11

The Scope of Cryptocurrency in the Information Age

Eric NESBITT

Abstract: In this information age we are living in, we are on the cusp of a major technological paradigm shift that will have reverberating effects through every aspect of society; cryptocurrency implementation into major security threats has the potential of altering the security world as we know it. The purpose of paper is to provide the reader with a basic understanding of what cryptocurrency is, blockchain technology, the use of cryptocurrency by illicit actors, terrorist organization's use of cryptocurrency, and ways in which law enforcement/security agencies can prevent the nefarious use of cryptocurrency. Additionally, this paper aims to provide resources to further expand on discussed topics; ultimately helping academics, decision makers, and policy setters with advancing the understanding of cryptocurrency in our modern world.

Keywords: Cryptocurrency, Security Threats, Blockchain, Peer-To-Peer (P2P) Network, Bitcoin, Public Ledger, Cryptography, Hash, Proof-of-work Mechanism, Fiat Currencies, Ransomware, Encryption, Mining, Bitcoin ATM, Altcoins, Terrorist Financing

Introduction

Right now, the largest theft of currency in history could be occurring. A single person, in a country across the world, could be draining the accounts of thousands without anyone being witness. By the time the theft would be noticed, authorities alerted, and the case transferred to the proper agency; all of that currency would be laundered and stored away. If that single person is strategic, they would hide their tracks exceptionally well

and may never get caught. This type of theft is a very real occurrence that is happening in the world today. The massive growth of cryptocurrency in our everyday global society has opened up entirely new categories of illicit activities that current legal precedent is being decided on this very day. What needs to be discussed is to what extent is cryptocurrency used to aid in illicit activities? This question, and subsequently related questions to cryptocurrency will be answered further on.

What is Cryptocurrency?

Before diving into the intricacies of cryptocurrencies use for nefarious purposes, the question of what cryptocurrency is must be addressed. It is very important to note that there is not a clearly defined single definition for cryptocurrency. Depending on which financial instructions, organizations, or government is defining it, there are slight differences. The best definition is put forth from a report requested by the European Parliament on combating cryptocurrency and crime. The definition used pulls from those issued by the World Bank and Financial Action Task Force (FATF) on the topic of cryptocurrency. The definition of cryptocurrency is as follows: "a digital representation of value that (i) is intended to constitute a peer-to-peer ("P2P") alternative to government-issued legal tender, (ii) is used as a general-purpose medium of exchange (independent of any central bank), (iii) is secured by a mechanism known as cryptography and (iv) can be converted into legal tender and vice versa"[491]. In the remainder of this paper, the term cryptocurrency will be referring to this definition.

Cryptocurrency started to gain popularity in 2008 with a paper titled *Bitcoin – A Peer to Peer Electronic Cash System* which was written by a Satoshi Nakamoto[492]. In this paper, the critical peer to peer exchange system of currency, including the all-important blockchain, was introduced. It was

---

[491] Robby Houben, Alexander Snyers, *Cryptocurrencies and Blockchain*, (Brussels, European Parliament, 2018), 23.

[492] Bernard Marr, *A Short History of Bitcoin and Cryptocurrency Everyone Should Read*, (Forbes, 2017).

not until 2009 that Bitcoin could be used by the public, at which point it quickly gained traction. It should be noted that there were other cryptocurrencies prior to Bitcoin, but none were nearly as successful, even up to today[493]. After 2010, Bitcoin saw steady growth, but also began its pathway towards illicit activity. The Silk Road, a black-market store located on the dark web sold anything from illicit drugs to firearms; its currency used, Bitcoin. This played a big factor in building the value of Bitcoin and sparked the creation of other forms of cryptocurrency. Today, there are around 1600 different types of cryptocurrency, but the 'big five' control most of the market –[494] Bitcoin, Ethereum, Ripple, Bitcoin Cash, and Litecoin[495]. The reasons for the development and growth of these other kinds of cryptocurrency all revolved around the changing market and privacy.

There are some key terms and functions that must be discussed in order to explain the growth of other cryptocurrencies, and how they factor into modern day illicit activities. The first is the *blockchain* this is essentially a public ledger of every single peer-to-peer cryptocurrency transaction that occurs. It is open to anyone with a connection to the internet and all transactions can be viewed. Another key term is a *wallet*, this is a digital application that allows cryptocurrency users to store and retrieve their digital assets. For every single exchange that happens in the blockchain, a new wallet is formed; this happens every time, with every transaction. For each wallet the user needs a key to be able to access it. This is a sophisticated string of letters and numbers that can be entered for a specific address that then unlocks the wallet. Keys are quite important, and often cryptocurrency users will have them on secure flash drives that will self-encrypt if tampered with. The final significant term is called *mining* or *cryptomining*; this is the process of verifying a transaction and adding it to the blockchain. This can serve two purposes, first is legitimizing the exchange of cryptocurrency and the other is hiding a transaction[496].

---

[493] Ibid.

[494] Matthew Frankel, *How Many Cryptocurrencies Are There?*, (The Motley Fool, 2018).

[495] Houben, Snyers, *Cryptocurrencies and Blockchain*, 30.

[496] Rosemary Bigmore, *Decoding crypto-speak: the ultimate cryptocurrency jargon-buster,* (The Telegraph, 2018).

In Depth Analysis of Blockchain Technology

Simply put, a blockchain is a distributed digital ledger that is completely open and accessible to everyone via the internet. Simply Explain describes a blockchain a string of blocks, each of which contains key information that once recorded, is almost impossible to change. In the case of Bitcoin currency, the information in each block relates to each separate transaction. When a transaction is completed using Bitcoin the information of who sent it, who received it, and how much is all stored permanently on the blockchain public ledger. What makes the blockchain a congruent string of information comes from the hash that is placed on the front and back of each block. The hash ties the information to the previous block and to the next one, thus creating a chain of information that can be traced back all the way to the genesis block, or the beginning of the ledger[497].

With the blockchain ledger being completely open and accessible by anyone with an internet connection, what makes it so secure and trusted? There are three measures in place in a blockchain to ensure it is secured and to prevent nefarious tampering actions. The first is the hash system. This is crucial because it creates the connection between each block and makes it possible to trace each transaction. The next is the mechanism called proof-of-work, and this is put in place to purposely slow down the creation of new blocks in the chain. Proof-of-work gives all important time for the final step of security, verification from the Peer-to-Peer (P2P) network that the blockchain is stored on. A blockchain ledger is not stored on a single computer but on multiple public servers across the globe[498]. In fact, each new person who joins the blockchain gets a copy of the complete ledger, and after each transaction it is updated.

If, for example there was a string of five blocks in a small blockchain, and in the second block a large quantity of cryptocurrency was sold that an illicit actor wanted to hide. The actor would go into the blockchain and try

---

[497] Simply Explain – Savjee. *How does a blockchain work – Simply Explained,* (Youtube, 2017).

[498] Savjee, *How does a blockchain work,* 2017.

to create an alternate chain from the transaction to hide the large quantity of cryptocurrency moved. By doing this they change the end hash of the second block, which does not match the next block and therefore must be changed. This process continues down the entire chain, and each hash must be changed. Modern computers are extremely fast, and this process would be easy if not for the Proof-of-work slowing mechanism and then verification from all members of the P2P network[499]. This is what makes blockchain technology so secure and has solidified it as a digital technology that will be developed and implemented into multiple modern-day industries.

With a secure blockchain in place in major cryptocurrencies like Bitcoin, the obvious question can be asked, what is drawing illicit actors to using cryptocurrency? One would assume that illicit actors would seek alternatives means of acquiring and distributing capital given that every cryptocurrency transaction can be traced, and that tampering is made nearly impossibly with the blockchain technology. The major drawing factor to illicit actors to use the cryptocurrency and blockchain technology, is its infancy[500]. Legislation is still being determined about the adaptation of cryptocurrency, law enforcement/security agencies are just beginning to understand and educate on illicit cryptocurrency activities, and crafty methodology transactions on the blockchain that can be well hidden. It should also be noted that each day new cryptocurrencies are being formed and gaining popularity, and each cryptocurrency is not created equally. Bitcoin has a well implemented blockchain at its disposal, but other cryptocurrencies do not follow such a strict standard. There are even new cryptocurrencies that do not utilize blockchain technology, and it is these that illicit actors to seek to exploit them for nefarious purposes.

---

[499] Simply Explain – Savjee. *How does a blockchain work – Simply Explained,* (Youtube, 2017).

[500] Cynthia Dion-Schwarz, David Manheim, Patrick Johnston, *Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats*, (Santa Monica, CA: RAND Corporation, 2019).

Analysis of Current Cryptocurrency Use

In 2017 there was a massive boom in Bitcoin, causing investors to turn into overnight millionaires with only owning a small amount of Bitcoin. Jackson reports, "It took Bitcoin less than a year to 20x its value through 2017"[501]. This boom caused the individual price of a Bitcoin to skyrocket, reaching nearly $1000 overnight. By October of 2017 Bitcoin saw an increase of nearly 300%, reaching its peak price of $4,900 for one individual coin[502]. This drew a large general public interest to Bitcoin, with hopes of new investors becoming overnight millionaires through buying and trading Bitcoin.

This explosion in Bitcoin caused a wave of creation of new types of Altcoins; these are alternative cryptocurrencies to Bitcoin that either imitate the same system of Bitcoin (publicly accessible ledger), or use alternative methods of operation[503]. Some employ a completely anonymous and untraceable system that has no public ledger, while others are fully accountable and require personal identifying information. The creation of these new cryptocurrencies had one goal in mind: develop a large enough group of investors to create a boom in the market, similar to the one that Bitcoin had gone through[504]. Several of these cryptocurrencies gained large popularity which shifted the market of cryptocurrency as a whole, and propelled cryptocurrency as a viable option for the general public.

As of the third quarter of 2019, the number of blockchain wallet users is 42,290,501[505]. This is nearly seven times larger than the number of wallet users in the Blockchain in 2016, and massively larger than when cryptocurrencies became mainstream in 2010. Below are the current standings of the top ten cryptocurrencies:

---

[501] Reuben Jackson, *Understanding the Last Three-year Cryptocurrency* Rollercoaster, (Bigthink, 2019).

[502] Ibid.

[503] Rosemary Bigmore, *Decoding crypto-speak: the ultimate cryptocurrency jargon-buster,* (The Telegraph, 2018).

[504] Reuben Jackson, *Understanding the Last Three-year Cryptocurrency* Rollercoaster, (Bigthink, 2019).

[505] Szmigiera, *Number of Blockchain Wallet Users Globally 2016–2019,* (Statista, 2019).

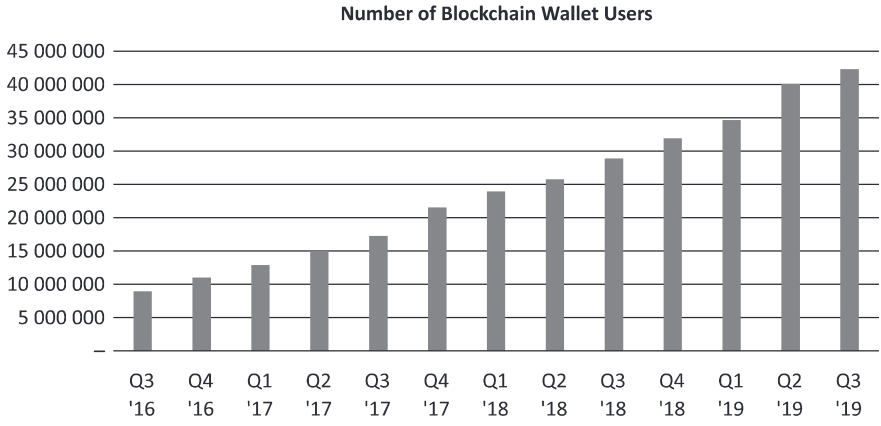
Table 11.1

Name	Symbol	Market Cap (USD)	Supply Limit
Bitcoin	BTC	$ 124,969,093,161.00	21 million
Ethereum	ETH	$ 57,462,517,858.00	Unknown
Ripple	XRP	$ 23,790,387,789.00	100 billion
Bitcoin Cash	BCH	$ 17,159,025,225.00	21 million
Litecoin	LTC	$ 6,704,709,572.00	84 million
Stellar	XLM	$ 5,128,373,973.00	100 billion
Cardano	ADA	$ 5,034,129,651.00	45 billion
IOTA	MIOTA	$ 4,038,240,572.00	2,779,530,283,277,760
NEO	NEO	$ 3,386,383,000.00	100 million
Monero	XMR	$ 2,626,586,260.00	18.4 million
Dash	DASH	$ 2,592,894,544.00	17.74–18.92 million

Houben, Snyers, *Cryptocurrencies and Blockchain*, 30.

Number of Blockchain wallet users worldwide from 3rd quarter 2016 to 3rd quarter 2019.

Figure 11.1. Szgiera, *Number of Blockchain Wallet Users Globally 2016–2019*, 2019



What Illicit Actors are Using Cryptocurrency?

The use of cryptocurrency in illicit activities has grown exponentially since it started to become mainstream in 2010. As a federal criminal analyst put it, "cryptocurrency is used in a variety of ways by criminals"[506]. Some illicit actors engage in illegal fraud schemes that require them to be paid in cryptocurrency. A very common one is a user downloading ransomware onto their computer, and the hacker demanding payment of Bitcoin. Another way that is becoming popular is targeting individuals who hold large volumes of cryptocurrency. These individuals, also known as 'whales' often brag or flaunt their wealth on social media sites, drawing attention from hackers[507]. Those hackers then use SIM swapping and identity theft techniques to drain the whales' crypto accounts. Some actors who usually run and operate organized crime have moved to cryptocurrency as a layering and laundering method to wash, store, and secure their criminal bounties too. Then there are the illicit purchases using cryptocurrency. While the darknet website Silk Road has been shut down, many other illicit sites that sell the same materials and services exist. A final way in which cryptocurrency is used in an illicit way is within the community itself. With new cryptocurrencies popping up frequently, illicit actors will develop a new currency that will get others to invest in. In reality they are just handing over their legitimate crypto assets to a fake one that then gets transferred to the creator's wallet and is gone.

The next group that uses cryptocurrency in their criminal endeavors are various types of organized crime groups. While there is no supporting evidence for street gangs using cryptocurrency in their operations, national mafias and outlaw motorcycle gangs (OMGs) have been known to exploit cryptocurrency[508]. National mafias, such as the Chaldean mafia, have a large presence in and around Detroit, Michigan, USA, often using

---

[506] Federal criminal analyst, interview by Eric Nesbitt, (United States of America, 2019).

[507] Rosemary Bigmore, *Decoding crypto-speak: the ultimate cryptocurrency jargon-buster,* (The Telegraph, 2018).

[508] Federal criminal analyst, interview by Eric Nesbitt, (United States of America, 2019).

cryptocurrency gambling sites to try to gain value and wash proceeds. They have been known to commit fraud schemes on businesses in the area and take their proceeds and hide them as cryptocurrency[509]. OMGs have adopted a much more physical and ludicrous approach to exploiting cryptocurrency. Like one off hackers, they scour social media in search of crypto whales who are flaunting purchases and leaving behind a trail of personal information. When the OMG has identified the individual, they then kidnap them and hold them hostage, demanding access to their crypto assets. Once given access, they drain the wallets into their own and are off. The first major instance of this was in 2017 and was conducted by a Bronx biker group[510]. While this was the first newsworthy attack, the potential for similar attacks is extremely high.

Terrorism and Cryptocurrency

Currently, terrorist organizations along with the rest of the world, are living on the edge of a paradigm shift in technology. One that will fundamentally change the global society as we know it in the near future. Every aspect of how we as humans operate will change – from daily interactions, to complex problem solving. In this wave of change falls cryptocurrency, specifically its potential use by terrorist organizations. It must be noted that, "there is little indication that terrorist organizations are using cryptocurrency in any sort of extensive or systematic way"[511]. The primary reason for this is the lack of use/acceptance from the global population. It is a small subset of certain individuals who are implementing cryptocurrency into their everyday lives. The technology, for many terrorist organizations is beyond the scope of their capabilities; and the time and resource investment to make cryptocurrency a viable option is not worth it.

---

[509] Federal criminal analyst, interview by Eric Nesbitt, (United States of America, 2019).

[510] Habiba Tahir, *Bronx Biker Gang Members Charged in $2 Million Ether Kidnapping*, (CNN, 2019).

[511] Cynthia Dion-Schwarz, David Manheim, Patrick Johnston, *Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats*, (Santa Monica, CA: RAND Corporation, 2019), 21.

Why then should law enforcement, state security agencies, and the world be concerned about terrorist use of cryptocurrency? The potential for terrorist organizations to gain massive amounts of funding through cryptocurrency is very high. Through further advancement of blockchain technology cryptocurrency will become a more viable option for everyday users, drawing in terrorist organization members. Additionally, new cryptocurrencies are appearing every day, and each have the potential to be used by a terrorist organization to fund their operations. One report warns, "Several recent advances in cryptocurrencies will facilitate their use by the most sophisticated groups that threaten terrorism against Western countries, and the use of cryptocurrencies will be especially enabling for actors that already engage in transnational fundraising and criminal activities"[512].

In summary, groups such as Al-qaeda, ISIS, Hezbollah, Narcoterrorist organizations, and lone-wolf attackers all have a potential need/use for cryptocurrency[513]. In the report by the RAND Corporation titled *Terrorist Use of Cryptocurrencies,* there are listed five major uses that terrorist groups, such as the one mentioned previously, use cryptocurrency for including: fundraising, illegal drug and arms trafficking, remittance and transfer of funds, attack funding, and operational funding[514]. Large terrorist organization may seek support through cryptocurrency donations, and often would prefer this method because it leaves the transaction anonymous to those who may try to trace it. Additionally, sourcing illegal weapons through the darknet via the use of cryptocurrency is easier and safer than doing above ground deals. As mentioned earlier from the RAND report, there is no overwhelming evidence suggesting that cryptocurrency is a mainstream part of everyday terrorist operations. The potential for use and major benefits reaped are there and must be monitored by law enforcement, security agencies, and governments.

---

[512] Cynthia Dion-Schwarz, David Manheim, Patrick Johnston, *Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats*, (Santa Monica, CA: RAND Corporation, 2019), 53.

[513] Dion-Schwarz, Manheim, Johnston, *Terrorist Use of Cryptocurrenices*, xii.

[514] Dion-Schwarz, Manheim, Johnston, *Terrorist Use of Cryptocurrenices*, xi.

Combating Nefarious Cryptocurrency Use

A common problem exists for all users of cryptocurrency for illicit purposes. Once they have acquired a large sum of cryptocurrency, they generally want to convert it into some form of fiat currency[515]. In an interview with a federal criminal analyst, they state the ways in which an illicit actor can convert cryptocurrency:

> Even then, most illicit actors still want to liquidate any cryptocurrency back into U.S. dollars, but this can be difficult. There are generally three ways to convert Bitcoin back into cash. First, an actor can utilize an exchange to move large amounts of cryptocurrency, but these exchanges generally follow anti-money laundering regulations and require know-your- customer (KYC) information. Second, an actor can rely on peer-to-peer marketplaces like LocalBitcoins.com or other – typically unlicensed – money remitters. Third, an actor may rely on a Bitcoin ATM, but the amount of money they can receive at a time is limited[516].

By using these methods, it allows law enforcement to be able to pick up the trail and begin to trace cryptocurrency transactions; but initially picking up that trail is not an easy task.

With Bitcoin being the most popular cryptocurrency, law enforcement has poured a large amount of manpower and time into understanding its complexity[517]. Often from an onlooker perspective, who has a basic understanding of Bitcoin and the blockchain; the question commonly asked is if every transaction is accounted for on the blockchain, why not just trace it back? The answer is it is not that simple. A Federal Criminal Analyst shared:

> The pseudo-anonymity of cryptocurrencies makes it difficult to effectively target criminals. Since Bitcoin's blockchain is a public ledger, technically anyone can track it, but it requires the initial identification of a transaction

---

[515] Rosemary Bigmore, *Decoding crypto-speak: the ultimate cryptocurrency jargon-buster,* (The Telegraph, 2018).

[516] Federal criminal analyst, interview by Eric Nesbitt, (United States of America, 2019).

[517] Joshua Lee, *Cryptocurrency 101: What cops need to know about crime, cryptocurrencies and the dark web*, (Policeone, 2019).

> or Bitcoin address of interest. This initial identification is generally more difficult than say tracking wire activity after a cash deposit at a financial institution[518].

As it was briefly touched upon earlier, nefarious users of cryptocurrency are very good at hiding their tracks. When a large amount of cryptocurrency is acquired, they run it through several methods that essentially wash and hide the transaction. This makes tracing it extremely difficult if not impossible for law enforcement/security agencies.

With this difficult task in front of law enforcement and security agencies, how can they best combat illicit cryptocurrency activities? The first step is to understand the terminology of cryptocurrency[519]. This way agencies can identify if and when they are dealing with aspects of a case related to cryptocurrency. Additionally, being able to know what key hardware pieces are valuable in a cryptocurrency case could prove vital. For example, knowing to search for an encrypted USB stick which may contain the key to a wallet, could open a new lead for a case. The next piece of information is knowing the basics of financial crimes, because in reality that is what all cryptocurrency cases are[520]. The terminology and method of acquiring the currency is different than typical financial crimes, but the end result is still the same. By educating law enforcement and security agencies on the subject, and able to predict an illicit actors next move, it makes solving or stopping the illicit activity that much easier. The final step that is critical for law enforcement is having allies within the cryptocurrency world[521]. Global state agencies need to work together on cases like these in order to ensure no information is lost in communication. Additionally, hiring experts who regularly participate in cryptocurrency markets will boost the knowledge of the entire team on a case. If law enforcement, security agencies, and

---

[518] Federal criminal analyst, interview by Eric Nesbitt, (United States of America, 2019).

[519] Joshua Lee, *Cryptocurrency 101: What cops need to know about crime, cryptocurrencies and the dark web*, (Policeone, 2019).

[520] Joshua Lee, *Cryptocurrency 101: What cops need to know about crime, cryptocurrencies and the dark web*, (Policeone, 2019).

[521] Joshua Lee, *Cryptocurrency 101: What cops need to know about crime, cryptocurrencies and the dark web*, (Policeone, 2019).

state governments can adopt and implement these steps; they will have a significant advantage in combating illicit cryptocurrency activities.

Concluding Thoughts: What Does the Future of Cryptocurrency Look Like in the Information Age?

A common question by the security world is what does the future of cryptocurrency look like? This is also a question that the general public should be considering too; will we eventually establish a global economy of only cryptocurrency? Many feel that cryptocurrency being adopted as a whole, in the state that it currently is in, will not work. The delay in transaction is too long and the processing power to mine a global level of transactions would be impossible; the technology simply does not yet exist. The blockchain technology though, is where we could see leaps and bounds of adaptations into our everyday lives. In an interview with a Federal Criminal Analyst, they stated:

> Blockchain technology can be used for anything that requires unique identifiers, high degrees of security, public trust, and rapid processing, and this could include anything from digital advertising to product purchases. I also think standardization of blockchain protocols could enable the technology to be transformational, but this standardization is almost antithetical to the decentralized nature of cryptocurrencies[522].

The potential for a far different future using blockchain technology is clearly out there and may be adapted, but it hinges on legislation.

What should security agencies, state actors, and the general public do till then? The simple answer: become familiar with cryptocurrency terminology and technology. Having an understanding of the basics can help prevent illicit actors who use cryptocurrency as their primary means of financial attacks from claiming more victims. Additionally, as security agencies continue to learn and develop strategies for tracking and preventing

[522] Federal criminal analyst, interview by Eric Nesbitt, (United States of America, 2019).

cryptocurrency crimes, the safety on the cryptocurrency market will only grow. As noted, "Cryptocurrencies have gone from nonexistent to an enterprise worth billions in less than 10 years"[523]. They are becoming mainstream by a society that is embracing and growing with new technology every day; and must be recognized by the world as a key financial staple in the global market economy.

Bibliography

Bigmore, Rosemary. "Decoding crypto-speak: the ultimate cryptocurrency jargon-buster" The Telegraph, last modified May 25, 2018. Accessed November 21, 2019. https://www.telegraph.co.uk/technology/digital-money/how-to-understand-cryptocurrency-terminology/

Ciccolo, Joe. "Crypto Crime for Law Enforcement Officials: What Do You Need To Know About Compliance?" BitAML, last modified May 27, 2018. Accessed October 27, 2019. https://bitaml.com/crypto-crime-law-enforcement/

Dion-Schwarz, Cynthia, David Manheim, and Patrick B. Johnston. *Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats*. Santa Monica, CA: RAND Corporation, 2019. https://www.rand.org/pubs/research_reports/RR3026.html.

Federal Criminal Analyst. Interview by Eric Nesbitt. Email Interview. United States of America, July 2019.

Frankel, Matthew. "How Many Cryptocurrencies Are There?" The Motley Fool, last modified March 16, 2018. Accessed November 10, 2019. https://www.fool.com/investing/2018/03/16/how-many-cryptocurrencies-are-there.aspx

Greenberg, Andy. "Crypto Currency." Forbes, last modified April 20, 2011. Accessed October 24, 2019. https://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html#43ee38af353e

Houben, Robby. Snyers, Alexander. *Cryptocurrencies and Blockchain*. Brussels: European Parliament, 2018. http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf

Jackson, Reuben. "Understanding the Last Three-year Cryptocurrency Rollercoaster." Bigthink, last modified July 11, 2019. Accessed November 13, 2019.

[523] Federal criminal analyst, interview by Eric Nesbitt, (United States of America, 2019).

https://bigthink.com/technology-innovation/review-of-cryptocurrency-history?rebelltitem=1#rebelltitem1

Lee, Joshua. "Cryptocurrency 101: What cops need to know about crime, cryptocurrencies and the dark web." Policeone, last modified January 4, 2019. Accessed November 6, 2019. https://www.policeone.com/police-products/investigation/articles/482382006-Cryptocurrency-101-What-cops-need-to-know-about-crime-cryptocurrencies-and-the-dark-web/

Malik, Nikita. "How Criminal And Terrorist Use Cryptocurrency: And How To Stop It." Forbes, last modified August 31, 2018. Accessed October 30, 2019. https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and-terrorists-use-cryptocurrency-and-how-to-stop-it/#7a8ac2d39904

Marr, Bernard. "A Short History Of Bitcoin And Cryptocurrency Everyone Should Read." Forbes, last modified December 6, 2017. Accessed November 3, 2019. https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/#4ef44ccc3f27

Simply Explained – Savjee. "How does a blockchain work – Simply Explained." *Youtube.* Video File. November 13, 2017. Accessed November 15, 2019. https://www.youtube.com/watch?v=SSo_EIwHSd4

Szmigiera, M. "Number of Blockchain Wallet Users Globally 2016–2019." Statista, last modified October 7, 2019. Accessed November 8, 2019. https://www.statista.com/statistics/647374/worldwide-blockchain-wallet-users/

Tahir, Habiba. "Bronx Biker Gang Members Charged in $2 Million Ether Kidnapping." CNN, last modified Jun 17, 2019. Accessed October 23, 2019. https://www.ccn.com/bronx-biker-gang-charged-in-2-million-crypto-kidnapping/

Tillier, Martin. "What Is A Cryptocurrency?" Nasdaq, last modified Jan 25, 2018. Accessed October 27, 2019. https://www.nasdaq.com/article/what-is-a-cryptocurrency-cm910816