Winter 1-15-2019

Money Laundering Through Cryptocurrencies

George Forgang
La Salle University, forgangg1@student.lasalle.edu

Money Laundering Through Cryptocurrencies

Greg Forgang

11/7/18

Integrative Capstone

Table of Contents

Executive Summary

Bitcoin, the world's first cryptocurrency, was first introduced in 2009, by Satoshi Nakamoto. While many believe the name is a pseudonym, and the true identity of the creator(s) is unknown, it is an undisputed fact that cryptocurrencies have introduced an indelible change to monies worldwide. Consequently, cryptocurrencies have also introduced a plethora of new opportunities for money laundering activity.

While cryptocurrencies follow the same three-step laundering process of placement, layering, and integration, the activity can be more difficult to detect due to the anonymous nature of cryptocurrencies. Moreover, while traditional schemes such as smurfing or gambling at a casino are still used as laundering techniques, more advanced methods such using mixers and tumblers or utilizing unscrupulous cryptocurrency exchanges are also being used to mask the flow of funds. Finally, the rapid increase in initial coin offerings (ICO's) provides yet another outlet for cryptocurrency money laundering to occur.

Fortunately, advancements are being made on a variety of fronts to address the increase in illicit activity. First, the largest cryptocurrency exchange, Coinbase, has implemented a robust know-your-customer (KYC) program, as evidenced by my own experience of opening an account with the exchange. Secondly, researchers are finding new ways to extract information about certain cryptocurrency transactions which were previously thought to be unidentifiable. Finally, both law enforcement and government agencies, including the SEC and the Financial Crimes Enforcement Network, are using innovative, aggressive, and even clandestine techniques to combat cryptocurrency money laundering activity.

Introduction

According to the Coin Market Cap website, as of October 2018, there are more than 2,000 cryptocurrencies in circulation with a combined value of more than $209 billion (Top 100 Cryptocurrencies by Market Capitalization, 2018). While bitcoin, Ethereum, and Ripple are certainly the most familiar coins, all of the cryptocurrencies in circulation are susceptible to money laundering. Moreover, the activity appears to be increasing at an alarming rate. Per an article from The American Banker, in 2017, $266 million was laundered through cryptocurrencies. However, in just the first half of 2018, the number has already risen to a staggering $761 million (Crosman, 2018). Therefore, in order to successfully identify and prevent money laundering through cryptocurrencies, it is imperative to understand the money laundering process, understand how cryptocurrencies can be used to launder money, and what actions are currently being taken to address the illicit activity.

The Difference Between bitcoin and Bitcoin

Since its inception, the world's first cryptocurrency has been identified in writing as both "bitcoin" and "Bitcoin." According to the BTCNN website, while both variations are acceptable, the consensus among the cryptocurrency community is that there *is* a distinction between the two. Bitcoin with a capital "B" refers to the infrastructure and the payment network, while bitcoin with a lowercase "b" refers to the cryptocurrency itself (BTCNN, n.d.). Therefore, for the purpose of consistency and clarification, for the remainder of the paper, all of the references to bitcoin will pertain to the cryptocurrency, and not the network associated with Bitcoin.

Defining Cryptocurrencies

Before understanding how cryptocurrencies can be used to facilitate money laundering, it is important to first understand what a cryptocurrency actually is. Merriam-Webster defines cryptocurrencies as "any form of currency that only exists digitally, that usually has no central issuing or regulating authority but instead uses a decentralized system to record transactions" (Merriam-Webster, 2018, par. 1). Currently, cryptocurrencies are not issued by any governing body, and in the United States, are not considered to be legal tender (Rooney, 2018). This means "there are no protections for either the consumer or the merchant, and that its use as payment is completely discretionary" (Acheson, 2018, par. 3).

A Brief History of Bitcoin

Bitcoin was first introduced in 2009 by Satoshi Nakamoto, but many people believe the name is a pseudonym (Harvey, 2014). Consequently, in the years since bitcoin was introduced, there has been a significant amount of speculation as to the true identity or identities of the developer(s), but "the identity of 'Satoshi' is a mystery yet to be solved" (Khatwani, 2018, par. 15).

Bitcoin was introduced to the world after the 2008 financial crisis, and was intended to be an alternative form of currency which would be free from corporate involvement and government regulation (Kharif, 2018). Individuals who possessed bitcoins could use the currency freely, without restriction, and could move money around the world without the need of

a financial intermediary. In fact, the first recorded bitcoin transaction was between two individuals on different continents.

According to an article from Slate, in an online forum, a Florida man offered 10,000 bitcoins in exchange for a pizza. (At the time, bitcoin had a significantly lower value than what it does today). An individual in the United Kingdom accepted the offer and arranged for two Papa John's pizzas to be delivered to the bitcoin trader back in Florida (Griswold, 2014). However, as innocuous as the transaction was, it would not be long before the anonymous and unregulated nature surrounding bitcoin was exploited for more nefarious purposes.

Silk Road

Between 2011-2013, an online marketplace called Silk Road operated on the dark web, allowing individuals who were able to access the site the ability to buy and sell a plethora of illegal goods with impunity. In fact, while the site was in operation, it is estimated that more than 100,000 users bought and sold more than $200 million worth of contraband including drugs, fake ID's, and pornography (Ramey, 2018). The only stipulation was that all purchases had to be made in bitcoin (Santori, 2017).

After an extensive investigation, the website was taken down by the FBI, and the site administrator, Ross Ulbricht, was arrested on charges of money laundering and narcotics trafficking. In addition, the Department of Justice seized approximately $3.5 to $4 million in bitcoin (Greenberg, 2013). While the big story was obviously that illegal products were being bought and sold online without consequence, it was now abundantly clear that bitcoin could be

used to facilitate illicit activity, and therefore could no longer be viewed as an innocent novelty item.

Cryptocurrencies Today

When the Silk Road website was in operation, bitcoin was the only cryptocurrency in circulation. Since then, thousands of additional cryptocurrencies have been introduced. While technically all non-bitcoin cryptocurrencies are deemed "altcoins," an additional clarification should be made as some cryptocurrencies are certainly more common than others (What is an Altcoin?, 2018). Per the Coin Market Cap website, bitcoin, Ethereum, and Ripple are the three cryptocurrencies with the greatest value, ostensibly making them the most recognizable, transferrable, and arguably, legitimate. Additionally, as a result of the research conducted for this paper, the term "altcoin" is also used to describe coins with a smaller market value (What is an Altcoin?, 2018). Therefore, for the purpose of this paper, widely recognized coins such as bitcoin, Ethereum and Ripple are referred to as primary coins, while lesser known coins are referred to as altcoins, as some cryptocurrencies appear to exist only for the purpose of assisting criminals engage in questionable or illegal activity.

Why Cryptocurrencies Are Susceptible to Money Laundering Activity

There are several reasons why cryptocurrencies are used to facilitate money laundering, but the predominant reason is anonymity. Individuals and criminal organizations can mask their true identities by using different aliases and pseudonyms, essentially allowing transactions to be conducted anonymously. Moreover, cryptocurrencies do not have to move through a regulated bank or even a third party. Instead, money can be moved freely and independently without

having the purpose or legitimacy of the transactions verified (Kelly, 2017). While transactions may be recorded on a blockchain, and the ledger is publicly available, the information can be of limited use to law enforcement without knowing the true identities of the transacting parties. As a result, it is no surprise that the FBI spends "approximately 75 percent of its financial crime-related man-hours investigating digital currency" (Fruth, 2018, par. 36).

Another reason why cryptocurrencies are susceptible to money laundering is the industry is not universally regulated, resulting in an unreliable level of the reporting of suspicious activity. After all, banks and money service businesses ("MSB's") such as Western Union have large compliance departments whose sole function is to follow the trace of money as it passes through their organizations. Sophisticated software programs are used to flag transactions which appear to be atypical or unusual, and an anti-money laundering investigator is tasked with reviewing the transactions to determine the legitimacy of the activity. During this process, efforts are made to identify the parties involved, the source of the funds, the purpose of the activity, and if the transactions are reasonable or have a discernable purpose. Then, if the activity cannot be reasonably understood, the information is reported to the Financial Crimes Enforcement Network (FinCen) through a Suspicious Activity Report (SAR).

However, cryptocurrencies are not issued by financial institutions and are therefore not subject to the same regulations. Individuals can exchange cryptocurrencies freely without the need of a financial intermediary, while cryptocurrency exchanges can also be used to facilitate money laundering activity. Exchanges are essentially trading platforms where cryptocurrencies can be legitimately bought or sold, allowing both traditional monies to be converted into cryptocurrencies, or vice versa, and allowing one cryptocurrency to be exchanged for another (Goodboy, 2018). It is important to note that while some exchanges have anti-money laundering

protocols in place, there are still weaknesses which can be exploited. After all, even the largest and most heavily regulated financial institutions are susceptible to money laundering activity. Just because these institutions have compliance departments and employ anti-money laundering investigators does not mean that money laundering activity does not continue to occur.

Another reason why cryptocurrencies are susceptible to money laundering is because some coins, dubbed privacy coins, are specifically designed to mask a user's information as well as the pertinent details linked to a transaction. Per an article from Nasdaq, "These cryptocurrencies are still public in the sense that they have public open ledgers, but transaction information is obfuscated in varying degrees to protect the privacy of the end users" (Etto, 2017, par. 8). As a result, privacy coins such as Monero and Zcash provide an additional layer of anonymity which can benefit criminals, while also hindering law enforcement.

According to the article, Monero "makes it difficult to trace the parties involved in a transaction because transaction signatures are shared by a large group of people; as a result, associating specific users with a transaction is very difficult." Meanwhile, Zcash operates slightly different, in that privacy is awarded as a result of the transaction history being "erased" after the transaction has occurred (Etto, 2017, par. 9).

It is important to note that while privacy coins can appear to be unreasonably favorable to money launderers, privacy coins were not developed with the intention of manipulating twenty-first century technology to modernize an age-old crime. Instead, privacy coins were designed to offer an additional layer of privacy, security, and anonymity to individuals in the digital age. In fact, according to one Monero developer, "Most people use it legitimately--they just don't want others to know whether they're buying a coffee or a car" (Kharif, 2018, par. 13). Unfortunately, like most technological developments, the inventors may have had the best intentions, but some

individuals will always find a way to use the technology for nefarious purposes. Although, privacy coins like Monero and Zcash have gained the attention of law enforcement, including the U.S. Secret Service (Malwa, 2018).

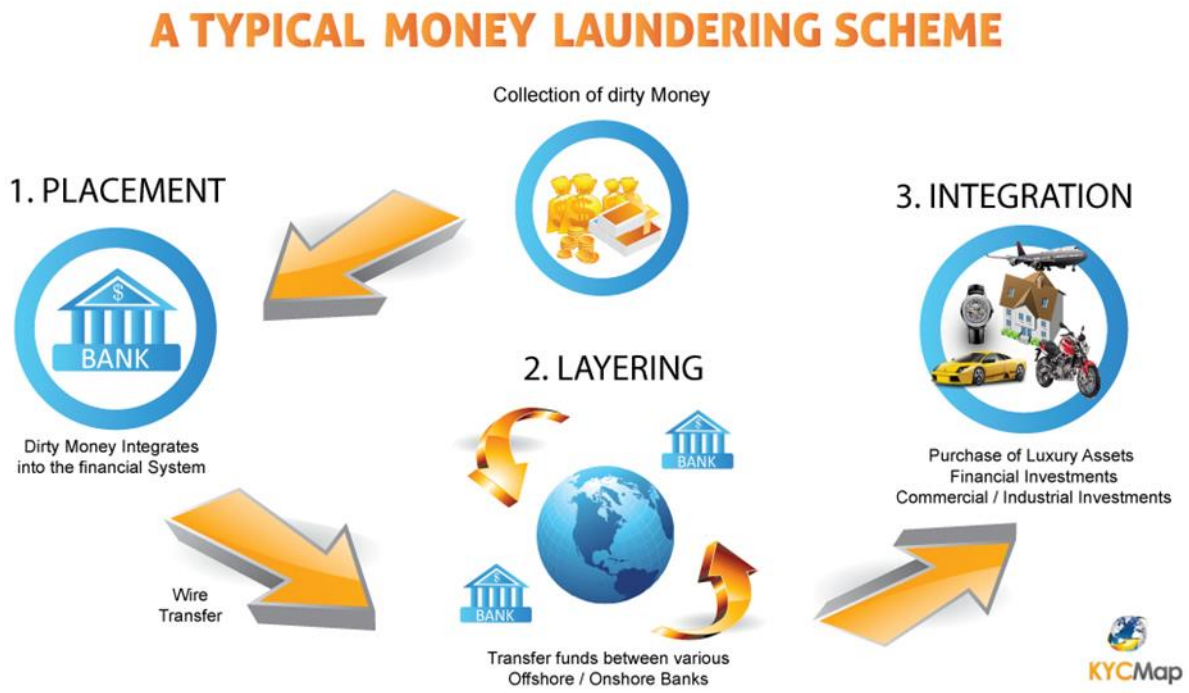
Which brings us to the next reason cryptocurrencies are increasingly susceptible to money laundering: inconsistent global regulation? According to an article titled Cryptocurrencies & the Challenge of Global Governance, "The anonymity and lack of regulations associated with cryptocurrencies have raised serious concerns that they facilitate money laundering, tax evasion, drug traffic and other forms of criminal activity" (Jacobs, 2018, p. 112).

When bitcoin was first introduced, the intention was not to provide a new vehicle for money laundering, but to be able to conduct a transaction without restriction or limitation. Now, nearly ten years later, while cryptocurrencies are still a relatively new concept, laws addressing cryptocurrency activity have not been keeping pace. While there is a global consensus as to the heightened risk of money laundering through cryptocurrency use, and some countries have passed laws to address the concern, there is no global standard in place.

For example, in the United States, bitcoin is not considered to be legal tender, and the legality of exchanges depends on the individual state. In Japan, cryptocurrencies are deemed legal tender, and exchanges are legal if they are registered with the Japanese Financial Services Agency. In China, bitcoin trading is illegal, while India is reportedly working to outlaw bitcoin altogether (Rooney, 2018).

How the Cryptocurrency Money Laundering Process Works

There are three distinct stages to the traditional money laundering process: placement, layering, and integration. In the placement stage, where cash is traditionally the currency being laundered, the dirty money which was generated from illicit means is first introduced into the financial system. While this can be done in a number of ways, it is also the stage where the launderer is the "most vulnerable to being caught," as depositing large amounts of cash can raise suspicions (Money Laundering: A Three Stage Process, n.d.). During the layering phase, the money is moved between accounts, products, financial institutions, and even to different countries and currencies, making it difficult to trace the money back to its original source. Finally, in the integration stage, the cleaned, "laundered" money is returned to the criminal with the funds now appearing to have been legitimately earned. The multi-stage process is also depicted in the KYC Map chart below:



To better understand the challenge of identifying money laundering activity, imagine if a person who owns a cash-intensive business regularly deposits large sums of cash into their account, which is held at Bank A. That same person also funnels the profits of their narcotics sales through their cash-intensive business, which also gets deposited into the same bank account. As long as the business owner/drug dealer does not make any obvious mistakes, such as depositing the exact same amount of money every few days, the activity may appear normal and difficult for the bank to detect as unusual. After all, who is the bank to determine how many people paid for their purchases in cash as opposed to using a debit or credit card?

Then, the owner of the account held at Bank A initiates a transfer to an account held at Bank B, which is then moved again to an account at Bank C. The owner of the account held at Bank C then withdraws the money in cash. At this stage, Bank C does not know the money

originated from an account at Bank A, or that the source of funds for the withdrawal was a cash deposit consisting of a mix of legitimate business profit and illicit drug sales. Without conducting further research, Bank C only knows that the money was an electronic transfer from Bank B. Therefore, if neither Bank A, B, or C consider the activity to be suspicious, it will be increasingly unlikely that law enforcement is alerted to the suspicious activity.

It is important to note that this is an oversimplified example which intentionally fails to take into consideration all of the safeguards that Banks A, B, and C have in place. The intention is merely to illustrate how the laundering process can work and how it can be difficult to identify money laundering activity. Now, with cryptocurrencies being added as an alternative means of moving money, the laundering process can be even more difficult to detect.

Consider the same fictitious business owner who is still laundering drug proceeds through his cash-intensive business. Like many money launderers, the business owner wants to keep altering the ways in which the money is laundered to avoid detection or attracting any unwanted scrutiny into the business. Therefore, the business owner/criminal starts making investments in cryptocurrencies, an innovative way to clean the dirty money.

According to an article found on Reuters, and written by the director of an anti-money laundering advisory service, the same three-stage laundering process applies to cryptocurrencies, but the intricacies associated with each stage are inherently different. For example, in the placement stage, funds are moved from a traditional bank to an account with a cryptocurrency exchange service in order to purchase primary coins such as bitcoin or Ethereum. Then, in the layering phase, the primary coins are exchanged for altcoins in an attempt to muddy the electronic paper trail, ostensibly making it harder for law enforcement to follow the trail of money. This process is also known as chain hopping (Kelly, 2017). Then, in the integration

stage, the launderer can exchange the altcoins back to primary coins, which can then be exchanged again for traditional money (Fruth, 2018).

While the description is again overly-simplified and the timeframe condensed, the description accurately depicts a well-devised scheme that skirts many of the red flags anti-money laundering investigators would look for. After all, cryptocurrencies have been viewed as a unique and lucrative investment opportunity, and it is not unreasonable to see more individuals starting to invest in cryptocurrencies. As a result, identifying placement activity or recognizing a suspicious transaction initiated through a cryptocurrency exchange can be difficult to detect.

This is especially true if cryptocurrency exchanges which onboard new clients have insufficient know-your-customer protocols. If the exchange service does not keep adequate records on their clients or make a reasonable attempt at verifying the information, then law enforcement does not have adequate recourse for investigating any suspicious activity. Unfortunately, that is exactly what is happening with certain cryptocurrency exchanges. Per an article in the Wall Street Journal, "tech-savvy criminals are increasingly opening accounts with fake names at overseas exchanges that don't comply with U.S. laws." In fact, according to a former U.S. attorney with the Justice Department, "Even though investigators can follow the funds by analyzing the blockchain, they may not be able to connect those funds to a culprit in the real world. We have received 'Mickey Mouse' who resides at '123 Main Street' in subpoena returns" (Ramey, 2018, par. 38).

Money Laundering Schemes

It is important to remember that money laundering has been occurring long before cryptocurrencies had been created. There are a myriad of schemes that criminals will employ to evade scrutiny and elude law enforcement, and some of the most basic schemes are still being used today. For example, earlier this year, a British man was arrested in the Netherlands for laundering cryptocurrencies through his own bank account. The scheme was very simple in that the launderer would accept bitcoins from criminals, and then use his own bank account to exchange the cryptocurrency for cash. Once converted, the money was withdrawn from the account and returned to the criminals, minus an obvious fee. The scheme occurred between 2014-2016, and roughly 11.5 million euros were laundered through the account (Pieters, 2018).

Another common scheme is smurfing, which is the process of utilizing several individuals to conduct transactions on behalf of, and for the ultimate benefit of the primary money launderer. The logic behind smurfing is that several people making small transactions at different locations is going to be far less suspicious and draw less attention than one person making an individual transaction for a significant amount of money.

Smurfing is certainly not a new scheme, but it has become a global problem due to the ease and speed in which cryptocurrencies can be moved across town or across the globe. One such scheme was uncovered as the result of a joint investigation between Europol, the Spanish Guardia Civil, authorities in Finland, and the U.S. Department of Homeland Security. The investigation identified a complex global smurfing scheme which resulted in the arrest of 11 people and the confiscation of $8 million euro (Europol, 2018).

The scheme originally started with criminals who were located in Spain and were tasked with collecting and dividing the proceeds from illegal drug trafficking into 174 different bank accounts. The criminals then travelled to Colombia and withdrew the cash from the accounts

using bank cards which were linked to the accounts. However, once the criminals realized their actions could easily be tracked by their transaction history, the scheme was modified to laundering bitcoin and other cryptocurrencies instead of cash (Europol, 2018).

Instead of withdrawing the cash in person, through the accounts where the dirty money was deposited, the criminals "used the exchange to convert their illicit proceeds into bitcoins, then change the cryptocurrency into Colombian pesos and deposit it into Colombian bank accounts on the same day." The scheme had ultimately unraveled once authorities discovered where the cryptocurrency exchange was located and gathered all of the personally identifying information the exchange had on the suspects (Europol, 2018, par. 4).

Laundering Cryptocurrencies Through Online Casinos

Another common method for laundering money is through gambling at a casino. In theory, a criminal could buy chips at a casino with their ill-gotten money, play a few rounds of a table game, such as blackjack or poker, and then cash out the chips for clean money from the casino. If the person loses money in the process, it is generally accepted that that is the cost of doing business. Naturally, however, if the launderer wins, the money is still cleaned, and an unexpected profit is made. While casinos certainly have a number of safeguards in place to monitor and prevent this type of activity from occurring, it can be much harder to monitor the activity in an offshore, online casino.

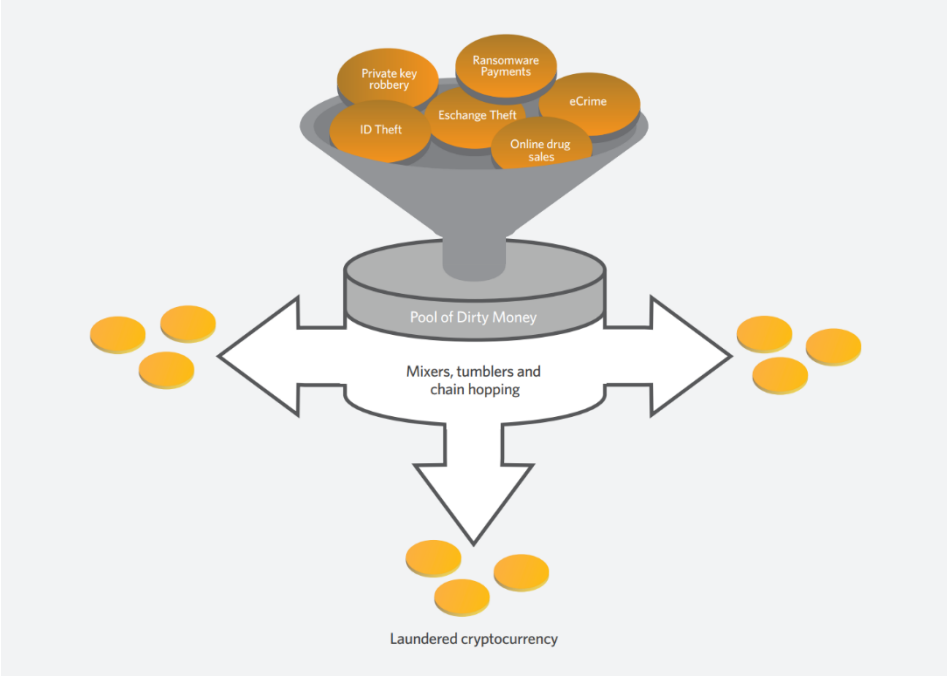
According to a 2018 anti-money laundering report by the cryptocurrency security firm CipherTrace, there are between 100-200 gambling sites on the Internet which allow gambling through cryptocurrencies (Cryptocurrency Anti-Money Laundering Report, 2018). Just like in a

regular casino, funds can be transferred to an online casino for betting purposes, but can presumably also be withdrawn without a minimum number of bets placed or a minimum amount of money spent. Per the report, the primary challenge with monitoring money laundering through online casinos is "because these gambling sites have little to no 'Know Your Customer' (KYC) regulation, it is difficult for law enforcement to obtain information about the transfers into and out of these services" (Cryptocurrency Anti-Money Laundering Report, 2018, p. 9).

A simple Internet search of cryptocurrency gambling websites yields a number of results, with one site in particular, https://bitcoinplay.net advertising different sites one can use to gamble. Moreover, the website promotes anonymity, potentially allowing for the websites to be exploited for money laundering activity.

Mixing and Tumbling

While many of the examples addressed so far identified modernized versions of traditional money laundering schemes, new technologies are also being used to launder cryptocurrencies and make dirty money appear clean. One of the most devious methods is a process called "mixing," which is also referred to as "tumbling." The concept is similar to that of a mutual fund in which disparate individuals can collectively pool their funds for the ultimate benefit of the group. However, instead of investing, the pooled money is moved between exchanges, ultimately making it extremely difficult to follow the trail of specific transactions (Cryptocurrency Anti-Money Laundering Report, 2018). An image from the CipherTrace report depicting the mixing process is shown below:



Initial Coin Offerings

While several schemes have been reviewed so far, perhaps the most pervasive outlet for cryptocurrency money laundering has resulted from the meteoric rise of the Initial Coin Offering, more commonly known as the "ICO." An ICO should not be mistaken for an IPO, or an initial public offering, as individuals are not buying a stake in an established company with the *intention* of receiving a recurring return on their investment. Instead, through an ICO, investors are "purchasing a virtual product offered by the company with the *hope* that it will materialize and appreciate in value" (Underhill, 2018, par. 3).

Some ICO's are certainly legitimate in nature and can be a lucrative investment opportunity. For example, Ethereum released an ICO in 2014 and raised over $18 million

dollars (Marshall, 2017). Today, Ethereum is the second largest cryptocurrency, based on market value (Top 100 Cryptocurrencies by Market Capitalization, 2018). However, Jordan Belfort, better known as "The Wolf of Wall Street," has also warned that ICO's are "the biggest scam ever" (Meyer, 2017, par. 2). While Jordan Belfort may have been alluding to the multitude of fraud schemes related to ICO's, including pump and dump and Ponzi schemes, ICO's are also especially susceptible to money laundering.

For starters, just like purchasing or exchanging cryptocurrencies, investing in an ICO can be an anonymous transaction as both the issuer and the purchaser can shield their true identities through fictitious names. Moreover, while the record of the transaction may be recorded in a public ledger, "there are now hundreds of blockchains on which criminals could transact. Concurrently, there's been a proliferation of exchanges that may be less inclined to cooperate with authorities" (Choudhury, 2017, par. 16).

A second concern for money laundering is the amount of money which can be raised through an ICO. In 2017, more than $5 billion was generated through ICO's. Yet in just the first quarter of 2018, more than $6 billion was raised (Floyd, 2018). While certainly *some* portion of the investments will be financially rewarding, according to a study published by the ICO advisory firm Satis Group, almost 80 percent of the ICO's offered in 2017 turned out to be scams (Morse, 2018). As a result, it is not unlikely that ICO's can be used as a vehicle to launder dirty money.

In fact, according to a hypothetical scenario described in an article from CNBC, the process can be alarmingly simple. In the scenario, an individual who previously decided to invest in an ICO ultimately decides to sell their coins. The seller has two choices: sell the coins on a major exchange, but for a lower return on their investment, or use a "fly-by-night" service

with potentially better rates. The major exchange may not be the most lucrative choice, but they maintain a sophisticated KYC program which will capture all of the pertinent information about both the buyer and the seller. However, that costs money to build and maintain, and it is of little interest to the seller, who simply wants to get the best deal possible (Choudhury, 2017). After all, most savers choose to open an account with the bank offering the best APR as opposed to the one promising to retain their clients' information for the benefit of law enforcement.

Meanwhile, a buyer is looking to launder money that was illegitimately earned, and is willing to pay a premium on an exchange where the pertinent transaction information is not captured and recorded. (Moreover, the buyer is willing to pay more for the coins as it is a recognized cost of doing business.) In the end, the buyer has clean money in the form of coins purchased from an ICO, which can then be exchanged again for another cryptocurrency, or converted again into cash (Choudhury, 2017).

While the seller may have been an honest and law-abiding citizen, it is unlikely that they would be concerned about the identity of the buyer or the source of funds used to purchase the coins. In fact, if there was any concern at all, the seller would likely assume that the exchange would be responsible for doing their due diligence and properly identify their own clients. Conversely, the buyer gets away with exploiting the fact that ICO's are a new and under-regulated investment, and takes advantage of both a potentially unscrupulous exchange and an unsuspecting seller to launder their dirty money.

Solutions and Safeguards

Money laundering is a global problem, and cryptocurrencies have certainly made the issue more complex. While a number of different methods and schemes have been addressed, there are fortunately several innovative and effective solutions being developed which can help detect and deter money laundering through cryptocurrencies.

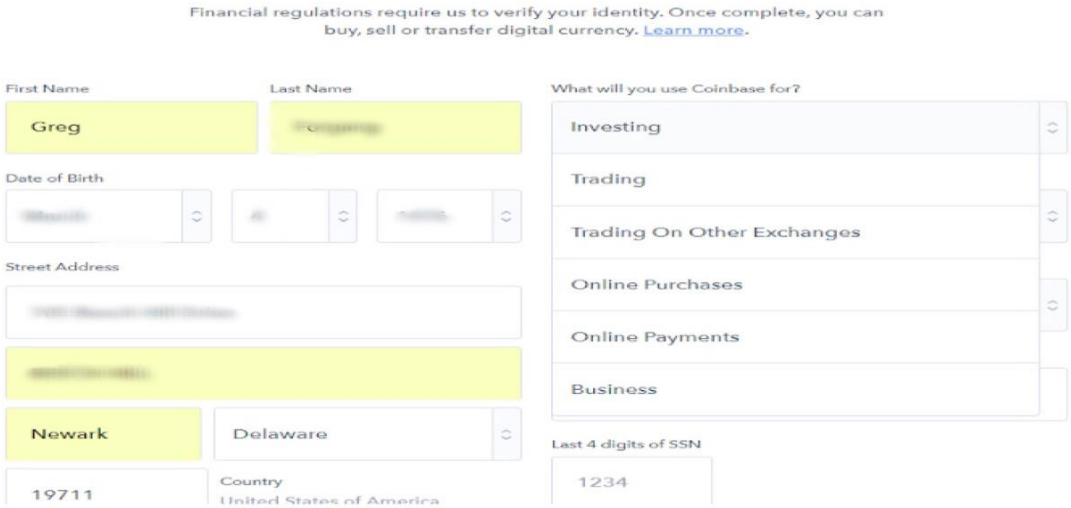
Improved KYC Through Exchanges

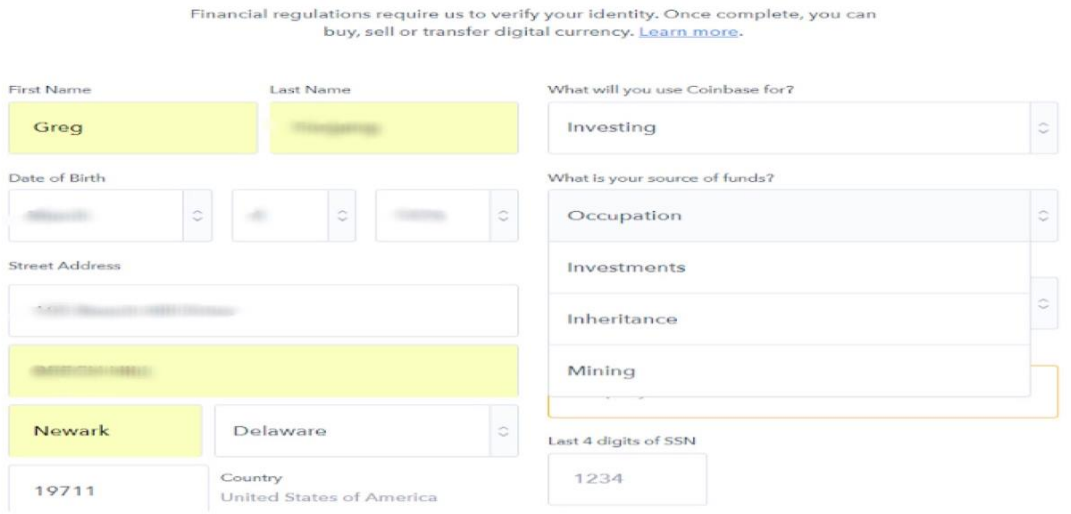
As previously addressed, according to Dan Fruth, the director of the anti-money laundering advisory service Matrix-IFS, cryptocurrencies are often converted to primary coins such as bitcoin, Ethereum or Ripple at least once during the laundering process. Therefore, as cryptocurrency exchanges are the primary facilitators for processing transactions involving primary coins, they are also the best suited to monitor the transactions and report any suspicious activity.

According to an article from Nasdaq, the cryptocurrency exchange Coinbase, is the largest exchange with more than 10 million registered users (Goodboy, 2018). Therefore, to see how thorough (and effective) their KYC program actually was, I decided to open account for myself. The account opening process was very simple and it only took a matter of minutes. But, in that time, I had to provide my name, my mailing address, an e-mail address, and a phone number. Then, both the e-mail and phone number had to be verified by separate confirmation messages. While none of that was any different from opening any other type of online account, the questions became more specific as I continued the enrollment process.

Before I could open an account, I had to advise how I intended to use my Coinbase account, specifying whether it would be used for investing, trading, trading with other exchanges, online purchases, online payments, or business. Then, I had to state where the money

being used on Coinbase was coming from. The options naturally included occupation, investments, or inheritance, but surprisingly included mining. Finally, I also had to provide my occupation, employer, and the last four digits of my social security number. A snapshot of the enrollment process was captured in the images below:





Unlike applying for a credit card or opening an account at a brick-and-mortar bank, I did not have go through an approval process, and my account appeared to be available for immediate use. However, it was not immediately clear if the account *would* have been declined if I had tried using a fake name, dummy address, or any other form of invalid identification. It should also be noted that I did not purchase any cryptocurrencies, which may have required additional verification.

While Coinbase was identified as one of the largest exchanges, it is obviously just one of many. For privacy enthusiasts seeking greater anonymity, there are exchanges that do not appear to gather and record pertinent information on their clients. In fact, a quick Internet search of cryptocurrency exchanges without KYC identified one article titled "7 Altcoin Exchanges to Start Trading on Without KYC & AML" (Khatwani, 2018). While the article went on to identify different exchanges one could use to buy and sell coins, thanks to recent groundbreaking research, individuals who wish to conduct transactions anonymously, for nefarious purposes, could find that their actions will not remain anonymous forever.

Uncovering the Path of Privacy Coins

Privacy coins such as Monero and Zcash were designed to provide a certain level of anonymity to the user in the same manner one receives when using cash. Not surprisingly, it was

only a matter of time before criminals realized that the coins could be exploited for more illicit purposes, including money laundering. However, that may soon be coming to an end. According to a January 2018 article from the Independent, researchers from Princeton University have "developed a tool that helps them analyze Zcash transactions at least to some extent" (Kharif, 2018, par. 12).

Additionally, according to a March 2018 article from *Wired* magazine, researchers from several universities, including Princeton, had collaborated on a project to review Monero. It turns out that due to flaws in the code, individual Monero transactions which occurred prior to February 2017 could be individually extracted. Moreover, even after the code was modified, the level of privacy may be reduced. According to one researcher, "The mental model that people have today for Monero is a simplistic one, that these transactions are private. That model is just incorrect" (Greenberg, 2018, par. 4).

As referenced in the article, any transactions prior to February 2017 which may have been used to facilitate any illegal activity, including money laundering, can now be scrutinized. Not only is this disconcerting for money launderers, but it is a boon for law enforcement. As a result of the research, privacy coin transactions can presumably be analyzed to identify patterns, link individuals to specific activity, and serve as evidence which can be used in court to prosecute money laundering activity.

Howey Coins and the SEC

While the SEC is still determining how to best regulate ICO's, they have taken a unique approach to warning investors of possible scam ICO's. The new approach could have a direct

impact on the aggregate amount of money raised through ICO's, potentially reducing the aggregate amount of money which would eventually need to be laundered.

According to a May 2018 press release from the SEC, a mock sale of Howey Coins was launched to promote an investment opportunity in the travel industry (U.S. Securities and Exchange Commission, 2018). However, despite the impeccably designed web page and the fact that a white paper is available for review, neither the coins nor the coin offering is real. In fact, the page exists solely to educate investors on the risks of investing in fraudulent ICO's.

Individuals who visit the website www.Howeycoins.com are shown a picturesque image of a luxury travel destination with a message declaring the "Pre-ICO sale is live." Additionally, to spur investors to act, a limited time 15% bonus offer is prominently displayed, while a countdown clock advises the potential investor of the limited amount of time remaining on the offer. However, upon clicking on the "token sale" tab, and selecting the "level" of investor one chooses to be, the visitor is immediately taken to a page which explains that the ICO offer is not real. The page then goes on to describe a series of red flags which can help potential investors better identify fraudulent ICO's.

While the Howey Coin website serves multiple purposes, it can be a particularly effective money laundering deterrent as it can advise individuals on how to recognize fraudulent coins, and hopefully make a person think twice before investing. Furthermore, assuming individuals learn about the risks of ICO's through the Howey Coins website, the mock sale could eventually reduce the number of fraudulent and dirty coins available on exchanges.

How Law Enforcement Is Combating Money Laundering Through Cryptocurrencies

Money laundering schemes are always evolving, and criminals are constantly changing their methods to avoid detection. Moreover, as certain schemes become increasingly complex, coordinated efforts by law enforcement are needed to effectively combat money laundering activity. In an effort to address the activity, earlier this year, "over sixty financial investigators from the Interpol and Europol organizations of over 30 countries attended a cryptocurrency workshop to discuss measures that can be taken to combat the misuse of cryptocurrencies by criminals" (Ozelli, 2018, par. 2).

Separately, in the United States, the Financial Crimes Enforcement Network has declared that exchanges that do not have appropriate anti-money laundering safeguards will be held accountable for their actions. This also includes offshore exchanges which deal with U.S. customers (Cryptocurrency Anti-Money Laundering Report, 2018). Other agencies are also working to prevent money laundering through cryptocurrencies, but their tactics are more secretive. ICE, the Immigration and Customs Enforcement agency, has confirmed that it employs secret techniques to "infiltrate and exploit peer-to-peer cryptocurrency exchangers who typically launder proceeds by using mixers (Ozelli, 2018, par. 11). Finally, the DEA is also using clandestine methods and shared that they have "ways of tracking currencies such as Monero and Zcash" (Suberg, 2018, par. 6).

Conclusion

Cryptocurrencies are a relatively new innovation, but they have quickly transitioned from a niche market to global commodity. Consequently, cryptocurrencies have been abused in a number of illicit and illegal ways. From buying contraband on Silk Road to using privacy coins

for nefarious purposes, criminals have exploited cryptocurrencies in order to launder millions of dollars through a variety of methods.

While the same three-stage laundering process applies, the anonymity and lack of standard global regulation surrounding cryptocurrencies has provided new opportunities for money laundering to occur. Moreover, ICO's and cryptocurrency exchanges can also be used to move money from one person to another or even from one currency to another.

Fortunately, efforts are being made on several fronts to both address the problem and provide effective solutions. Exchanges are making greater efforts to identify their clients, while researchers are working to unmask transactions which were previously thought to be untraceable. Finally, and perhaps most importantly, law enforcement and other government agencies are modifying and enhancing their methods of identifying and combating money laundering activity through cryptocurrencies.

Bibliography

Acheson, N. (2018, July 5). *Is bitcoin legal?* Retrieved from CoinDesk: https://www.coindesk.com/information/is-bitcoin-legal/

BTCNN. (n.d.). Retrieved from BTCNN: https://www.btcnn.com/why-is-bitcoin-sometimes-spelt-with-an-uppercase-b-and-other-times-spelt-with-a-lowercase-b/

Choudhury, S. R. (2017, August 5). *It's a very good time to be a money launderer, and you can thank cryptocurrencies*. Retrieved from CNBC: https://www.cnbc.com/2017/08/04/icos-may-be-seen-as-securities-by-u-s-and-singapore-regulators.html

Crosman, P. (2018, September 8). Retrieved from American Banker: 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

Cryptocurrency. (n.d.). Retrieved from Merriam-Webster: https://www.merriam-webster.com/dictionary/cryptocurrency

(2018). *Cryptocurrency Anti-Money Laundering Report.* CipherTrace. Retrieved from https://cdn2.hubspot.net/hubfs/4345106/crypto_aml_report_2018q2.pdf?submissionGuid=bdfa787b-da63-4c11-b509-b9d7bc3574ee

Etto, F. (2017, September 22). *Know Your Coins: Public vs. Private Cryptocurrencies*. Retrieved from Nasdaq: https://www.nasdaq.com/article/know-your-coins-public-vs-private-cryptocurrencies-cm849588

Europol. (2018, April 9). *ILLEGAL NETWORK USED CRYPTOCURRENCIES AND CREDIT CARDS TO LAUNDER MORE THAN EUR 8 MILLION FROM DRUG TRAFFICKING*. Europol. [Press Release]. Retrieved from https://www.europol.europa.eu/newsroom/news/illegal-network-used-cryptocurrencies-and-credit-cards-to-launder-more-eur-8-million-drug-trafficking

Floyd, D. (2018, April 19). *$6.3 Billion: 2018 ICO Funding Has Passed 2017's Total*. Retrieved from Coin Desk: https://www.coindesk.com/6-3-billion-2018-ico-funding-already-outpaced-2017/

Fruth, J. (2018, February 14). *'Crypto-cleansing:' strategies to fight digital currency money laundering and sanctions evasion*. Retrieved from Reuters: https://www.reuters.com/article/bc-finreg-aml-cryptocurrency/crypto-cleansing-strategies-to-fight-digital-currency-money-laundering-and-sanctions-evasion-idUSKCN1FX29I

Goodboy, D. (2018, January 8). *The 3 Best Cryptocurrency Exchanges*. Retrieved from Nasdaq: https://www.nasdaq.com/article/the-3-best-cryptocurrency-exchanges-cm902049

Greenberg, A. (2014, January 29). *End Of The Silk Road: FBI Says It's Busted The Web's Biggest Anonymous Drug Black Market*. Retrieved from Forbes: https://www.forbes.com/sites/andygreenberg/2013/10/02/end-of-the-silk-road-fbi-busts-the-webs-biggest-anonymous-drug-black-market/#48ee28075b4f

Greenberg, A. (2018, April 23). *The Dark Web's Favorite Currency Is Less Untraceable Than It Seems*. Retrieved from Wired: https://www.wired.com/story/monero-privacy/

Griswold, A. (2014, May 23). *The First-Ever Bitcoin Purchase Was Remarkably Inglorious*. Retrieved from Slate: https://slate.com/business/2014/05/first-bitcoin-purchase-two-pepperoni-pizzas-from-papa-john-s.html

Harvey, T. (2014, May/June). *Cryptocurrencies opening fraud gates*. Retrieved from Fraud Magazine: http://www.fraud-magazine.com/article.aspx?id=4294982435

Jacobs, G. (2018, May 28). Cryptocurrencies & the Challenge of Global Governance*. *Cadmus, 3*(4), 15. Retrieved from http://cadmusjournal.org/article/volume-3/issue-4/cryptocurrencies-challenge-global-governance

Kelly, J. (2017, May 18). *Bitcoin's murkier rivals line up to displace it as cybercriminals' favourite*. Retrieved from Reuters: https://www.reuters.com/article/cyber-attack-

bitcoin/bitcoins-murkier-rivals-line-up-to-displace-it-as-cybercriminals-favourite-idUSL8N1II1MV

Kharif, O. (2018, August 6). *A Culture War Is Brewing Between Bitcoin's Old and New Money*. Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2018-08-06/a-culture-war-is-brewing-between-bitcoin-s-old-and-new-money?utm_campaign=news&utm_medium=bd&utm_source=applenews

Kharif, O. (2018, January 2). *Bitcoin is being dropped by criminals in favour of privacy coins like monero*. Retrieved from Independent: https://www.independent.co.uk/news/business/analysis-and-features/bitcoin-latest-updates-price-privacy-coins-cryptocurrency-monero-digital-currency-price-a8137901.html

Khatwani, S. (2018, October 13). *7 Altcoin Exchanges To Start Trading On Without KYC & AML*. Retrieved from CoinSutra: https://coinsutra.com/altcoin-exchanges-without-kyc-aml/

Khatwani, S. (2018, October 11). *9 Interesting Bitcoin Facts Every Bitcoin Owner Should Know*. Retrieved from CoinSutra: https://coinsutra.com/bitcoin-facts/

Malwa, S. (2018, July 5). *$1.2 Billion in Cryptocurrency Laundered Through Bitcoin Tumblers, Privacy Coins*. Retrieved from CCN: https://www.ccn.com/1-2-billion-in-cryptocurrency-laundered-through-bitcoin-tumblers-privacy-coins/

Marshall, A. (2018, August 13). *ICO, Explained*. Retrieved from Coin Telegraph: https://cointelegraph.com/explained/ico-explained

Meyer, D. (2017, October 23). *The Wolf of Wall Street Thinks Some ICOs Are 'The Biggest Scam Ever'*. Retrieved from Fortune: http://fortune.com/2017/10/23/jordan-belfort-wolf-wall-street-icos-initial-coin-offerings-scam/

Money Laundering: A Three Stage Process. (n.d.). Retrieved from About Business Crime Solutions, Inc. : https://www.moneylaundering.ca/public/law/3_stages_ML.php

Morse, J. (2018, July 12). *Shocking no one, study finds almost 80 percent of ICOs are scams*. Retrieved from Mashable: https://mashable.com/2018/07/12/majority-ico-scams/#eZDWhjSulqqT

Ozelli, S. (2018, February 20). *Illicit Uses of Cryptocurrency Gaining Attention Around the World: Expert Take*. Retrieved from Coin Telegraph: https://cointelegraph.com/news/illicit-uses-of-cryptocurrency-gaining-attention-around-the-world-expert-take

Pieters, J. (2018, February 22). *BRIT HELD IN BITCOIN LAUNDERING SCHEME COULD GET 5 YEARS IN PRISON*. Retrieved from NLTimes: https://nltimes.nl/2018/02/22/brit-held-bitcoin-laundering-scheme-get-5-years-prison

Ramey, C. (2018, April 26). *The Crypto Crime Wave is Here*. Retrieved from The Wall Street Journal: https://www.wsj.com/articles/the-crypto-crime-wave-is-here-1524753366

Rooney, K. (2018, March 27). *Your complete guide to cyprocurrency regulations around the world and where they are headed*. Retrieved from CNBC: https://www.cnbc.com/2018/03/27/a-complete-guide-to-cyprocurrency-regulations-around-the-world.html

Santori, M. (2017, May 16). *Silk Road Goes Dark: Bitcoin Survives Its Biggest Market's Demise*. Retrieved from Coindesk: https://www.coindesk.com/bitcoin-milestones-silk-road-goes-dark-bitcoin-survives-its-biggest-markets-demise/

Suberg, W. (2018, August 7). *US DEA: Criminal Activity in Cryptocurrency Has Dropped 80 Percent Since 2013*. Retrieved from Coin Telegraph: https://cointelegraph.com/news/us-dea-criminal-activity-in-cryptocurrency-has-dropped-80-percent-since-2013

Top 100 Cryptocurrencies by Market Capitalization. (2018, September 8). Retrieved from Coin Market Cap: https://coinmarketcap.com/

U.S. Securities and Exchange Commission. (2018, May 16). *The SEC Has an Opportunity You Won't Want to Miss: Act Now!* [Press Release]. Retrieved from https://www.sec.gov/news/press-release/2018-88

Underhill, J. (2018, March/April). *Initial Coin Offerings*. Retrieved from Fraud Magazine: http://www.fraud-magazine.com/article.aspx?id=4295000887&Site=ACFEWEB

What is an Altcoin? (2018). Retrieved from CryptoCurrency Facts: https://cryptocurrencyfacts.com/what-is-altcoin/