2023

The Criminal Side of Cryptocurrency

Angelo Kevin Brown
Arkansas State University - Jonesboro, angbrown@astate.edu

Chapter 8
The Criminal Side of Cryptocurrency

Angelo Kevin Brown
Arkansas State University, USA

ABSTRACT

As cryptocurrency (crypto) has become more and more popular, so has crypto-related crime. There has been a lack of academic research on crypto-related crime, but it is becoming more prevalent in the last couple of years. Crypto-related crime became especially significant in the impact it had on victims and the awareness of these crimes in the media and the government in late 2019 and early 2020 as various criminal organizations and criminal opportunities opened up as cryptocurrency became mainstream. The common crimes related to cryptocurrency include fraud, theft, and money laundering. In 2021 estimates of crypto-related crime were estimated to be as high as $14 billion, which is a small fraction of a percent of the cryptocurrency transactions that were around $15.8 trillion in 2021. The purpose of the chapter is to provide a detailed account of the common crypto-related crimes and scams that have occurred and to evaluate the effectiveness of enforcement of these crimes.

INTRODUCTION

As Bitcoin is one of the most popular cryptocurrencies it is also one of the most exploited by criminals (Leuprecht et al., 2022). Cryptocurrencies have various vulnerabilities that allow criminals to exploit them and the people who use them. The enforcement of cryptocurrency fraud and scams has also been limited due to the difficulty in tracking and prosecuting the offenders and the lack of law enforcement expertise and laws related to cryptocurrencies.

DOI: 10.4018/978-1-6684-8368-8.ch008

A major way that blockchains like Bitcoin can be exploited is through one issue known as a transaction malleability problem (De Filippi, 2014). The transaction malleability problem is an aspect of blockchain that opens up a vulnerability to the cryptocurrencies by the alternation of a cryptographic hash, especially the digital signature that identifies a transaction of cryptocurrency. The exploitation can be used to change the ID of a transaction before the transaction has been confirmed and a hacker can trick a computer system into sending multiple transactions through manipulation of the ID. This is considered a top vulnerability of blockchains like Bitcoin (Liu et al., 2017). The issue became known around 2011 by the Bitcoin community. The largest Bitcoin exchange in 2014 was Mt. Gox which was targeted by a transaction malleability, and the company soon lost $100s of millions because of this and later had to close the site down (Rajput et al.,2014).

In 2020 various well-known Twitter accounts were hacked including Apple, Barack Obama, Bill Gates, Elon Musk, Jeff Bezos, Joe Biden, Kanye West, Uber, and over 100 others (Rosengren, 2022). The scammers had hacked the accounts to send posts to the millions of followers to transfer Bitcoin into a wallet and the victims were told that their contribution would be doubled (Anderson & Saleh, 2021). There were around 320 transactions that occurred after the fraudulent posts, and victims sent over $110,000 worth of Bitcoin. Twitter had become aware of the attack and had created a statement a few hours after and stopped the hackers from creating any more messages.

There are many different black markets online on the regular web and on the dark web which often use cryptocurrency transactions (Leuprecht et al., 2022). The crimes that are supported through cryptocurrency exchanges include illegal pornography such as child pornography and revenge porn, illicit drugs, counterfeit pharmaceutical drugs, murder for hire, weapons trafficking, terrorism funding, counterfeit luxury goods, and much more (Han et al., 2020). Funding through cryptocurrency gives law enforcement and intelligence agencies a difficult time investigating and finding out who these people are because of the decentralized and anonymous nature of cryptocurrencies. When criminal organizations that use websites to sell illegal goods online are shut down by law enforcement they often open up again which can have a new name, or can be in a new country, as the ability to run a website anywhere in the world with an internet connection makes it difficult to shut down these criminal organizations.

Crypto Fraud and Scams

Most cryptocurrency frauds are cyber-enabled crimes. These crimes allow the perpetrator to use technology to increase the reach of the offense (McGuire & Dowling, 2013). For example, many of these frauds have been used before the

invention of cryptocurrency like the Ponzi schemes which occurred in the 1920s by Charles Ponzi (Jacobs & Schain, 2011) but criminals can increase anonymity and reach through the use of cryptocurrency (Choi et al., 2022).

Crypto scams have even hit the mainstream media with the story of Gerald "Gerry" Cotton. Cotton was suspected of stealing about $250 million through a cryptocurrency scam and later reportedly died in India. Cotton was the founder of QuadrigaCX, and at the time there was no official bank account as there was no system of managing cryptocurrency. While Cotton was wanted for crimes he was diagnosed with septic shock, perforation, peritonitis, and intestinal obstruction and died a day later on December 9th, 2018 in Jaipur India. At the time of his death, he was supposedly the only person who had the password to the wallet with all the cryptocurrency. There was a lot of controversy over the death and if the death was real, factors that made it suspicious was that he had signed a will just 12 days before his death leaving his entire estate to his wife Jennifer Robertson. The story became a Netflix original documentary called "Trust No One: The Hunt for the Crypto King".

Cryptocurrency fraud had become a serious issue internationally. Many governments started to warn about these scams and have tried to gather data to report on the occurrence. Government agencies that track these crimes have had difficulties as many people do not report these crimes when they are victimized. In the last couple of years, the complexities and rates of these scams have increased. Researchers have identified at least 47 unique types of scams being used (Trozze et al., 2022). Ransomware and pump-and-dump schemes have been some of the most lucrative scams.

Scam Tokens

The creation of scam tokens increased in the last couple of years. In 2022 there was about an average of 350 scam tokens created each day according to Solidus Labs an organization that tracks cryptocurrency tokens, they counted 117,629 scam tokens created in the year, an increase of about 41 percent compared to 2021 (Coghlan, 2022). The scam tokens come from various serious but Build N Build (BNB) Chain and the Ethereum networks have been reported to harbor the most. One of the most common scams related to these tokens was the honeypot, where a token contract does not permit the buyer to resell the token (Agarwal et al., 2022). An infamous example of the honeypot was the Squid Game token.

A pump-and-dump scam involved a fake charity to entice customers called Save the Kids token (Barry, 2021). A pump-and-dump scam has been used for decades but has gotten a new variety with cryptocurrency. Pump and dump in general is a type of securities fraud where the scammers create an artificially inflated price of a stock or in the case of cryptocurrency an inflated token. The scammers give a

false impression of the worth of the asset so that they can sell it at a high price and dump off the asset making the value fall significantly which makes the victims lose money. This has become common in the cryptocurrency market as it is generally an unregulated market compared to traditional investments like stocks and bonds (De Filippi, 2014). There have been various organized pump and dump scams that were organized through social media platforms including Discord, Telegram, Twitter, and Reddit.

The scammers marketed the Save the Kids token as a charity token. The scammers stated that each coin would provide a percentage of the transaction fee to a charity for kids. The token was supported by various well-known Youtubers and influencers including the rapper RiceGum who has had over 10 million subscribers and billions of views. The token used an anti-whaling mechanism to help stop the larger investors from trading a large portion of their tokens. The token originally was said to allow an investor who owned more than .5 percent of the tokens to be defined as a "whale" which meant they could only trade 20 percent of their supply in 24 hours, but this was later changed as the code had been updated allowing for these "whales" to sell all of their tokens without the limitations. Most of the marketing was targeted toward the youth who followed YouTubers. Once the token had crashed after the top holders sold off the majority of their tokens, Binance who supposedly received the donations had stated they had not received any donations from Save the Kids or other altcoins.

Romance scammers have been commonly attempting to gain cryptocurrency through deception. The Federal Trade Commission (FTC) has established that romance scammers have stolen about $139 million in 2021. The amount stolen of cryptocurrency through romance scams was about five times as much as it was just a year before and on average each victim lost about $9,700 (Roth, 2022). The scammers use dating apps like Tinder and social media apps including Facebook and Instagram to target victims to send money to fake profiles (BBC, 2022).

Romance scams are often a type of catfish scam where profiles are made using pictures of people taken from the internet to trick people. The perpetrators often tell the victim that they are in a crisis and need money to get out of their crisis and that they will pay the victim back. An infamous example of a romance scam was the Netflix true crime documentary called the Tindler Swindler, where Shimon Hayut known as Lev Leviev had used Tinder to manipulate women out of money. Hayut has claimed to become a successful and legit businessman after the scams as he started trading in Bitcoin.

Scammers also have attempted to hold private data for ransom in exchange for Bitcoin. In 2020 a Finnish company Vastaamo had its data stolen from hackers. The hackers reportedly stole 40,000 patient files and were holding them for ransom for around $500,000 worth of Bitcoin (40 Bitcoin). The company refused to give

the Bitcoin for ransom and the hackers attempted to extort the individual patients directly (Rosengren, 2022).

Energy Theft and Factories

Cryptocurrencies need electricity to operate. Some criminals engage in electricity theft to mine cryptocurrency. Some large cases of these crimes include the arrest of six Malaysian men in February of 2021 who were accused of stealing about $2 million in electricity for their Bitcoin mining operations. Malaysia has had various crackdowns on cryptocurrency mining schemes and in July 2021 they destroyed a reported 1,069 mining systems that were reportedly stealing electricity. Later in July of 2021, the Ukrainian government found an underground cryptocurrency farm that was illegally stealing electricity for an estimated 259,000$ a month.

Some of the criminals operate in well-organized groups including in fraud factories. Fraud factories are often operated out of Asia including prior operations that have operated in Cambodia, Laos, Thailand, and Myanmar by Chinese gang members. These fraud factories often trick Africans into traveling to Asia and then force them into slavery and into scamming people into purchasing cryptocurrencies. The gang members threatened their hostages in various ways including the threat of selling their organs or forcing them into prostitution.

A fraud factory operation that operated out of Mynamar had used mostly people from Kenya and Uganda and was used to target young victims from African and Western nations. The scams are usually based on fake social media profiles and dating profiles where human-trafficked victims attempt to build trust with people online and scam them into fake romantic relationships where they will ask for cryptocurrency. This scam is also known as pig butchering. After a victim died from an attempted organ harvest the Kenyan government conducted an investigation and was able to rescue 76 human trafficking victims. The operations often are conducted in Myanmar as the Kachin conflict makes the region difficult to get to and difficult to investigate human trafficking and associated crimes.

Money Laundering

Money laundering is when money is gained through illegal means and is made to look like it was gained through legitimate means. Money laundering usually goes through three phases of laundering include placement, layering, and integration. The first step is when illegally obtained currency is introduced into a financial system, next the currency is moved around in several steps to make it difficult to trace, and lastly, It is incorporated further into the legitimate financial system (Bartoletti et al., 2021).

Investment Scams

Investment scams usually advertise high-interest rates for investors. A common investment scam is a Ponzi scheme. In these scams, the returns on investments are paid to the earlier investors by the funds invested by the newer investors. The scam continues until the perpetrator can no longer find new victims, this has been used with people who invest in cryptocurrency. The majority of investors in Ponzi schemes end up losing most of their investment.

There have been many similar Ponzi-like schemes in the crypto market including Bitconnect. Bitconnect operated in various countries including the United Kingdom (UK) and the United States (US) before it was given a cease and desist order by the Texas State Securities Board in 2018 and was soon shut down after Bitconnect had raised over $2.5 billion. Bitconnect had peaked at around $525 before plummeting down below $1. Through a federal investigation, the US Securities and the Federal Exchange Commission (SEC) sued the company and the founder Satish Kumbhani for the scheme that defrauded American investors an estimated $2 billion.

OneCoin another Ponzi scheme and a pyramid scheme was defined as 'one of the biggest scams in history' by the *Times* as the fraud had gained an estimated $4 billion. The part of the company that made it a pyramid scheme was that it did not have an actual product but recruited new people to invest. OneCoin which is a centralized currency had created false databases to simulate transactions that were not registered by a real blockchain. They claimed to be involved in selling educational materials for cryptocurrency trading, which was reported to be plagiarized from other sources according to a lawsuit filed. OneCoin was based in Bulgaria but had been registered in Belize and Dubai. Countries like these especially Belize have been used by Americans as a tax haven as they have less tax liability and are assumed to be less likely to investigate money laundering than the US government. By 2016 various governments were aware that this company was a scam including the Italian Antitru Authority described the company as an "illegal pyramid sales system".

The Chinese government was also involved in the prosecution and enforcement of the OneCoin scam and was able to recover around $267 million. The founder Ruja Ignatova also known as the Cryptoqueen was wanted by US authorities, but she was unable to be found and became a top ten most wanted fugitive by the Federal Bureau of Investigations (FBI) with a $100,000 reward. Other involved parties have been on the run or arrested including her brother Konstantin who was arrested in 2019 and pleaded guilty to money laundering and fraud and faced a maximum of 90 years in prison. Ignatova was born in Bulgaria and immigrated to Germany as a child and had various arrests and crimes related to fraud including a conviction in 2012 that she was involved with her father in illegal business practices. In 2013 she was involved in a multi-level marketing scheme known as BigCoin.

Ponzi scams on cryptocurrencies have been detected by analyzing the transactions made. Machine learning has been used to help identify such scams by looking at previous Ponzi scam datasets and the factors that they have in common which include contracts that distribute the money among financiers, money received only from other financiers, financiers making profits when other investors contribute enough, the later financiers who join the higher their risk of losing their money (Bartoletti et al., 2021).

An initial coin offering (ICO) is a strategy used for crypto to create funds before they are officially put on the market, which is like an Initial Public Offering (IPO) that shares use before they go public. Like IPOs many ICOs are legitimate but criminals exploit these and create fake advertisements and fraudulent currencies. In 2017 it was reported that about 80 percent of ICOs were fraudulent with about $150 million spent on them. A major fraudulent ICO was Pincoin which launched in 2018 and had $660 million raised.

A large scam known as PlusToken began in 2018. The scam operated mostly in China and South Korea. The scam started off offering monthly payments to the user's wallets. The PlusToken had risen in 2019 to be worth over $2 billion before the arrest of the operators who were six Chinese citizens who were arrested in the South Pacific island of Vanuatu. By the end of the investigation over a hundred, different people were arrested according to China's Ministry of Public Security.

Rug Pull

Rug pull scams have been used to scam investors by inviting investors to help invest in a new nonfungible token (NFT) or other coins to pump it up. As the funds increase and the scammers have access to the victims invested the money they leave and take the money. The scammers code the currency so that the investors cannot sell it so they have valueless currency. This scam occurred with the Squidcoin scam which the Squidcoin went from being worth a penny to around $90 and peaked at about $2,856. As the price peaked the money disappeared which led to the token being worthless and the scammers taking around $2.5 million from the victims (Dickens, 2021).

Exchange Scam

In early 2022 an exchange platform called Wormhole had last over $300 million after a cyber attack by crypto scammers. This was one of the largest attacks of the year of cryptocurrency stolen that totaled more than $1 billion in the last year. A common bitcoin investment scheme occurs when fake investment managers claim that they can help manage people's cryptocurrency investments and promise that the investors can make money. The investors make an upfront payment fee to pay the

manager, but the fees are just stolen and the scammers often request more personal information and gain access to the victim's entire crypto assets.

Cryptojacking

Different cryptocurrencies have different levels of security and vulnerabilities. Cryptojacking has been a major form of crypto crime. This type of theft is when a person hijacks a computer to mine cryptocurrency that they do not own. This can be done through various methods including through a website or software like Coinhive. Coinhive was becoming popular in 2017 to mine but was eventually shut down in 2019.

When successful cryptojacking malware is intended for the victim to be unaware they were 'jacked'. The malware can slow down or crash the computer that it is jacking and covertly mining bitcoin or other cryptocurrencies. One large case of cryptojacking occurred with E-Sports Entertainment which was suspected of hijacking around 14,000 computers, another case occurred when Yahoo Europe used an ad that contained malware that infected millions of computers for bitcoin mining.

According to The European Union Agency for Law Enforcement Cooperation (Europol), Bitcoin was used in about 40 percent of illegal transmissions in the European Union (2015 report). This is likely due to more people using cryptocurrency, more scams of cryptocurrency users, and the government becoming more aware of such issues. The cryptocurrency scams do not seem to be slowing down anytime soon.

Exit Scams

Exit scams have been another cryptocurrency fraud. The use of a centralized market escrow permits a market to close and leave with the buyer's cryptocurrency. A notable case of his was with Evolution. The process of exit scams usually happens after the vendors have created a good reputation and have sold enough items to have accumulated a significant amount of escrow funds and then exit before having to compete in the market. Evolution was brought down by Operation Onymous which was a law enforcement operation that was directed by the FBI and Europol.

Onymous also had various other law enforcement agencies to aid in the operation including the Drug Enforcement Agency (DEA), U.S. Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), and The European Union Agency for Criminal Justice Cooperation (Eurojust). This operation brought down hundreds of websites that were involved with crypto-related crimes including the Silk Road 2.0 and seized $1,000,000s in cryptocurrencies and other assets.

Onymous consisted of law enforcement agencies from 17 countries and there were 17 arrests made including a software developer who was infamously known

as Defcon. During the Silk Road 2.0, it was also targeted by hackers and they lost $2.7 million through exploited transaction malleability. Soon after the arrests and seizures are just a couple hours a new Silk Road was activated known as Silk Road 3.0 showing the difficulty in stopping the Silk Road and other illicit markets. Onymous was seen as a success by the agencies involved with DHS stating that they stopped a black-market site that allowed for "murder-for-hire".

The closure of the Silk Road had little if any impact on the illicit drug market. The sales of illegal drugs online had increased as the Silk Road closed. There have been many others who sold drugs online and have inspired a popular Netflix series called *How to Sell Drugs Online (Fast)*, and a Netflix documentary called *Shiny Flakes: The Teenage Drug Lord*. The series is inspired by the true story of Maximilian Schmidt who was arrested and sentenced to seven years in prison. Schmidt had started selling drugs for crypto as a child until his arrest after having sold thousands of pounds of drugs worth $1,000,000s. It is suspected that Schmidt still has over $1,000,000 worth of Bitcoin that law enforcement was unable to seize. This has been a serious issue for authorities when they arrest suspects and get a conviction the cryptocurrencies can be difficult to seize as they would other assets.

With the effort of governmental task forces, the anonymity of cryptocurrency no longer is as strong as it once was. The punishment that some of these criminals received may act as a deterrent for some would-be offenders. Ulbricht who was the creator of the Silk Road was given a double life sentence plus 40 years in prison in February 2015. Once Ulbricht was arrested on August 21st, 2014 and he was given no bail which is usually given to those who are suspected of serious violent or sexual crimes. He was convicted of all charges of money laundering, conspiracy to commit computer hacking, and conspiracy to traffic narcotics. This a severe sentence as the average sentence length for murder in the US in 2016 was 40.6 years, the average for rape/sexual assault was 12.2 years, and for manslaughter was 10.1 years (Kaeble, 2018).

Ransomware

Ransomware has been used to hack victims' computers and to demand money in the form of cryptocurrency to allow the victims to gain access to their computers. The hackers use a type of malware that holds the computer 'hostage' (Musiala et al., 2020). One such way victims get tricked is through an upgrade scam. Crypto software is constantly upgraded and scammers attempt to imitate a legitimate upgrade so that a person will accept a fake upgrade and the scammers can access their crypto and private keys. This occurred when scammers took advantage of the Ethereum merge

Crytpo Loggers are another type of crypto scammer who attempts to steal information about a victim's wallet through a crypto service through the use of

malware. Crypto loggers attempt to get the private key to necessitate a transfer of the funds from a victim's account to theirs.

A SIM-swap scam is a newer scam that has become more common recently. A SIM swap is when a person gets access to a person's SIM card from their phone and uses it to access information from the phone. If a person can successfully Sim-swap then one can often access the crypto wallets and other information to steal the crypto.

Crypto Wallet

Wallets are a way that crypto users can manage their currency. Some scammers have created fraudulent wallet services where they can take a person's entire wallet or take a small percentage at a time. Other fake wallet scammers wait until their wallet exceeds a certain amount and that deposit all the money to another wallet (Bartoletti et al., 2021).

A related scam to the fake wallet is a fake exchange (Horch et al., 2022). This is when a scammer creates a fake exchange to trick people into purchasing cryptocurrencies. The scammers often offer competitive prices and they manipulate users to believe their exchanges are cheap and easy to use.

Impersonation

The impersonation of government officials or celebrities was yet another way criminals have tried to obtain cryptocurrency. This scam was often perpetrated by scammers who were pretending to be federal agents. Other scams would use the image of a celebrity that is well known to use their name to sell a product with cryptocurrency or have people invest in c cryptocurrency.

Some celebrities have been accused of allegedly supporting crypto scams. Such cases include the influencers and boxers Jake and Logan Paul, Mark Cuban, Kim Kardashian, Floyd Mayweather, and many others. The Paul brothers were accused of supporting a pump-and-dump scheme for the token SafeMoon and a class-action lawsuit was filed against the company (Franceschi-Bicchierai, 2022). The Paul brothers are defendants in the case for their role in the scheme. A lawsuit was filed against Kim Kardashian, Floyd Mayweather, and former Boston Celtic Paul Pierce for their promotion and or involvement in the EthereumMax token. These issues related to people promoting scam tokens have led to governments acknowledging that there needs to be more regulation of crypto.

Blackmail

The use of blackmailing has occurred with the demand for cryptocurrency for ransom, especially Bitcoin (Choi et al., 2022). These scams often involve the scammer having hacked or claiming to have hacked the victim's webcam and that they have video of them that they will release unless they get paid through Bitcoin. This type of scam can also fall into sextortion, which is one of the most successful types of crypto scams (Flodmark & Jakum, 2022). A sextortion email that became widespread in 2018 used the threat of releasing videos of the victim performing sexual acts that were recorded through the email. The scammers didn't have any videos but were still able to con people into paying.

Phishing

Phishing has been used to generate cryptocurrency. Phishing is when a scammer sends a fraudulent email, message, or link that is created to manipulate the victim so that they reveal information to the scammer or hack the victim's computer with ransomware to gather personal information. Phishing websites have been used to collect wallet keys, steel passcodes, and more. One such website stole up to $4 million of MIOTA tokens up until it was discovered in 2018. A common way to lure victims is to have a link that brings a person to a fake website, and that allows the scammers to steal account information. The fake websites can make people believe they are on a legitimate website like Amazon, a governmental website, or a bank's website. The famous film producer Seth Green was a victim of this type of scam when his Bored Ape NFTs were stolen (Guadamuz, 2022). Eventually Green was able to get his Bored Apes back but reports indicate he paid $260,000 for the return of the Bored Apes (Hogg, 2022).

Counterfeit Goods

The ability to sell counterfeit luxury goods has been exploited through the transaction of cryptocurrencies (Hemantha, 2022). The counterfeit goods industry is about $1 trillion a year and the amount that is transferred by blockchain peaked in 2021. The scammers have especially exploited the pre-owned luxury goods market which is valued at about $32.6 billion.

Luxury brands have been attempting to fight counterfeiters by using their blockchain technologies. The companies have been testing using a unique identifier for each product so that it can be traced from the raw material to the secondhand market (Tramatm, 2022). This can help provide digital proof to the potential buyer of the product's authenticity through a smart tag system.

A trust tag can give real-time location tracking and update each transaction with a time stamp through each step to provide a layer of trust. Various luxury brands have implemented this technology including Cartier, Christian Dior, Louis Vuitton, and Prada. One system is called Aura which is used by Louis Vuitton, Prada, and other companies it was the first blockchain system platform to track the history and authenticity of luxury goods with the help of Microsoft in assisting the platform (Akhtar, 2021).

ENFORCEMENT

One of the largest seizures of cryptocurrency occurred in 2021 according to the United States Department of Justice (DOJ). In November 2021 law enforcement agents seized over 50,000 Bitcoins that were hidden in the home of James Zhong who was later found guilty of using the Silk Road in acquiring Bitcoin. The Silk Road is a marketplace on the darknet that functions as a marketplace for the black market including the selling of illegal products including weapons, drugs, counterfeit items including currency, stolen credit card information, forged documents like passports, and other illegal goods (Martin, 2014).

The original Silk Road was investigated through the Silk Road Task Force which used various agencies in the US and abroad including the DEA. The task force agencies including a DEA agent (Carl Mark Force) and a Secret Service agent (Shaun Bridges) had attempted to extort the founder of the Silk Road Ross Ulbricht for Bitcoin. The agents had faked the killing of an informant to pressure Ulbricht into giving bitcoins. Force had pleaded guilty to his involvement in money laundering, obstruction of justice, and extortion under the color of official right and was sent to federal prison. Bridges also plead guilty to depositing about $800,000 worth of bitcoins to his account and was also guilty of money laundering of cryptocurrency and was also sent to federal prison.

Darknet users often use cryptocurrency to help with the anonymity of their activities so that they are less likely to be caught (Choi et al., 2022). Bitcoin has been a major cryptocurrency used in these markets. Law enforcement operations have caused serious issues with some of these markets for example the Bloomsfield Market had to close because the operators of the site were arrested by authorities. Bloomsfield was set up by the former Silk Road drug market users and was used to sell illegal drugs and other products.

In 2018 there was growing concern that terror groups including al-Qaeda (the group behind the September 11th, 2001 attacks) were using the Darknet and Bitcoin to fund their organization (Irwin, & Milad, 2016). As terrorist organizations need secrecy to be successful the ability of anonymity and cryptocurrency exchange has

been an important factor to current terrorist groups (Whyte, 2019). It also gives criminal groups protection from being scammed by other criminals because of the financial security that blockchains like bitcoin provide.

Terror groups are known to operate with significant funding from donors. Donors are often at risk of being charged with a crime if they are caught funding terror groups so the higher the perceived risk for a would-be donor the less likely they will donate. Cryptocurrency helps reduce that risk for donors. The challenge terror groups like the Islamic State of Iraq and Syria (ISIS) have are that cryptocurrencies are limited in their usability and acceptability as a currency in the regions that they operate (Abboushi, 2017).

The vendors that terror groups like ISIS interact with often prefer cash as bitcoin and other cryptocurrencies are not practical in most of the middle east. There are other limitations with cryptocurrencies for terror groups and organized crime including the lack of reliability of cryptocurrencies, their constant fluctuation in price, and volume can be limited. Many cryptocurrencies have a low volume which makes the transfer of large amounts expensive and noticeable. As transactions are often posted publicly through blockchain networks they can be identified by law enforcement as suspicious (Dion-Schwarz et al., 2019).

Government agencies have continued to put more resources into stopping cryptocurrency-related crimes. Recently the FBI acknowledged a Crypto Task Force at the Munich Cyber Security Conference on February 17th, 2022. The task force named Virtual Asset Exploitation Unit (VAXU) to better investigate cryptocurrency and to be better able to seize virtual assets. A statement made by the task force helped detail their goals "Ransomware and digital extortion, like many other crimes fueled by cryptocurrency, only work if the bad guys get paid… The currency might be virtual, but the message to companies is concrete: if you report to us, we can follow the money and not only help you but hopefully prevent the next victim."

The United Nations (UN), and international cooperation have used significant efforts in attempting to reduce crypto terrorism financing through the Global Coordinated Programme on Detecting, Preventing and Countering the Financing of Terrorism (CFT Programme) of the United Nations Counter-Terrorism Centre (UNCCT) within the United Nations Office of Counter-Terrorism (UNOCT) and other methods (Dion-Schwarz, et al., 2019). The UN has passed various resolutions with the support of the international community to counter the funding, especially Resolution 2462 (2019). The UN has analyzed terror attacks that are related to crypto funding and the number has significantly increased (Shukla, 2022).

The Financial Action Task Force (FATF) is a multi-agency group that investigates suspected terror group funding (Choo, 2015). This task force has made it a priority to check to ensure that nations are implementing annual anti-money laundering

and anti-terrorist financing laws regarding criminal organizations and specifically terrorism.

In 2015 there were various reports about ISIS using crypto wallets to fund terrorism, ones such claim was from Deutsche Welle who stated they had evidence of a Bitcoin wallet connected to ISIS that was worth $10s of millions. Another report by Ghost Security Group which is an anti-terror group of hacktivists claimed that they found transactions of Bitcoin owned by ISIS operatives. The reported worth of these wallets was estimated to be up to $15 million (Irwin, & Milad, 2016).

Zcash is an important currency regarding terrorism and organized crime as it is a departure compared to traditional cryptocurrencies in regards to the technical infrastructure. Zcash which was launched in 2016 does not allow for transactions to be in the visible blockchain so it has a higher level of privacy. The transactions are viewable to those possessing the view key and the originator because it uses the Zero Knowledge Succient Arguments of Knowledge (ZK-SnARKs). The ability for Zcash to be transferred online can make it very difficult for law enforcement and intelligence agencies to know about the funding of terror groups.

Bitcoin has been a popular way to purchase child pornography. Europol has a cybercrime unit that has helped investigate and arrest people who have been buying illegal material like child pornography. There are at least 30 websites known to exclusively accept Bitcoin for its pornography. There has even been a deep web crowdfund to support a child pornography website (Cook, 2014).

Victims

During the COVID-19 epidemic, there was a significant increase in the use of cryptocurrencies, crypto scams, and victims of scams (Barry, 2021). These included various types of scams the buyer was thought to be buying protective equipment, and donations scams (National Services Scotland, 2020).

Victims of crypto scams are unlikely to get their crypto back after it has been stolen. There is very little crime control in the crypto market, especially in the beginning (Mackenzie, 2022). As this market has been largely unregulated it has been open to manipulation and scams have been normalized with many victims who are ready to invest in speculative opportunities.

The crypto market is prescribed as *responsibilized* where an investor has a loss even when a victim of a crime is to write it off (Mackenzie, 2022). There are various reasons for this but the main factors include the lack of law enforcement dedicated and trained to deal with crypto crimes and the confidentiality of crypto in general (Read, 2022).

The theft of cryptocurrency can happen to a person by a roommate or a person that is on the other side of the planet. Many perpetrators that victimized Americans

are from other countries. US law enforcement agencies will usually not investigate these crimes where the perpetrator is thought to be in another country unless the amount stolen is very high and even then it may not be seriously investigated.

Local law enforcement usually does not have the resources to conduct international investigations so these crimes are usually handled by federal law enforcement such as the FBI (Moggridge & Montasari, 2022). Victims can report to various non-law enforcement agencies. The main agencies that victims of crypto scams report to include the FTC, Securities and SEC, Commodity Futures Trading Commission (CFTC), Internet Crime Complaint Center, and the crypto exchange platform that was used by the victim. Federal and state agencies have tried to educate and warn potential victims about scams and what red flags to look out for.

CONCLUSION

The research and knowledge of cryptocurrency scams are incomplete as there are few public databases about such crimes (Bartoletti et al., 2021). Governments, corporations, and other agencies are constantly trying to fight crypto crime. It seems that the vast majority of crypto crime goes away without any investigation and that this will continue for some time.

The prevention of crypto crime is important. Education is an important factor, as educated investors seem to be significantly less likely to be victimized. Improved reporting systems need to be established so more scams can be reported to authorities and blockchain platforms. Current public data sources on scams related to cryptocurrency are unreliable and incomplete. An improved dataset can help improve scam detection systems. This can help improve resource detection systems for non-technical investors to be warned of potential fraudulent websites and platforms.

REFERENCES

Abboushi, S. (2017). Global Virtual Currency–Brief Overview. *Journal of Applied Business & Economics*, *19*(6).

Agarwal, R., Thapliyal, T., & Shukla, S. (2022). Analyzing malicious activities and detecting adversarial behavior in cryptocurrency based permissionless blockchains: An Ethereum usecase. *Distributed Ledger Technologies: Research and Practice*.

Akhtar, T. (2021). Louis Vuitton, Cartier, Prada to Use Bespoke Blockchain to Tackle Counterfeit Goods. *CoinDesk*. https://www.coindesk.com/business/2021/04/20/louis-vuitton-cartier-prada-to-use- bespoke-blockchain-to-tackle-counterfeit-goods/

Anderson, C., & Saleh, T. (2021). Investigating cyber attacks using domain and DNS data. *Network Security*, *2021*(3), 6–8. doi:10.1016/S1353-4858(21)00028-3

Barry, T. M. (2021). # NotFinancialAdvice: Empowering the Federal Trade Commission to Regulate Cryptocurrency Social Media Influencers. *Ohio St. Bus. LJ*, *16*, 279.

Bartoletti, M., Lande, S., Loddo, A., Pompianu, L., & Serusi, S. (2021). Cryptocurrency scams: Analysis and perspectives. *IEEE Access : Practical Innovations, Open Solutions*, *9*, 148353–148373. doi:10.1109/ACCESS.2021.3123894

BBC. (2022). The Kenyans lured to become unwitting 'love' fraudsters. *BBC*. https://www.bbc.com/news/world-africa-63654637

Choi, J., Kim, J., Song, M., Kim, H., Park, N., Seo, M., & Shin, S. (2022). A Large-Scale Bitcoin Abuse Measurement and Clustering Analysis Utilizing Public Reports. *IEICE Transactions on Information and Systems*, *105*(7), 1296–1307. doi:10.1587/transinf.2021EDP7182

Choo, K. K. R. (2015). Cryptocurrency and virtual currency: Corruption and money laundering/terrorism financing risks? In *Handbook of digital currency* (pp. 283–307). Academic Press. doi:10.1016/B978-0-12-802117-0.00015-1

Coghlan, J. (2022). *350 new 'scam tokens' were created every day this year*. Solidus Labs.

Cook, J. (2014). Paedophiles Have Created A Deep Web Version Of Kickstarter To Crowdfund Child Porn. *Business Insider*. https://www.businessinsider.com/pedophiles-have-created-a-deep-web-version-of-kickstarter-to-crowdfund-child-porn-2014-11

De Filippi, P. (2014). Bitcoin: a regulatory nightmare to a libertarian dream. *Internet Policy Review, 3*(2).

Dickens, S. (2021). Squid Game meme coin crashes by 99.9% after developers pull the plug. *Yahoo!* https://www.yahoo.com/now/squid-game-meme-coin-crashes-131908065.html

Dion-Schwarz, C., Manheim, D., & Johnston, P. B. (2019). *Terrorist use of cryptocurrencies: Technical and organizational barriers and future threats*. Rand Corporation. doi:10.7249/RR3026

Flodmark, A., & Jakum, M. (2022). *Characterizing Bitcoin Spam Emails: An analysis of what makes certain Bitcoin spams generate millions of dollars*. Linköping University.

Franceschi-Bicchierai. (2022). Meet the Blockchain Detectives Who Track Crypto's Hackers and Scammers. *Vice News*. https://www.vice.com/en/article/xgd9zw/meet-the-blockchain-detectives-who-track-cryptos-hackers-and-scammers

Guadamuz, A. (2022). These are not the apes you are looking for. *Communications of the ACM*, *65*(9), 20–22. doi:10.1145/3548761

Han, W., Duong, V., Nguyen, L., & Mier, C. (2020, May). Darknet and bitcoin de-anonymization: Emerging development. In 2020 Zooming Innovation in Consumer Technologies Conference (ZINC) (pp. 222- 226). IEEE.

Hemantha, Y. (2022). Embracing block chain technology in supply chain to combat counterfeiting luxury and fashion brands. *Asian Journal of Management*, *13*(2), 145–150.

Hogg, R. (2022). Seth Green pays $260,000 ransom for a stolen Bored Ape Ethereum NFT meant to feature in his new TV show. *Business Insider*. https://www.businessinsider.com/seth-green-pays-260000-return-stolen-bored-ape-ethereum-nft-2022-6

Horch, A., Schunck, C. H., & Ruff, C. (2022). Adversary Tactics and Techniques specific to Cryptocurrency Scams. *Open Identity Summit 2022*.

Irwin, A. S., & Milad, G. (2016). The use of crypto-currencies in funding violent jihad. *Journal of Money Laundering Control*, *19*(4), 407–425. doi:10.1108/JMLC-01-2016-0003

Jacobs, P., & Schain, L. (2011). The never ending attraction of the Ponzi Scheme. *Journal of Comprehensive Research*, *9*, 40–46.

Kaeble, D. (2018). *Time Served in State Prison, 2016 (NCJ 252205)*. US Department of Justice, Bureau of Justice Statistics.

Leuprecht, C., Jenkins, C., & Hamilton, R. (2022). Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency. *Journal of Financial Crime*.

Liu, Y., Liu, X., Zhang, L., Tang, C., & Kang, H. (2017). An efficient strategy to eliminate malleability of bitcoin transaction. In *2017 4th International Conference on Systems and Informatics (ICSAI)* (pp. 960-964). IEEE.

Mackenzie, S. (2022). Criminology towards the metaverse: Cryptocurrency scams, grey economy and the technosocial. *British Journal of Criminology*, *62*(6), 1537–1552. doi:10.1093/bjc/azab118

Martin, J. (2014). Lost on the Silk Road: Online drug distribution and the 'cryptomarket'. *Criminology & Criminal Justice*, *14*(3), 351–367. doi:10.1177/1748895813505234

McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. Research Report 75.

Moggridge, E., & Montasari, R. (2022). A Critical Analysis of the Dark Web Challenges to Digital Policing. In *Artificial Intelligence and National Security* (pp. 157–167). Springer. doi:10.1007/978-3-031-06709-9_8

Musiala, R. A. Jr, Goody, T. M., Reynolds, V., Tenery, L., McGrath, M., Rowland, C., & Sekhri, S. (2020). *Cryptocurrencies: Forensic techniques to meet the challenge of new fraud and corruption risks | FVS eye on fraud*. AICP.

National Services Scotland. (2020). *NHS counter fraud services rolling COVID-19*. Intelligence alert no. 14. Author.

Rajput, U., Abbas, F., Hussain, R., Eun, H., & Oh, H. (2014, August). A simple yet efficient approach to combat transaction malleability in bitcoin. In *International Workshop on Information Security Applications* (pp. 27-37). Springer.

Read, C. L. (2022). No More Duffel Bags Full of Cash. In *The Bitcoin Dilemma* (pp. 113–119). Palgrave Macmillan. doi:10.1007/978-3-031-09138-4_11

Rosengren, K. (2022). *Contribution of Open-Source Intelligence to Social Engineering Cyberattacks*. Turku University.

Roth, E. (2022). *Romance scammers collected $139 million in crypto last year*. The Verge.

Shukla, S. (2022). UN Says Crypto Use in Terror Financing Likely Soaring. *Bloomberg*. https://www.bloomberg.com/news/articles/2022-10-31/un-finding-more-cases-where-crypto-involved-in-terror-financing

Trama, T. (2022). Brands are introducing new Blockchain Technologies to fight Counterfeit. *Lexology*. https://www.lexology.com/library/detail.aspx?g=a1559142-01a7-400e-97f9-31ef6a853640

Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S. D. (2022). Cryptocurrencies and future financial crime. *Crime Science*, *11*(1), 1–35. doi:10.118640163-021-00163-8 PMID:35013699

Whyte, C. (2019). Cryptoterrorism: Assessing the utility of blockchain technologies for terrorist enterprise. *Studies in Conflict and Terrorism*, 1–24. doi:10.1080/1057610X.2018.1531565