virga, M. (2015). International criminals and their virtual currencies: The need for an international effort in regulating virtual currencies and combatting cyber crime. *Revista de Direito Internacinoal, 12*(2), 511-526.

Wortley, R. & Mazerolle, L.G. (2008). *Environmental criminology and crime* a*nalysis*. Cullompton, Devon, UK: Willan.