Revolution in Crime: How Cryptocurrencies Have Changed the Criminal Landscape

A Thesis Presented in Partial Fulfillment of the Requirements for the Masters of Science in Digital

Forensics and Cybersecurity

John Jay College of Criminal Justice

City University of New York

Igor Groysman

February 2019

-

Abstract

This thesis will examine the ways in which various cryptocurrencies have impacted certain traditional crimes. While crime is always evolving with technology, cryptocurrencies are a game changer in that they provide anonymous and decentralized payment systems which, while they can be tracked in a reactive sense via the blockchain, are seen by criminals as having better uses for them than traditional fiat currencies, such as the ability to send money relatively fast to another party without going through an intermediary, or the ability to obscure the origin of the money for money laundering purposes. Every week there are new cryptocurrencies flooding the market, and it doesn't look like it will abate any time soon. Blockchain technology, the underlying technology behind all cryptocurrencies, has uses that far surpass just the currency aspect. Criminals also see the potential that sending money anonymously, without a middleman beholden to regulations and tracking those transactions has. Any new technology while being revolutionary, will always trickle down to seedier elements of society who will always find a use for it. This paper will look at how cryptocurrencies have impacted drug trafficking, money laundering, and ransomware. I will also explore a new kind of crime called cryptojacking that has become possible because of cryptocurrency mining. Law enforcement may be playing a reactive and not a proactive role in the age of cryptocurrencies, but this paper will provide information that can be useful for law enforcement and applicable to their investigations.

Table of Contents

Introduction

Crime has always evolved with the advent of new technologies. It seems a universal law that whatever new technology is developed can be utilized for criminal purposes through direct use or through loopholes in the technologies design. Since the dawn of the internet age, we have seen the democratization of information go into lightspeed, and with it came the exploitation of information. Openness of technology will be exploited by criminal elements as long as there are criminal elements in society. One new technology that has existed for not quite a decade seems to have revolutionized the criminal world in more ways than one. Cryptocurrencies come in many different styles and forms but essentially all have the same purpose; a digital currency which by design is meant for a certain level of anonymity.

Before proceeding, a few definitions must be made clear. *Cryptocurrencies* are "digital or virtual currency that uses cryptography for security" (Investopedia, n.d.). Because of this cryptographic element, they are difficult to counterfeit, and they are decentralized, meaning they are not subject to a central authority, with few exceptions. Cryptocurrencies are designed to run on a digital ledger, which tracks every single transaction for that cryptocurrency. For this paper, the definition of cryptocurrency should be seen to be the same as the definition for the terms *virtual currency* and *digital currency* as well.

Blockchain

This digital ledger, or *blockchain*, is the defining technology of all cryptocurrencies. An easy way to understand the blockchain is to imagine a constantly updating database that contains a record of all the transactions of the cryptocurrency, and exists as a public ledger on all copies of each particular cryptocurrency. A block is a group of transactions that need to be verified before they are placed on the blockchain. Each block is cryptographically verified and confirmed that all transactions on the block are sound and not a double spend (Wilson, 2018). The nodes confirm the blocks by solving a mathematical puzzle. The nodes may be individual computers or servers run by a person or groups. This verification process is known as *mining*, and I will discuss it more in depth when I discuss cryptojacking. The blockchain is built on the principle of trusted transactions directly between two or more parties.

It is difficult not to overestimate the effect that the blockchain has had on the financial industry. According to the Financial Times (Noonan, 2018), JPMorgan has partnered with 75 banks to help test a new blockchain-based cross-border payment system. Bank of America has over 50 patents related directly to blockchain technology (O'Neal, 2018). A decentralized digital ledger has uses that far surpass the digital currencies that they power. The trust system made possible by blockchain technology can be used for monitoring supply chains, data sharing, data management, copyright and royalty protection, digital voting, title transfers, regulation and compliance, medical record-keeping, weapons tracking, tracking prescription drugs, and much more

(Williams, 2018). Blockchain technology's continued adaptation by traditional industries, who were naturally skeptics of the technology in the beginning, based on it's sole association with cryptocurrencies, has grown year by year. An assumption can be made that in the future the most trusted technologies will be the ones powered by blockchain.

There are many websites that allow for exploration of the blockchain. Known as "explorers", they provide users with relevant information for each transaction on the blockchain. An explorer like "Block Explorer" can take as input the transaction hash, which is a unique ID for every transaction, or a particular public address or public key, and provide you with the details for the transaction, as well as the historical details for all transactions of a particular public key (Skvorc, 2017). In any explorer you will see information for both blocks and transactions. Block information contains the height, which is the total number of blocks mined; the age is when the block was mined; transactions, which are the number of transactions within the block; the size of the block, usually in megabytes (MB); and who it was mined/relayed by. Transaction information contains the hash addresses of the sender and receiver, the amount sent (in the particular cryptocurrency), and the date and time of the transaction. Because the blockchain is immutable, this data is persistent and can be accessed anytime with the knowledge that all transactions and all blocks can be effectively analyzed going back to the very first block.

Storing, Sending, and Spending Cryptocurrencies

Cryptocurrencies rely on cryptography to function, and to store cryptocurrencies, users need a *wallet*. Wallets are used to store hexadecimal codes known as private keys, which are known only to you and your wallet. This private key has to match with a public key for you to be able to make any kind of transaction (Blenkinsop, 2018). The ledger contains the public address that is used to track transactions. A wallet is a piece of software or hardware that stores the unique public and private keys of the user's cryptocurrency. The wallet may have multiple keys. However, if the private key is lost, then the cryptocurrency in the user's possession is also lost. Wallets come in the form of software which can be downloaded on a user's computer, or special hardware wallets that can be used like a USB or hard drive. The most effective ways to keep your cryptocurrency safe is to either keep it in cold storage, meaning either keep your hardware wallet disconnected from your computer and in a safe place, or even resorting to low tech methods such as writing your private key down on paper and storing it in a safe place, or memorizing a unique "seed phrase" which connects to your private key through any wallet you use in the future. This last method may be the most secure, since you can lose USB's, hard drives, and pieces of paper, but the only limitation to losing the phrase which connects to your private key is forgetting it.

A Brief History

Bitcoin was the first cryptocurrency on the market. It was created in 2008, by a person or group using the pseudonym Satoshi Nakamoto who posted a white paper on bitcoin to a cryptography mailing list, explaining how the cryptocurrency would work (Cochrane, 2018). The identity of Satoshi Nakamoto has to this day remained a mystery, but the impact of Bitcoin and the blockchain technology it runs on has revolutionized the world. According to CoinMarketCap, there are over 2,000 different cryptocurrencies on the market and new ones are created constantly. The most common ones, or the ones with the biggest market cap are Bitcoin, Ethereum, and Ripple. Ethereum differentiates itself by offering the concept of smart contracts, which is basically code that executes once a certain condition is met, for instance if a certain team wins the Super Bowl, money held in an escrow account will automatically go to the person who bet for that team. There are a plethora of applications for smart contracts and they are powered by the cryptocurrency which facilitates them. There are also those cryptocurrencies that specialize in privacy, such as Monero and Dash, which are popular on the darknet markets, and which we will discuss later. Each cryptocurrency has its own functions and uses, but essentially, they are all designed using the same blockchain technology principle at their core, and under the same philosophy of anonymous currency. Because it is cryptographically sound, the transactions are safe, however this same cryptography is what attracts criminals who wish to utilize the anonymous aspect of digital currency to facilitate their crimes.

Cryptocurrencies are traded through exchanges, where they can also be exchanged for dollars and other traditional currencies. Most of these exchanges are

regulated, and must abide by the Bank Secrecy Act (BSA), which will be discussed later when we go into how cryptocurrencies are used to launder money. There are numerous exchanges, and most retain the information of every user, which can be used by law enforcement to analyze that user's transactions. As we will discuss, the job of law enforcement in the cryptocurrency age has become a little harder due to the anonymity of cryptocurrencies, but there are still ways to track transactions and identify criminal activity using blockchain analysis.

For this paper, I will be focusing on three main areas in which the use of cryptocurrencies has changed the nature of crime. First, I will look at how drug markets have been affected, and I will focus on the darknet drug markets, which allow for the facilitation of drug trafficking using cryptocurrencies as the payment method. Second, I will explore how cryptocurrencies have changed the game when it comes to money laundering and explore some techniques used by criminals to effectively obscure the origin of their ill-gotten gains. Finally, I will discuss ransomware and how it has evolved into cryptojacking, a form of seizing control of a subjects computer without their knowledge, and using the computing power to mine cryptocurrencies. I will also discuss how law enforcement can approach investigations that involve cryptocurrencies, because as the technology grows and becomes more widely adapted, law enforcement will certainly come into contact with it in their investigations.

Facts: Illicit Use of Cryptocurrency

In the years since bitcoin and the other cryptocurrencies have become prevalent, some studies have been done to determine the levels of illicit use. The methodologies of these studies rely on historical criminal data and other sources, such as prevalence of darknet markets, but to the extent of giving us a good picture of the criminal use of cryptocurrencies, there is no real consensus, just very educated guesses. Unfortunately, that is all we can go on due to the anonymous nature of cryptocurrencies. Even still, these studies give us a good idea of the extent of illicit use of cryptocurrency. It is important to note that for the purposes of this thesis, "illicit use" will refer to any use that is associated with an intended criminal act.

According to DEA Special Agent Lilita Infante, a member of the Cyber Investigative Task Force, about 90% of bitcoin use was for criminal purposes five years ago, around 2013 (Russo, 2018). However as of 2018 that number has gone down to 10% of all Bitcoin use. Per Infante, "The volume has grown tremendously, the amount of transactions and the dollar value has grown tremendously over the years in criminal activity, but the ratio has decreased''. 2013 is an interesting year since it was in this year that the Dread Pirate Roberts case took place, with federal agents shutting down the Silk Road darknet marketplace. I will discuss this case later when I discuss the darknet drug markets, but suffice it to say that case brought the more criminal aspects of cryptocurrencies out into the public consciousness.

While the clear majority of bitcoin users are speculators and true believers in decentralized currency, criminal use remains strong. This is partly due to criminals

turning to virtual currencies in general, not just bitcoin, for illegal purposes such as money laundering and sending money across borders without going through official money transfer protocols. In the money laundering section, I will discuss further studies about the level of money laundering using cryptocurrencies. For this section I wanted to see if there was a broad idea of the level of illicit use of cryptocurrencies.

While Bitcoin is still the most widely used cryptocurrency, more privacy oriented virtual currencies such as Monero and Dash are gaining more prevalence on the darknet. They are not as easy to liquidate as Bitcoin however. Agent Infante says that these more anonymous virtual currencies can still be tracked through the public ledger. "'The blockchain actually gives us a lot of tools to be able to identify people,'' she said. 'I actually want them to keep using them'" (Russo, 2018).

The most thorough study on the level of illicit use of cryptocurrencies was published by three researchers in a paper (Foley, Karlsen, & Putnins, 2018) and found that one quarter of Bitcoin users and one half of bitcoin transactions are for illicit purposes. This is an extrapolation that was formulated utilizing three specific approaches, coupled with two refinement methods known as network cluster analysis and detection controlled estimation.

The first approach used in this study was to analyze information from law enforcement agencies and seized information. With this information, they were able to analyze the activity on the blockchain of these specific addresses that were known to be involved in illicit activities by law enforcement. Since the blockchain is public to all, anybody could do historical analysis on red flagged addresses to get a better

understanding of the known illicit use. However, this doesn't give an idea about the total number since these are only the addresses that are known to law enforcement.

The second approach was to use the "Wallet Explorer" service to identify "hot wallets", which are similar to escrow accounts and are used by darknet marketplaces. This approach relies on the assumption that anybody using a darknet marketplace is using it for illegal purposes, which is a fair assumption to make for the purposes of this type of study, and is supported by anecdotal as well as "objective empirical evidence in the form of darknet market scrapes that show the goods and services traded there" (Foley, et al., 2018). Using Wallet Explorer, they were able to identify 17 marketplaces that fit the criteria, mainly that these wallets used small "probing" transactions similar to other financial services and market places online that might send a few cents to an account for the purposes of verification. Using this approach, they identified over 6 million darknet marketplace users.

The third and final approach uses information from users identified in darknet forums. Users post their addresses in these forums for private transactions. They scraped darknet forums for the period of 2013-2017 for postings with addresses that might not "have been caught by authorities and might not be otherwise identified in the data through transactions with known darknet marketplaces" (Foley, et al., 2018). These reflect privately negotiated trade, which users engage in by posting their bitcoin addresses "in cases such as fraud (they did not receive their goods), quality checking, and for the purposes of advertising the address to which funds should be sent" (Foley, et al., 2018). An additional 448 users were identified using this approach that might not otherwise have been observed using the previous two approaches.

Using data culled from these three approaches, the authors of the study next utilized two methods to classify whether users were “illegal users” or “legal users”. The first method uses network cluster analysis to draw connections between users. The useful thing about this method is that it would “reveal ‘communities’ of users and can thereby identify other illegal users that were not part of our initial sample” (Foley, et al., 2018). We can see that this method allows for more refinement of the data found in the three approaches. “In simple terms, the method works as follows. If users A, B, and C are known to be involved in illegal activity (e.g., their bitcoin was seized by law enforcement agencies), a user X that trades exclusively or predominantly with users A, B, or C is likely to also be involved in illegal activity. Similarly, a user Y that trades predominantly with users that are not identified as illegal is likely to be a legal user. This intuition drives the classification of users into legal and illegal on the basis of their transaction partners” (Foley, et al., 2018).

The second method to refine the data is called Detection Controlled Estimation (DCE). This method exploits the differences between legal and illegal users. It also utilizes two processes, violation and detection and models the two to obtain estimates of illegal activity, and culling legal activity and legal users from the estimates. Violation uses a mathematical formula to determine whether a user is involved in legal or illegal activity. Detection uses a similar formula to determine whether or not an illegal user is “detected”. The illegal users used for the sample in the detection formulation are taken from the estimates arrived at using the three approaches.

The conclusions of this study arrive from a scientific study of bitcoin transactions. Using the approaches and methods, they were able to give an estimate of illicit use of

Bitcoin. The study found that 24 million bitcoin users used the cryptocurrency for illicit purposes, with an annual 36 million illicit transactions adding up to $72 billion, with these illicit user's current holdings being around $8 billion (Foley, et al., 2018). However, this is only one cryptocurrency among many, albeit it is the most widely used. A more accurate estimate of illicit use of all cryptocurrencies remains elusive, but the methodology developed in this study can be applied to other cryptocurrencies as well.

The conclusions of this study (50% of all bitcoin transactions are illicit) are different from the DEA's estimates (10% of bitcoin transactions are illicit). They may be closer than expected since the DEA study did say that back in 2013, 90% of bitcoin transactions were illicit, so accounting for historical data, the DEA's estimations may yet line up with the authors of the study. However, the DEA methodologies aren't publicly available, so we can't deconstruct and analyze their estimates.

These two estimates, one by law enforcement and one by academics, give us some insight into the levels of illicit use of cryptocurrencies. It's true that they both only focused on Bitcoin, but knowing the estimates for the most widely used cryptocurrency may give us hints at overall levels for all cryptocurrencies, based on traffic and overall market shares. For the purposes of this paper, I will not delve deeper into estimates of overall illicit use. The goal of this paper is to present the ways in which certain crimes have morphed due to the advent of cryptocurrencies. I will look at more studies when I examine money laundering, however, based on these studies, it is not unfair to say that illicit use of cryptocurrencies accounts for billions of dollars of transactions since the start of the cryptocurrency age.

Cryptocurrency and its effect on the Drug Trade

The drug trade has been influenced by the advent of cryptocurrencies. Whereas in the traditional model of drug trafficking, a drug dealer would sell drugs to a user in person and would receive fiat currency in exchange, the new model allows for the drug dealer and drug purchaser to never meet in person, and the currency traded for the illicit substance is a cryptocurrency which can be sent directly from the users to the dealers wallet. The new model has simplified the process and eliminated some of the risk for both dealer and user. The drugs are sent through the mail, and while there is still some risk of being discovered, overall, the new model seems to be a more effective way for the drug markets to function.

Darknet and Tor

Before we continue, a few terms must be clarified. An *online drug market* is a marketplace that can be accessed via websites located on the darknet for exchanging drugs. The *darknet* or *dark web* is a part of the *deep web*, which is that part of the internet that is not indexed by traditional search engines and can only be accessed through particular authorization, software, or configuration, according to Techopedia (“What is the Darknet?”, n.d.). The darknet is distinct from the deep web, which contains a lot of content that just isn’t accessible to the public, like online banking and websites with a paywall. Email services also account for the bulk of the deep web. The darknet is the area of the deep web where illegal goods, services and content can be procured and accessed.

To access certain websites on the darknet, a user would need a special browser known as a *Tor Browser*.

The core principal of Tor browsing is the onion router, which was developed by the Navy and further refined by DARPA (Defense Advanced Research Projects Agency). Tor browser is run by a nonprofit organization called the Tor Project, a group that believes in anonymity on the Internet. There are two key aspects of onion routing: the first is volunteers who use their computers as "nodes", which are then assigned by the Tor router to randomly go through these nodes before reaching the destination server, and the second aspect of Tor routing is using layers of packets when sending the information through the nodes, where the packets for each node are removed as it passes to its ultimate destination (Nicol, 2016). No individual node knows the destination of a packet of information, only the last place that the packet was. Onion routing was developed with encrypted communication in mind and is used legitimately by journalists for secure communication online or by citizens in countries with Internet censorship, like China. However, it has also allowed the spread of web sites and web markets that would not normally be found on the "surface" Internet, since they traffic in illegal content, products, or services.

Case Study: Ross Ulbricht and the Silk Road

For the purposes of this case study, I will be citing the investigative articles, "The Untold Story of Silk Road, part 1 and 2" (Bearman, 2015). In October 2013, Ross Ulbricht, a 29-year old former Eagle Scout with a Master's Degree in Material Sciences

and Engineering, was arrested for creating and running Silk Road, the largest (at the time) darknet marketplace. Ulbricht was also known as the Dread Pirate Roberts, a moniker he used after he created Silk Road. His arrest and ultimate conviction brought the seedier aspects of the digital world into light. Silk Road was a marketplace fueled by bitcoin and this case was the first to truly demonstrate the effect cryptocurrencies had on the drug markets of the new century -- digital drug markets.

Ulbricht, a Libertarian, was a true believer in Bitcoin when it first came out. That coupled with his views that drug use was a personal choice and that the war on drugs was a failure, led him to come up with the idea of the Silk Road. “Combining an anonymous interface with traceless payments in the digital currency bitcoin, the site allowed thousands of drug dealers and nearly 1 million eager worldwide customers to find each other—and their drugs of choice—in the familiar realm of ecommerce”. The website went live in January of 2011, with Ulbricht selling his own homegrown Psilocybin Mushrooms as the first “vendor”. Before long, more sellers and buyers began flocking to Silk Road and it became an active and ever expanding marketplace. “For a brief time, from 2011 to 2013, it was a wild success. In that relatively short span, Silk Road managed to rack up (depending on how you count) more than $1 billion in sales” (Bearman, 2015). Silk Road had every kind of drug imaginable, from cocaine, marijuana, LSD, and black tar heroin, to prescription medication such as Xanax and Oxycontin. While the usernames and transactions were anonymous on Silk Road, the addresses and names they were sent to were real. The website, which was modeled on Amazon and eBay in terms of its interface, even had a “seller’s guide” on the proper ways to ship the drugs through the mail for the purposes of evasion.

It took about a year for law enforcement to become aware of Silk Road, when postal inspectors began noticing the prevalence of drugs being sent through the mail. A Homeland Security task force, Operation Marco Polo, was assembled to investigate Silk Road. It didn't take long for them to discover that the mastermind behind it was known as Dread Pirate Roberts. DEA Special Agent Carl Force reached out to Dread Pirate Roberts in April of 2012, posing as a drug trafficker called "Nob", looking to purchase the website. Ulbricht gave Force a price for his website; $1 Billion. This number accurately reflected the scale of Silk Road's growth and profits, and Ulbricht/Dread Pirate Roberts would have been considered one of the greatest digital entrepreneurs at this time. However, he was reluctant to sell it for more philosophical reasons. "'It would not be easy to pass the baton without hurting the enterprise,' he messaged Nob. 'And right now, that is more important to me than the money'" (Bearman, 2015). Although this initial attempt at "purchasing" Silk Road was not successful, Force maintained a relationship with Ulbricht through encrypted chat sessions.

Operation Marco Polo wasn't the only investigation that was opened into the Silk Road. Other agencies had opened investigations, including the FBI's cybersquad, but it was a bureaucratic mess to determine who had the lead in the investigation. The FBI's investigation was more focused on the technical side of the Onion Router, trying to find a way to penetrate its seemingly impenetrable encryption. Ultimately it was Operation Marco Polo which got the first big catch, when agent Force lead a sting operation which nabbed Curtis Green, a 47-year-old grandfather who was an administrator for Silk Road. Green agreed to work with Force. Ulbricht quickly realized one of his top employees was arrested, and simultaneously $350,000 in bitcoin had disappeared from several accounts,

which he traced to Green's admin identity. Furious, Ulbricht got in touch with "Nob", and asked him if he would be able to torture Green into returning the stolen bitcoin. Green told Force he knew nothing about any stolen bitcoin, and that his computers where all seized by the DEA around the time the money went missing. Force and the task force then proceeded to stage a torture scene with Green which they videotaped. However, Ulbricht who was becoming increasingly more paranoid around this time, feared that Green would flip and endanger the Silk Road. He got in touch with "Nob" and asked how much it would cost to kill Green. They agreed to $40,000 initially, and another $40,000 when the job was completed. Both were sent to a government controlled account. Force and the other agents on the task force staged an execution with Green participating, and sent photos of the "execution" to Ulbricht.

Around this time, the FBI cybersquad was also able to discover the true IP address of the Silk Road server. After some investigation, they found the physical server was located in Reykjavik, Iceland. They found the IP address because of carelessness on Ulbricht's part. The investigator's "lucky break" came from a thread on Reddit: A user posted a warning that Silk Road's IP address was "leaking"—visible to other computers. Dread Pirate Roberts (or DPR, as he was often called) had been alerted to the problem by a user but ignored the warning. Silk Road's success was making DPR arrogant. He had let down his guard, confidently telling colleagues that the site would never be found (Bearman, 2015). The investigators were able to attain a mirror drive of the server from Icelandic authorities.

After subpoenaing the IP address of the last known login to the Silk Road VPN (virtual private network) the investigators were able to find a physical address. What the

investigators at the FBI also found was more evidence, through chat logs, of Ulbricht ordering other assassinations of people who were blackmailing him. The physical address was a cafe half a block away from where Ulbricht lived. Through information gleaned from a separate investigation, Ulbricht's identity was discovered and connected to the address. A surveillance operation was set up. Search warrants were drawn up and it was decided that they would need to arrest Ulbricht when he was logged into his laptop, so they could get definitive proof that he was accessing the Silk Road server. Ulbricht was in a library working on Silk Road when undercover agents distracted him and proceeded to separate him from his computer and arrest him simultaneously. While performing forensics on Ulbricht's laptop, agents found a mountain of evidence: a list of all the Silk Road servers and the names Ross had purchased them under, 144,000 bitcoins, an accounting spreadsheet for Silk Road (which was thorough and included the very laptop that was seized as an expense), and personal diaries that Ulbricht kept which provided evidence of him organizing and running a criminal conspiracy.

Ultimately, in 2015, Ulbricht was convicted and sentenced to two life sentences without the possibility of parole. While the evidence of Ulbricht procuring murder was factored into his sentence, he was not convicted of any violent crime counts. In a strange twist, DEA Agent Force, "along with a Secret Service agent on his team, was also indicted and arrested this past March for running an elaborate series of rackets and thefts on Silk Road. The 95-page indictment alleged that they stole bitcoins from Silk Road and other exchanges (the digital equivalent of keeping the suitcase full of cash after a dockside heroin bust)" (Bearman, 2015). Force is now serving six and a half years in prison (Jeong, 2015). It was revealed that they were the one's responsible for the theft of

the $350,000 in bitcoin which led to Ulbricht putting a hit on Green. None of this information, however, came out during Ulbricht's trial, and he has subsequently been on appeal with this new evidence. As of today, Ulbricht remains in Prison.

The Opioid Epidemic and Cryptocurrency

In the years since the government took down the Silk Road, the prevalence of darknet markets has not waned. Silk Road was the king at the time, but since its servers were seized by the government, new markets like Agora and Alphabay vied to take over. A familiar cycle was initiated as new markets opened up or expanded and law enforcement, which learned a great deal since Silk Road, was launching operations to take down darknet markets with regularity. Drugs weren't the only things these markets were selling; guns, fake ID's/Passports, counterfeit currency, child pornography, stolen credit card details, and even hacking for hire and assassination services were available. But drugs would remain the focus of most of these markets, especially as the second decade of the twentieth century progressed and the Opioid epidemic in the United States grew to all-time highs.

According to the United States Department of Health and Human Services, which has declared opioid abuse as a public health emergency, since the late 1990's, prescriptions for opioids have increased (HHS, 2018). People were being prescribed strong opioid-based pain medication for injuries and post-surgery and after they recovered, they remained addicted to opioids. This addiction has led to switching to

heroin and other stronger alternatives to satisfy the addiction. According to the government, in 2016 alone, 42,249 opioid overdoses have been recorded (HHS, 2018).

Fueling the opioid epidemic is Fentanyl, a synthetic opioid which, according to the United States Centers for Disease Control (CDC, 2016), is more than fifty times more potent than heroine and one hundred times more potent than morphine. And China seems to be the origin of a lot of Fentanyl coming into the United States. According to an article in the BBC (Reality Check team, 2018), “Katherine Pfaff, spokesperson for the US Drug Enforcement Agency, told the BBC that interceptions from the US postal system, information from people on the ground, and tracking cyber footprints, leads them to believe a ‘significant amount’ comes from China.” China has denied officially that it is the source of most of the fentanyl on the market, but a lot of fentanyl can be traced back to Chinese labs. “The European drug monitoring agency report states: "It appears that most shipments of new fentanyl’s coming into Europe originate from companies based in China" (Reality Check team, 2018). A UN representative has said that China is cracking down on fentanyl production, however government corruption is a problem in China, and once controls are placed on certain chemical substances, new chemicals are created which get around the controls.

According to an article in CNBC (Mui & Sloan, 2018), a man named Aaron Shamo, a former Eagle Scout and cryptocurrency enthusiast, was arrested for trafficking Fentanyl and financing his operation with bitcoin. He was the head of a drug ring that may be linked to 28 fatal overdoses. When his house was raided, authorities found 500 bitcoins. Shamo allegedly ordered the fentanyl from China, and it was shipped to him through the mail. “In 2016, Customs and Border Patrol (CPB) found seven shipments of

fentanyl at the airport. Last year, they found 86. In the first few months of 2018, the number grew to 146" (Mui & Sloan, 2018). The seized shipments account for only a tiny percentage of all fentanyl shipments. The United States Postal Service has a loophole that does not require a sender's address and knowing the contents of the package, unlike UPS and FedEx which do require this information. According to the court documents, Shamo used the purchased fentanyl to make fake oxycodone tablets which he sold on the darknet. He used the USPS to ship the pills to customers in multiple different states.

When Shamo was arrested and his house was raided, several things were seized like cash, gold bars, and a BMW. However, it took a year for any of the bitcoin he had to show up in court paper. This highlights the difficulty to law enforcement when it comes to seized cryptocurrencies. As mentioned before, without knowing the private key, it is cryptographically impossible to get into a suspect's crypto wallet. Lawmakers in Washington have introduced legislation targeting digital currencies that would make them comply with anti-money laundering laws. According to advocates of cryptocurrencies, "'Cryptocurrencies do not kill people. Opiates are killing tens of thousands of people a year,' said Perianne Boring, president of the Chamber of Digital Commerce. 'Blaming bitcoin for this crisis would make as much sense as blaming the internet or cars that drug traffickers have to use'" (Mui & Sloan, 2018). For law enforcement, one of the areas they focus on is the exchanges, where cryptocurrencies are converted to and from fiat currencies. But it becomes difficult once users, who use cryptocurrencies for illegal purchases and sales, turn to creative methods such as using conversion services or "mixing", which will be discussed more in the section on money laundering.

While Shamo was sitting in jail, the price of bitcoin went from $750 to $19,000. On paper, Shamo was worth around $10 million in bitcoin. The government usually liquidates assets after a conviction, but in this case, they were desperate to do it before the price went back down. To foster goodwill, Shamo authorized the government to auction his bitcoin. Shamo has plead guilty and is currently awaiting trial. It would be safe to assume that for every person like Aaron Shamo who gets caught, there are many more who don't and continue to operate today, facilitating the Fentanyl trade using cryptocurrencies like bitcoin to buy the supply from China and accepting it as payment from users who it is shipped to.

Solving the opioid epidemic in the United States is a multifaceted problem. Where cryptocurrencies fit into the mix is in helping facilitate the trade, without knowing the origin and destination. Cryptocurrencies, by their very nature are attractive to those who want anonymous purchases. And eliminating the ability to use cryptocurrencies seems to be the only solution of lawmakers and law enforcement at combatting that aspect of the drug trade. A solution that is less feasible than it might seem, for many financial institutions are seeing the opportunities of the blockchain. As the legitimate uses of cryptocurrencies begin to increase, law enforcement must necessarily become more creative in their investigations to uncover the source and destination of illicit drug purchases. But it would seem that it is just as unfeasible to get rid of the darknet drug markets as it is the traditional drug markets. According to John Collins, head of the International Drug Policy Institute at the London School of Economics (LSE), "In the presence of a demand, supply finds a way" (Reality Check team, 2018). One thing is

certainly clear, cryptocurrencies have become an integral part of facilitating that supply and demand.

Monero

Recently, cryptocurrency analysts and observers have noticed that the cryptocurrency most widely used on the dark web is Monero (McQuaid, 2018). Developed in 2014, it solves many of the privacy issues that Bitcoin and other cryptocurrencies still have, as somebody's Bitcoin address can be linked to their real identity, and hence all their transaction history can be observed on the blockchain. With Monero, that problem has been solved, and that has attracted those who prefer more privacy in their transactions than other cryptocurrencies can provide. Likewise, it has proved popular among criminals on the dark web for this very reason.

Monero uses three essential techniques that are core components of the cryptocurrency (Greenberg, 2017). The first technique that Monero uses is called 'stealth addresses', which are used to generate addresses for receiving Monero that are essentially encrypted; the recipient can retrieve the funds, but no one can link that stealth address to the owner. The second technique is called 'ring signatures,' which groups every Monero spent with as many as a hundred other transactions, mixing the spender's address with strangers', and every subsequent movement of that money makes it exponentially more difficult to trace back to the owner. And the final technique that is used is called 'ring confidential transactions,' which hides the amount of every transaction. In the next section on money laundering I will discuss "mixing" services which obscure bitcoin and

other cryptocurrency transactions, however with Monero that extra step is not needed, since it is baked into the cryptocurrency itself. Some users use Monero in tandem with bitcoins, using exchange tools like Shapeshift to change Monero into bitcoin.

So, what does this mean for the drug trade? Monero has become integrated with the dark web markets Alphabay and Oasis, a move that increased its value by a factor of six (Greenberg, 2017). Along with Dash, another privacy oriented cryptocurrency, Monero is responsible for millions of dollars in revenue in drug sales on the dark web. Going forward the idea of using bitcoin on the dark web for drugs becomes less attractive since, according to another article in Wired (Greenberg, 2018), “if you weren't particularly careful in how you spent your cryptocurrency, the evidence of that drug deal may still be hanging around in plain view of law enforcement, even years after the Silk Road was torn off the dark web.” The blockhain is immutable, and the records of every transaction going back a decade to its inception are there for all the world to see.

Cryptocurrency and its effect on Money Laundering

Money laundering has always played an integral role in any criminal enterprise. Criminals don't want to disclose the origins of their ill-gotten gains, so they obscure those origins. The methods may vary, but the intention is always the same. With the rise of cryptocurrencies, the world of money laundering experienced a revolution. Decentralized, unregulated currencies became attractive to criminals. Additionaly, with stronger Anti-Money laundering laws, traditional methods of money laundering have become more difficult, and cryptocurrencies have become a more attractive alternative.

Anti-Money Laundering Laws in the United States

According to an article published by the United Nations Asia and Far East Institute (Weld, 2011), "As a basic concept, money laundering consists of any act which converts money or other property which is acquired through illegal activity into money or property that appears legitimate, thereby concealing its illegitimate source. The financing of much criminal activity, including terrorist acts, originates with laundered proceeds, generally in the form of cash." In the United States, there are several Anti-Money Laundering (AML) laws. *Basic Money Laundering Statute – 18 U.S.C. § 1956,* enacted in 1986, criminalizes any transaction involving actual proceeds of "over 200 federal, state, or foreign 'specified unlawful activities' (SUAs) by someone who knows that the funds constitute criminal proceeds and conducts the financial transaction in order to accomplish any one of four objectives: (1) to promote the carrying on of SUA; (2) to evade taxes; (3)

to conceal or disguise the nature, source, location, ownership or control of the proceeds; or (4) to avoid any Federal or State transaction reporting requirement" (Weld, 2011).

The Treasury department in 1990 established the Financial Crimes Enforcement Network (FinCEN). According to its mandate, FinCEN's responsibility is to implement, administer, and enforce compliance with the authorities contained in what is commonly known as the 'Bank Secrecy Act'" (FinCEN.gov). According to an article by The Federal Reserve Bank of St. Louis, *The Financial Record Keeping and Reporting of Currency and Foreign Transactions Act of 1970*, commonly known as the *Bank Secrecy Act (BSA),* assigns "requirements for record keeping and reporting by private individuals, banks and other institutions involved in the money transfer business. These records provide evidence used by law enforcement agencies in prosecuting money laundering and other financial crimes" (Stackhouse, 2018). It has been modified several times since its inception, including with the USA PATRIOT Act, which would focus on financial transactions related to terrorism. Every bank must abide by the regulations set out in the BSA, and their compliance programs must coincide with the size and complexity of their operations. And cryptocurrencies have been made to fit into this legal framework. In 2014, FinCEN "designated an administrator or exchanger of cryptocurrencies as a 'money transmitter,' and thus a 'money services business' (MSB) under the regulations" (Stackhouse, 2018). Any exchange where cryptocurrencies are converted to fiat currency must abide by the BSA framework if they wish to be seen as legitimate and avoid legal complications.

Cryptocurrency Money Laundering Studies

But with the anonymous, mostly deregulated nature of cryptocurrencies, AML compliance is a difficult proposition, and criminals have found ways to go around the exchanges adherence to the BSA. Before I go into the methods employed to launder money with cryptocurrencies, I will talk a little bit about some studies that have been done on money laundering with cryptocurrencies. A few terms must be defined before I proceed. *Mixing*, or *tumbling*, are services that "function through the use of an algorithm that allows the service to obscure the history of the tokens they receive", according to an article by the website Cryptonews (Lielacher, 2018). These services have their own addresses that receive the cryptocurrency from a user in small increments, and are mixed in with money sent by other users as well. The "clean" cryptocurrency is then sent back to the original address of the user, or to a different address specified by the user. An example of some of these services is Coinmixer.se, Helix, and Bitcoin Blender. Most tumblers are on the dark web.

According to a report by Ciphertrace, "a quantitative analysis of all the transactions on the 20 top cryptocurrency exchanges globally revealed that 97% of direct bitcoin payments from identifiable criminal sources were received by unregulated cryptocurrency exchanges" (Ciphertrace, Q3 2018, p. 2). Their analysis also found 380,155 bitcoins that were received by cryptocurrency exchanges from criminal sources between January 2009 and September 2018. With exchanges seeking legitimacy by conforming to BSA guidelines, it would appear that using the exchanges to launder money has become more difficult. This is because to use a BSA compliant

cryptocurrency exchange, a user must use their true identity to register and connect a bank account. All transactions are then logged by the exchange and on the blockchain, and can be analyzed by FinCEN and other law enforcement. Those seeking to launder using cryptocurrencies would be attracted to exchanges that are registered in countries with weak AML laws. According to an earlier report by Ciphertrace (Ciphertrace, Q2 2018, p. 3), over $1 Billion dollars were laundered using conversion services such as tumblers. A large amount of the laundered funds came from cryptocurrencies that were stolen from exchanges.

Another study by *Elliptic* and the *Center on Sanctions & Illicit Finance* (Fanusie & Robinson, 2018), found that from 2013 to 2016 the rate of money laundered through conversion services has increased. This study's focus was narrow, looking at only bitcoin, but the methodologies it discovered can prove useful to understanding the way laundering is done using all cryptocurrencies. According to their analysis, "bitcoin exchanges received the greatest amount of identified illicit bitcoins out of all conversion services, but they also processed the majority of Bitcoin transactions overall. The conversion services with the highest proportion of Bitcoin laundering within their platforms were mixers and online gambling sites." Conversion services based in Europe received five times more illicit bitcoins than North America. "A large percentage of conversion services that receive illicit bitcoins appear to conceal their country of operations, making it a challenge to identify the legal jurisdictions responsible for their AML enforcement." This would seem to match the conclusion of the Ciphertrace report that countries with lax AML standards are more attractive for cryptocurrency money laundering.

Methods for Crypto Money Laundering

A criminal or group who wishes to launder their money using cryptocurrencies can do so in ultimately three different ways (Crosman, 2018). One way is to use a mixing service, as mentioned before. In this method, you contribute funds into a pool that isn't traceable on the blockchain, so when you receive the cleaned funds there's no way to know using the blockchain that the new money is connected to the old money. Mixing services usually charge a rate of 3% to perform one of these cleaning transactions and are usually written by people with high levels of education (Crosman, 2018).

Another method for laundering money through cryptocurrencies is to use service like Shapeshift. "These can have legitimate uses, but they can also be used to take bitcoin, flip it into Ethereum and into another currency before turning it back into bitcoin" (Crosman,2018). Once the new coin comes out after the flipping process, it is nearly impossible to connect it back to the original. The final way to launder money is to simply do it through the exchange, without using any service. However, this is the least secure and most easily identifiable method if the launderer were to come under any scrutiny.

It is believed that about $9 million dollars of an estimated $88 million laundered over a two-year period, was laundered through ShapeShift, following an investigation by Wall Street Journal reporters (Scheck & Shifflett, 2018). However, this avenue for money laundering may not last long as after the Wall Street journal investigation came out, the Chief Legal Officer of ShapeShift has said they will begin requiring users to provide

identification in order to minimize the company's risk. It is possible that a competitor will fill the role of shapeshift in the future, perhaps in a jurisdiction with less AML regulations.

A lot of money laundering with crypto currencies is related to hacking of exchanges, like CoinCheck Inc. which is a Tokyo based crypto exchange. Hackers made off with $500 million dollars that were kept in "hot wallets", which in this context refers to wallets that are connected to external networks (Alpeyev & Nakamura, 2018). And as mentioned before, the Ciphertrace Q2 report mentioned that over $1 billion dollars had been stolen from exchanges and laundered. Exchange theft would seem to be the number one cause of crypto money laundering at the moment, trumping the amounts laundered by other criminals.

Ultimately privacy coins like Monero, Dash, and Zcash, would seem to be the preferred cryptocurrencies of any money laundering operation due to their anonymous nature. In less private cryptocurrencies, the blockchain records all transactions and if an address is known to law enforcement, it can be traced to any user that transacted with that address and vice versa. However, in most case criminals and money launderers just assume that exchanges have no AML regulations and that their transactions aren't being tracked (Crosman, 2018). For the less sophisticated money launderers, the only thing stopping law enforcement from uncovering them is sufficient and focused analysis of the blockchain and subpoenas to the exchanges for the identification of the owner of the suspicious address.

Ransomware and Cryptojacking

The concept of *ransomware* is not a new one. In a ransomware attack, a user's downloads a piece of malware inadvertently and this malware proceeds to encrypt files on the user's pc (Palmer, August 2018). The only way to get back access to the encrypted files is by paying the criminals who designed the ransomware. The first ransomware attack was recorded in 1989 (Kassner, 2010), when Dr. Joseph Popp sent out a trojan called "PC Cyborg" which encrypted and hid files on a user's C: drive. Next a dialogue box popped up and asked for $189 to be sent to the PC Cyborg Corporation. The PC Cyborg ransomware was easily overcome because it relied on symmetric cryptography, which was easy to decrypt, and the culprit was soon identified. Since then, ransomware attacks have not stopped being in use by cyber criminals looking to make money by tricking computer users to going to bad sites or downloading files that may seem safe enough, but which contain the Trojan malware that infects and decrypts their computers. These attacks have also become more sophisticated and complex.

Infecting individual users was one thing, however these cyber criminals began to infect corporate networks with ransomware, which is bad in two ways; the ransom being demanded to decrypt the files, which may be a substantial sum, and the loss of productivity due to the encryption of files and drives needed for business. Another type of ransomware was a "law enforcement" ransomware, which purported to be from a law enforcement organization and notified the user that they have committed illegal online activity and would be arrested if they didn't pay a fine (Palmer, 2018). While fiat currencies were the traditionally preferred ransom payment, in the last decade

ransomware attacks have become exclusively bitcoin and cryptocurrency-based, in terms of the preferred method of payment for decryption of the user's files and drives.

Cryptowall

Between April 2014 and June 2015, the FBI received almost a thousand complaints regarding a new type of ransomware called "Cryptowall" which utilized bitcoin as its preferred payment method (Higgins, 2015). Targets ranged from law enforcement to public schools, and the ransom demanded ranges from $200 to $10,000. The FBI estimates around $18 Million in losses for that period from Cryptowall. The payments requested were to be made in bitcoin, something that the FBI at the time recognized as more preferable to fiat currencies due to it being decentralized, secure, and anonymous.

Ultimately it was found that over 600,000 computers were infected by Cryptowall (Counter Threat Unit, 2014). It spread through an aggressive campaign of spam emails with malicious attachments and links, download attacks from infected websites, and installations by another malware already running on the computer. The command-and control servers for Cryptowall assigned unique identifiers to each infected PC, and generated RSA public keys for each one. The public keys would be used to decrypt files on the infected PC's, like videos, documents, and photos. To get the private key that would decrypt those files, the victim would need to send bitcoin to the assailant. Earlier versions of cryptowall utilized other payment methods such as pre-paid cards (Counter Threat Unit, 2014). And if the victim didn't pay the ransom in the allotted time, the

ransom amount increased. According to researchers at the Counter Threat Unit at Dell SecureWorks (Counter Threat Unit, 2014), “Of nearly 625,000 infections, 1,683 victims (0.27%) paid the ransom, for a total take of $1,101,900 over the course of six months”.

When Cryptowall is executed, it injects its malicious code into new processes that are created. By creating a process called “explorer.exe”, Cryptowall is then able to execute more processes which cause Windows Volume Shadow Copy Service (VSS) to delete all shadow copies on the system and disables the system restore function by modifying the windows registry. VSS is important for accessing an earlier “snapshot” of your system. Finally, the ransomware creates a malicious process called “svchost.exe -k netsvcs” which allows it to run with all of the victim’s user privileges (Counter Threat Unit, 2014). Once Cryptowall is active on a victim’s computer, it sends a message to its home server over HTTP on TCP port 80. Some of these servers are on the Tor network, adding a layer of security to the operation. After the server sends an RSA public key, encryption of the victim computer is initiated. The victim would be presented with a bitcoin address of where to send the ransom too. This address would change about once a day. The analysts at the Counter Threat Unit found that by analyzing the known addresses, they were able to account for 939 BTC of paid ransom money, which at the time was worth close to half a million dollars. This was however a small subset of all the payments.

WannaCry

In May 2017, a new ransomware attack spread across the globe. It was called WannaCry, and it was not only one of the biggest ransomware attacks, it was one of the biggest cyber-attacks. Hundreds of thousands of computers worldwide were infected. This ransomware was more dangerous than others because it utilized an exploit within the Windows system itself, called "EternalBlue" (Symantec Security Response, 2017). WannaCry encrypts 176 different file types and adds .WCRY to the filename. The victim is then told to pay $300 in bitcoin, which would double after three days. There was also a threat that if after seven days the ransom wasn't paid, then the encrypted files would be deleted, however Symantec researchers found nothing within the code that would cause file deletion. The exploit that allowed for the propagation of WannaCry was patched by Microsoft in March 2017, but if a user hadn't updated their computer, they were vulnerable.

Similar to Cryptowall, the victims are given a unique bitcoin address to send the ransom to. WannaCry is composed of multiple components (Noerenberg, Costis, & Quist, 2017), "an initial dropper contains the encrypter as an embedded resource; the encrypter component contains a decryption application ("Wana Decrypt0r 2.0"), a password-protected zip containing a copy of Tor, and several individual files with configuration information and encryption keys". It makes use of an exploit discovered by NSA Analysts and stolen and leaked to the world by a group known as Shadow Brokers (Ng, 2017). This is the exploit that was patched in March 2017. The vulnerability was in the Server Message Block (SMB) protocol, which allowed the malware to spread to all

systems that had this protocol enabled, and “this vulnerability allows remote code execution over SMB v1. WannaCry utilizes this exploit by crafting a custom SMB session request with hard-coded values based on the target system. Notably, after the first SMB packet sent to the victim’s IP address, the malware sends two additional packets to the victim containing the hard-coded IP addresses 192.168.56.20 and 172.16.99.5” (Noerenberg, et. al, 2017). Like CryptoWall, WannaCry deletes any Windows Shadow Copies, making recovery impossible. The WannaCry attack caused a lot of finanical damage to many organizations mostly in the form of productivity loss but also more real world damage, costing the British National Health Service around £100m, and 19,000 cancelled appointments (Palmer, October 2018).

Ransomware, which used to have the ransom paid using fiat currencies and through prepaid cards, has evolved to use bitcoin in some of the biggest, and costliest attacks in recent years. Bitcoin is anonymous, and the attacker’s addresses are known, but the money can easily be laundered through the use of mixers and tumblers, as well as applications like Shapeshift, and other crypto laundering methods. It is believed that the hacking group Lazarus, which may have connections to North Korea, was responsible for WannaCry. On September 6, 2018, the United States Department of Justice charged a 34-year-old North Korean programmer named Park Jin Hyok for propagating WannaCry, as well as several other cyber-attacks in recent years, including the Sony Hack (Cimpanu, 2018). Hyok has yet to be apprehended and is wanted by the FBI (FBI, 2018).

Crypto-Mining and The Rise of Cryptojacking

In recent years, a new type of cyber-attack has become prevalent (Dimov, 2018). It is called *cryptojacking,* and it installs cryptocurrency mining malware onto a victim's computer for the purposes of utilizing a victims central processing unit (CPU) or graphics processing unit (GPU) to mine cryptocurrencies. To better understand cryptojacking, we need to discuss how cryptocurrency mining works.

As mentioned earlier, whenever a transaction is made on the blockchain, it needs to be encrypted and put into a "block". For each block to be added to the blockchain, it must be verified using cryptographic math puzzles, which require a lot of computing power. This is where *miners* come in. A miner is a person or persons running a computer or group of computers that solve the mathematical puzzles that verify each block. For this service, the miners earn a fee, a small portion of that block's coin as well as an additional reward, depending on the particular blockchain architecture (Evangelho, 2018). The amount of the fee isn't a lot, but with enough computing power, mining can be a profitable enterprise, or at least it was before, when there were less blocks mined. Since there are a finite number of bitcoins and hence blocks to be mined, the value of mining corresponds to how many bitcoins are left. And it requires more and more CPU power to mine a single block as time goes by. On average, the reward for mining a block is halved every four years or so (Hong, 2018). However, it is not only a matter of verifying transactions, a miner needs to be the first to answer the mathematical puzzle, which requires having a high "hash rate" when it comes to computing power. The hash rate refers to the number of hexadecimal strings that a computer guesses. Mining can be very lucrative if a

significant investment in computing power has been made, allowing for the faster hash rate and quicker verification of the block of transactions. In Russia, scientists at a nuclear facility were arrested by authorities when it was discovered that they were using powerful supercomputers to mine bitcoin (Gallagher, 2018).

To mine cryptocurrencies, a user needs a computer with a powerful CPU or GPU. The user would then download software to mine a specific cryptocurrency and connect their wallet address to it for their miner's fee and rewards to be sent to it. Mining became so popular among cryptocurrency enthusiasts and those wishing to make some money in the last few years, that they have caused the price of graphics cards to go up due to scarcity (Warren, 2018).

How Cryptojacking Works

Essentially, cryptojacking is a piece of malware that infects a victim's computer and uses it to power a cryptocurrency mining operation. To illustrate how it works, I will examine the dofoil attack. Using traditional methods of inserting a Trojan into a victims pc, dofoil proceeds to use "process hollowing" which creates a new instance of legitimate process and replaces it with a malicious program that proceeds to run a coin mining operation (Dimov, 2018). Dofoil also modifies the registry, similar to ransomware attacks. Dofoil connects to a command and control server that provides it with malware and instructions. Victims will sometimes never know their computers are being used to mine cryptocurrencies, except for noticing their computer fans working overtime to reduce the heating caused by the high CPU or GPU usage. Internet of Things (IoT)

devices are an attractive target for cryptojacking operations because they aren't as monitored by users on a day-to-day basis (Biasini, et. al, 2018).

Cryptojacking is being seen by cybercriminals as an easier and more profitable attack than ransomware, due to the fact that only a small percentage of ransomware recipients will pay up (Biasini, et. al, 2018). Also as systems and technology improve, the methods of detection for ransomware become easier, and it becomes more detectable and instantly blocked. Cryptojacking may be a good alternative for cybercriminals in the meantime. An average "cryptojacked" computer can produce around $0.25 of Monero a day, and if there are around 2,000 computers that is about $500 a day or over $180,000 a year (Biasini, et. al, 2018). Using a *botnet*, which is a network of computers working in tandem to fulfill certain tasks, cryptojacking operators can leverage a large amount of computing power for the purposes of mining cryptocurrencies. An illegal botnet is a collection of infected computers which have traditionally been used for nefarious purposes like Distributed Denial-of-Service (DDoS) attacks, which send a large amount of internet traffic to a particular website or server, overwhelming it with requests and causing legitimate users not to be able to access that website or server due to the massive amount of traffic.

Smominru, a massive botnet, has been used for just this purpose. It leverages the EternalBlue exploit, targets the Windows Management Infrastructure, and is activated after a Microsoft Word file, which is sent as an attachment in phishing emails, is opened (Bloomberg, 2018). Once the file is opened, a Microsoft Word macro executes a script that in turn runs a Powershell script which downloads and then installs a mining program which runs on the infected computer. The Smominru botnet mines Monero exclusively,

and has made an estimated upwards of $3.6 million dollars for its operator (Kafeine, 2018).

An interesting new development in terms of cryptojacking is the concept of some websites using cryptojacking in lieu of advertising. Known as in-browser cryptojacking, a website visitors CPU power would be hijacked for the purposes of cryptojacking (Saad, et. al, 2018). One such service that allows cryptojacking in-browser is Coinhive, which was pitched as a way for website owners to make money off of website visits without running ads (Krebs, 2018). Coinhive is a javascript program which can be added to the code of any website (Saad, et. al, 2018). Coinhive specifically mines Monero, which it does by utilizing the CPU of a user's computer for the duration of their visit to that website. However idealistic cryptojacking instead of ads can be, the concept of in-browser cryptojacking has been hijacked my malicious users that run the Coinhive service on websites without the website owner's knowledge or permission, routing all the funds mined to an address not associated with the owner of the website. An estimated 32,000 websites run Coinhive scripts, and many of them are the result of malicious takeover through script injection (Saad, et. al, 2018). To address this, Coinhive have released a new version called "AuthedMine" which seeks a user's consent when they visit a website to mine using their CPU power, however AuthedMine accounts for only 35% of the total use of Coinhive services (Krebs, 2018).

Cryptojacking is a lucrative path for cyber criminals that doesn't require the risks of ransomware, where the victims know they are being attacked. In a cryptojacking situation, most victims will not know they have been infected by malware which uses their computers processing power to mine cryptocurrencies. While the cybercriminal is

still infecting a user's computer with malicious code, there is no overt threat for money and there is no encryption or destruction of files. Going forward, and analyzing how simple it is to set up a botnet and send out phishing emails with malicious code, it would appear that cryptojacking will be used more and more. It may be that there will come a day when crypto mining is no longer feasible to earn the necessary profits that attract it currently, but until that day comes, we have a new kind of computer crime that nets criminals millions of dollars which did not exist and could not exist without cryptocurrencies.

Law Enforcement and Cryptocurrencies

This thesis has highlighted how cryptocurrencies have provided a new avenue for carrying out certain crimes. The reason cryptocurrencies have been used is because it has been seen as an alternative to the riskier, older models for crimes such as drug trafficking and money laundering. However, this does not mean that law enforcement is without any tools or methods to fight crime in the cryptocurrency age.

Essentially, the blockchain is the number one tool that law enforcement has to track illicit transactions. Effective analysis of the blockchain can yield a great deal of useful information for criminal investigations. Blockchain startup companies like Chainalysis, have developed tools like Chainalysis KYT (Know your transaction) which track suspicious transactions in real time and are used by exchanges for compliance purposes (Milano, 2018). Chainalysis is also used by law enforcement organizations for tracking transactions on the blockchain. There are other startups offering blockchain analysis tools as well. The Bitfury group launched Crystal, an all-purpose and user-friendly blockchain analysis tool which is easy to navigate and can be used by law enforcement (Bitfury Group, 2018). The prevalence of blockchain analysis tools seems to be growing.

Also, law enforcement can be more effective by identifying cryptocurrency artifacts like wallets and cryptocurrency hashes on suspect computers (Tziakouris, 2018). Criminals might leave their public addresses in plain view on their computers or on pieces of paper. If law enforcement knows all of a criminal's public addresses they could better analyze their transactions on the blockchain. Also, if a criminal is careless enough to leave their private key in plain view as well, either saved on their computer or a drive,

or written on a piece of paper, this would give law enforcement direct control of a criminal's cryptocurrency assets. Even the random assembly of words that form the seed phrase linked to their private key can be useful and law enforcement should know what these look like if they are performing digital forensics on a suspects computers.

Conclusion

The purpose of this thesis was to examine the effects of cryptocurrencies on the criminal landscape. This thesis focused on three avenues of crime, drug trafficking, money laundering, and ransomware/cryptojacking. Ransomware and cryptojacking were grouped together because they are based on a similar principle, hijacking a user's computer for the purposes of extracting money from the user. The methods might be different but the result is the same. Whereas the first two, drug trafficking and money laundering are traditional crimes which have existed long before cryptocurrencies and computers, ransomware and later cryptojacking are fairly new types of computer crimes that rely on malicious software. I chose not to look at other types of crimes, because I felt that these three would give a good impression of the level of sophistication that cryptocurrencies have brought to the table in terms of facilitating these crimes.

Drug trafficking has always been a dangerous business for both buyer and seller. The risks of in-person drug transactions are clear, whether by law enforcement, or by rival drug dealers, a presence on the "street" necessarily presents risks that the use of darknet drug markets don't. Buyer and seller never have to meet in person with the use of a market place like AlphaBay or in previous years Silk Road. The transaction is smooth, using cryptocurrencies, the buyer sends the seller his money and once received the seller ships the drugs through the USPS. The risks here are that an inspection will lead to confiscation, but these instances are rare, and since the USPS does not require a sender's address, as well as knowledge of the packages contents, it would be a safer alternative than dealing on the street. Any disputes are regulated through the markets, and sellers who pocket money and don't send the product are not tolerated by the drug market

moderators. Repeat business on these dark markets would mean upholding their end of the bargain. As long as these drug markets exist, they will continue the drug trade, and cryptocurrencies will continue being used as the payment method.

Money laundering has been made simpler through the use of cryptocurrencies because of the use of mixers/tumblers and currency exchangers like Shapeshift and others. AML/KYC (Anti Money Laundering/Know Your Customer) regulations are being adapted by the larger exchanges like Coinbase, however many exchanges still remain outside of United States regulations, especially exchanges in countries with weak AML regulations.

Cryptocurrencies anonymous nature also allows for the circumventing of the SWIFT banking system, which allows for cross-border money transfers between participating financial institutions. Cryptocurrencies don't discriminate based on country and a person can send any amount of money to an address in another country, including a country that is sanctioned by US law. While analysis of a blockchain coupled with forensic accounting could trace transactions, using mixers can further obscure the origin of a particular piece of cryptocurrency. And with cryptocurrencies like Monero, that have complete anonymity baked into its design, the appeal of money laundering using cryptocurrencies remains a viable alternative to traditional money laundering methods.

In the coming years, cryptocurrencies will grow in use and prevalence beyond just for speculation purposes. As more organizations and vendors begin to accept cryptocurrencies, and as the prices stabilize, cryptocurrencies will be used for transactions more often. And with wider adopted legitimate use, the illegitimate uses will grow concurrently. Law enforcement will have to embrace tools that analyze transactions

on the blockchain if they wish to keep up with the growing use of cryptocurrencies in criminal cases. Ultimately, better AML regulation of exchanges will play a big role as well, but that seems to be trending in a positive direction as many cryptocurrency exchanges seek to minimize their risk by adapting AML/KYC regulations. With billions of dollars worth of illicit transactions, it can be confidently said that crime has changed due to cryptocurrencies, and will continue to as long as the profits and ease of use continue.

References

All Coins. (n.d.). Retrieved from https://coinmarketcap.com/coins/views/all/

Alpeyev, P., & Nakamura, Y. (2018, January 29). How to Launder $500 Million in Digital Currency. Retrieved from https://www.bloomberg.com/news/articles/2018-01-29/how-to-launder-500-million-in-digital-currency-quicktake-q-a

Bearman, J. (2017, May 01). The Untold Story of Silk Road, Part 1. Retrieved from https://www.wired.com/2015/04/silk-road-1/

Bearman, J. (2017, May 01). The Untold Story of Silk Road, Part 2: The Fall. Retrieved from https://www.wired.com/2015/05/silk-road-2/

Biasini, N., Brumaghin, E., Mercer, W., Reynolds, J., Khodijbaev, A., & Liebenberg, D. (2018, January 31). Ransom Where? Malicious Cryptocurrency Miners Takeover, Generating Millions. Retrieved from https://blog.talosintelligence.com/2018/01/malicious-xmr-mining.html

Bitfury Group. (2018, January 30). Bitfury Launches Crystal - A Blockchain Investigative Tool for Law Enforcement and Financial... Retrieved from https://medium.com/meetbitfury/bitfury-launches-crystal-a-blockchain-investigative-tool-for-law-enforcement-and-financial-3d7712dd5dce

Blenkinsop, C. (2018, August 13). Crypto Wallets, Explained. Retrieved from https://cointelegraph.com/explained/crypto-wallets-explained

Bloomberg, J. (2018, March 04). Top Cyberthreat Of 2018: Illicit Cryptomining. Retrieved from

https://www.forbes.com/sites/jasonbloomberg/2018/03/04/top-cyberthreat-of-2018-illicit-cryptomining/#284806fd5ae8

Centers for Disease Control and Prevention. (2016, December 16). Opioid Overdose. Retrieved from https://www.cdc.gov/drugoverdose/data/fentanyl.html

Ciphertrace (2018). 2018 Q2 Cryptocurrency Anti-Money Laundering Report (Rep.). Retrieved https://cdn2.hubspot.net/hubfs/4345106/crypto_aml_report_2018q2.pdf?submissionGuid=10035160-48de-4567-adc7-6bd8e1b725cd

Ciphertrace (2018). 2018 Q3 Cryptocurrency Anti-Money Laundering Report (Rep.). Retrieved https://ciphertrace.com/wp-content/uploads/2018/10/crypto_aml_report_2018q3.pdf

Cimpanu, C. (2018, September 07). How US authorities tracked down the North Korean hacker behind WannaCry. Retrieved from https://www.zdnet.com/article/how-us-authorities-tracked-down-the-north-korean-hacker-behind-wannacry/

Cochrane, M. (2018, April 03). The History of Bitcoin. Retrieved from https://www.fool.com/investing/2018/04/02/the-history-of-bitcoin.aspx

Constantin, L. (2014, August 29). CryptoWall ransomware held over 600K computers hostage, encrypted 5 billion files. Retrieved from https://www.pcworld.com/article/2600543/cryptowall-held-over-halfamillion-computers-hostage-encrypted-5-billion-files.html

Crosman, P. (2018, July 03). Crypto money laundering up threefold in 2018: Report.

Retrieved from https://www.americanbanker.com/news/crypto-money-laundering-rose-3x-in-first-half-2018-report

Dell SecureWorks Counter Threat Unit Intelligence. (2014, August 27). CryptoWall Ransomware Threat Analysis. Retrieved from https://www.secureworks.com/research/cryptowall-ransomware

Dimov, D., & Juzenaite, R. (2018, June 14). The Decline of Ransomware and the Rise of Cryptocurrency Mining Malware. Retrieved from https://resources.infosecinstitute.com/the-decline-of-ransomware-and-the-rise-of-cryptocurrency-mining-malware/#gref

Evangelho, J. (2018, March 13). Mining 101: An Introduction To Cryptocurrency Mining. Retrieved from https://www.forbes.com/sites/jasonevangelho/2018/03/13/mining-101-what-exactly-is-cryptocurrency-mining/#3fff36f4a83a

Fanusie, Y. J., & Robinson, T. (2018). Bitcoin Laundering: An Analysis of Illicit Flows Into Digital Currency Services (Rep.). Retrieved from https://cdn2.hubspot.net/hubfs/3883533/downloads/BitcoinLaundering.pdf

FBI. (2018). PARK JIN HYOK. Retrieved from https://www.fbi.gov/wanted/cyber/park-jin-hyok

FinCEN's Mandate From Congress. (n.d.). Retrieved November 6, 2018, from https://www.fincen.gov/resources/fincens-mandate-congress

Foley, S., and Karlsen, J., and Putnins, T. (January 17, 2018). Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies? Available at SSRN: https://ssrn.com/abstract=3102645 or http://dx.doi.org/10.2139/ssrn.3102645

Gallagher, S. (2018, February 09). Russian nuclear weapons engineers caught minting blockchange with supercomputer. Retrieved from https://www.arstechnica.com/tech-policy/2018/02/russian-nuclear-weapons-engineers-caught-minting-blockchange-with-supercomputer/

Greenberg, A. (2017, June 03). Monero, the Drug Dealer's Cryptocurrency of Choice, Is on Fire. Retrieved from https://www.wired.com/2017/01/monero-drug-dealers-cryptocurrency-choice-fire/

Greenberg, A. (2018, February 01). Your Sloppy Bitcoin Drug Deals Will Haunt You for Years. Retrieved from https://www.wired.com/story/bitcoin-drug-deals-silk-road-blockchain/

Higgins, S. (2015, August 13). FBI: Recent Bitcoin Ransomware Losses Top $18 Million. Retrieved from https://www.coindesk.com/fbi-bitcoin-ransom-attack-loss-18-million/

Hong, E. (2018, October 31). How Does Bitcoin Mining Work? Retrieved from https://www.investopedia.com/tech/how-does-bitcoin-mining-work/

Investopedia. (2018, August 04). Cryptocurrency. Retrieved from https://www.investopedia.com/terms/c/cryptocurrency.asp

Jeong, S. (2015, October 20). DEA Agent Who Faked a Murder and Took

Bitcoins from Silk Road Explains Himself. Retrieved from https://motherboard.vice.com/en_us/article/8q845p/dea-agent-who-faked-a-murder-and-took-bitcoins-from-silk-road-explains-himself

Kafeine. (2018, January 31). Smominru Monero mining botnet making millions for operators. Retrieved from https://www.proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators

Kassner, M. (2010, January 11). Ransomware: Extortion via the Internet. Retrieved from https://www.techrepublic.com/blog/it-security/ransomware-extortion-via-the-internet/

Khormali, A., Mohaisen, A., & Saad, M. (2018). End-to-End Analysis of In-Browser Cryptojacking. Arxiv, 1809.02152, 1-15. Retrieved from https://arxiv.org/pdf/1809.02152.pdf

Krebs, B. (2018, March 18). Krebs on Security. Retrieved from https://krebsonsecurity.com/2018/03/who-and-what-is-coinhive/

Lielacher, A. (2018, June 22). Coin Mixers: How Do They Work and Should You Use Them? Retrieved from https://cryptonews.com/exclusives/coin-mixers-how-do-they-work-and-should-you-use-them-2070.htm

McQuaid, D. (2018, January 23). Bitcoin warning: Criminals turning to other cryptocurrencies on Dark Web. Retrieved from https://www.express.co.uk/finance/city/908747/bitcoin-monero-dark-web-Chainalysis-North-Korea-cryptocurrency

Milano, A. (2018, April 05). Chainalysis Raises $16 Million for Real-Time Crypto

Compliance. Retrieved from https://www.coindesk.com/chainalysis-raises-16-million-for-real-time-crypto-compliance

Mui, Y., & Sloan, K. J. (2018, April 15). How bitcoin is fueling America's opioid crisis. Retrieved from https://www.cnbc.com/2018/04/13/how-bitcoin-and-cryptocurrencies-are-fueling-americas-opioid-crisis.html

Ng, A. (2017, May 16). Hackers behind stolen NSA tool for WannaCry: More leaks coming. Retrieved from https://www.cnet.com/news/hackers-behind-stolen-nsa-tool-for-wannacry-more-leaks-coming/

Nicol, W. (2016, January 19). What is Tor? A Beginner's Guide to the Deep Web. Retrieved from https://www.digitaltrends.com/computing/a-beginners-guide-to-tor-how-to-navigate-through-the-underground-internet/

Noerenberg, E., Costis, A., & Quist, N. (2017, May 16). A Technical Analysis of WannaCry Ransomware. Retrieved from https://logrhythm.com/blog/a-technical-analysis-of-wannacry-ransomware/

Noonan, L. (2018, September 25). JPMorgan widens blockchain payments to more than 75 banks. Retrieved from https://www.ft.com/content/41bb140e-bc53-11e8-94b2-17176fbf93f5

O'Neal, S. (2018, November 05). Bank of America Has the Most Blockchain Patents, But Is It Actually Going to Use Them? Retrieved from https://cointelegraph.com/news/bank-of-america-has-the-most-blockchain-patents-but-is-it-actually-going-to-use-them

Palmer, D. (2018, August 22). What is ransomware? Everything you need to know about

one of the biggest menaces on the web. Retrieved from https://www.zdnet.com/article/ransomware-an-executive-guide-to-one-of-the-biggest-menaces-on-the-web/

Palmer, D. (2018, October 12). This is how much the WannaCry ransomware attack cost the NHS. Retrieved from https://www.zdnet.com/article/this-is-how-much-the-wannacry-ransomware-attack-cost-the-nhs/

Reality Check Team. (2018, September 24). Fentanyl crisis: Is China a major source of illegal drugs? Retrieved from https://www.bbc.com/news/world-45564744

Russo, C. (2018, August 7). Bitcoin Speculators, Not Drug Dealers, Dominate Crypto Use Now. Retrieved from https://www.bloomberg.com/news/articles/2018-08-07/bitcoin-speculators-not-drug-dealers-dominate-crypto-use-now

Scheck, J., & Shifflett, S. (2018, September 28). How Dirty Money Disappears Into the Black Hole of Cryptocurrency. Retrieved from https://www.wsj.com/articles/how-dirty-money-disappears-into-the-black-hole-of-cryptocurrency-1538149743

Skvorc, B. (2017, March 10). How to Read Bitcoin Blockchain Data on Blockexplorer? Retrieved from https://bitfalls.com/2017/10/03/read-bitcoin-blockchain-data-blockexplorer/

Stackhouse, J. (2018, April 23). What Is the Bank Secrecy Act, and Why Does It Exist? Retrieved from https://www.stlouisfed.org/on-the-economy/2018/april/what-bank-secrecy-act-why-exist

Symantec Security Response. (2017, October 23). What you need to know about the

WannaCry Ransomware. Retrieved from https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack

Tziakouris, G. (2018), Cryptocurrencies—A Forensic Challenge or Opportunity for Law Enforcement? An INTERPOL Perspective, IEEE Security & Privacy, vol. 16, no. 4, pp. 92-94, July/August 2018.
doi: 10.1109/MSP.2018.3111243

United States Health and Human Services. (n.d.). What is the U.S. Opioid Epidemic? Retrieved November 5, 2018, from https://www.hhs.gov/opioids/about-the-epidemic/index.html

Warren, T. (2018, January 30). Bitcoin mania is hurting PC gamers by pushing up GPU prices. Retrieved from https://www.theverge.com/2018/1/30/16949550/bitcoin-graphics-cards-pc-prices-surge

Weld, J. B. (2011). Current International Money Laundering Trends and Anti-Money Laundering Co-Operation Measures. Resource Material Series (UNAFEI), 37-47.

What is the Darknet? - Definition from Techopedia. (n.d.). Retrieved fro https://www.techopedia.com/definition/2395/darknet

Wild, J., Arnold, M., & Stafford, P. (2015, November 01). Technology: Banks seek the key to blockchain. Retrieved from https://www.ft.com/content/eb1f8256-7b4b-11e5-a1fe-567b37f80b64

Williams, S. (2018, April 11). 20 Real-World Uses for Blockchain Technology. Retrieved from https://www.fool.com/investing/2018/04/11/20-real-world-uses-for-blockchain-technology.aspx

Wilson, S. (2018, June 01). Blockchain explained in plain English. Retrieved from https://www.zdnet.com/article/blockchain-explained-in-plain-english/