INTERNATIONAL E-JOURNAL OF CRIMINAL SCIENCES
Supported by DMS International Research Centre

Crypto-Assets Illicit Activities: Theoretical Approach with Empirical Review

Ivana Cunjak Matakovič

PhD student, University of Zagreb, Faculty of Economics and Business

Abstract

Transnationality, enabled by global processes and the rapid development of the Internet, has led to the creation of new dynamics of criminal activities, where cyberspace becomes a place, goal and mean of committing criminal activities. The aim of this paper is to present criminal activities related to crypto-assets in a coherent and concise way. The misuse of crypto-assets will be investigated in a systematic way, especially from the perspective of financial fraud and in the context of white-collar crime. The paper will present the characteristics of cryptocurrencies that make them suitable for criminal activities. The empirical analysis will explore the role of cryptocurrencies within traditional criminal activities but also within cyber-dependent crimes. This paper will contribute to the theoretical perspective of crypto-assets abuse and the taxonomy of criminal acts related to crypto-assets.

Key words: crypto-assets, cryptocurrencies, cybercrime, fraud, white-collar crime

[1] E- mail: ivana.cunjak@gmail.com

INTERNATIONAL E-JOURNAL OF CRIMINAL SCIENCES
Supported by OMS International Research Centre

1. Introduction

The innovativeness of cryptocurrencies and distributed ledger technology represents strong potential for the global economy, but without adequate legislation, can be used for criminal activities. Europol points out that the use of virtual currencies in illegal activities has been growing in recent years. Tools that facilitate the use of cryptocurrencies have become widely available, and criminal activities related to cryptocurrencies are well established, so cryptocurrencies are no longer limited to cybercrime but are linked to all types of criminal activities that involve money transfers (Europol, 2021).

Chainalysis in the annual report *The 2022 Crypto Crime Report* states that criminal activities related to cryptocurrencies in 2021 had the strongest increase so far, and legally prohibited payments through addresses amounted to more than $14 billion, which is a significant increase compared to 2020 when those payments amounted to $7.8 billion (Chainalysis, 2022). The question is what is the role of crypto-assets in the implementation of criminal activities?

Before analysing the role of cryptocurrencies in the implementation of criminal activities, it is necessary to understand the basic characteristics that make them attractive to illegal activities. Therefore, this paper is organized as follows: in the second part of the paper, the conceptual definition and basic features of crypto-assets will be presented, with an emphasis on cryptocurrencies. In the third part of the paper, the factors that determine the attractiveness of cryptocurrencies for criminal activities will be explained. Taking into account the taxonomy of criminal acts, in the fourth part of the paper in a systematic way, the role of cryptocurrency in traditional crime based on information technology and in cyber-dependent crime will be presented. Part five of the paper analyses the role of crypto-assets within white-collar crime. In the final part, the theoretical perspective of cryptocurrency misuse and the results of the empirical analysis will be presented.

2. Definition and Characteristics of Crypto-Assets

Regulators use different definitions of crypto-assets, so the European Central Bank Crypto-Assets Task Force defines crypto-assets as "any asset recorded in digital form that is not and does not represent either a financial claim on, or a financial liability of, any natural or legal person, and which does not embody a proprietary right against an entity" (ECB Crypto-Assets Task Force, 2019, p. 7). Coelho, Fishman and Garcia Ocampo (2021) defines crypto-assets as "type of digital asset that depends primarily on cryptography and distributed ledger or similar technology" (Coelho, Fishman & Garcia Ocampo, 2021, p. 3). The European Banking Authority defines crypto-assets as "a type of private asset that depend primarily on cryptography and distributed ledger technology as part of their perceived or inherent value" (European Banking Authority, 2019, p. 4), that is "neither issued nor guaranteed by a central bank or public authority" and which "can be used as a means of exchange and/or for investment purposes and/or to access a good or service" (European Banking Authority, 2019, p. 11). In the document prepared for the European Parliament's Committee on Economic and Monetary Affairs, Houben and Snyers (2020), describes crypto-assets as "a private digital asset that: a) is recorded on some form of a digital distributed ledger secured with cryptography, b) is neither issued nor guaranteed by a central bank or public authority, and c) can be used as a means of exchange and/or for investment purposes and/or to access a good or service" (Houben & Snyers, 2020, p. 17). There is no common taxonomy of crypto-assets in use by international standard-setting bodies. For the purpose of this paper, a basic taxonomy of crypto-assets will comprise two main categories: cryptocurrencies and tokens (European Banking Authority, 2019).

Cryptocurrencies, such as Bitcoin or Litecoin, are designed to take on the role of money, i.e., to be accepted as a means of payment, units of account and store of value.

Fiat money issued by central banks is generally accepted, unlike cryptocurrencies which are mostly considered valuable only by their customers. Characteristics of cryptocurrencies such as Bitcoin, one of the most popular cryptocurrencies, due to which they can be attractive to different users are: (1) decentralisation and disintermediation without the need for a central institution and intermediaries; (2) limited quantity, which means that there is no possibility of monetary expansion, so inflation is impossible; (3) security, which means that each transaction is verified and registered in the general ledger; (4) transparency, where each transaction is publicly registered and anyone can see it; (5) protection of personal data, which means that all transactions are public, but there are no personal identifiers since the addresses are cryptographically protected and the system is thus anonymous or pseudo-anonymous; (6) economic incentives, which means that the cryptocurrency system is not based on social incentives, but participants in the system compete with each other in solving cryptographic problems (so-called *mining*) and earn a reward; (7) simplicity of the transaction, where the transfer of funds resembles sending an e-mail; and (8) electricity coverage that forms the basis of global infrastructure (Sajter, 2018). Tokens are those crypto-assets that are issued on existing platforms to raise capital for new entrepreneurial projects or to fund start-ups or the development of new (technologically) innovative services (Houben & Snyers, 2020).

3. Factors that Determine the Attractiveness of Cryptocurrencies for Criminal Activities

Cryptocurrencies are slowly being integrated into the financial culture, and criminal activities involving cryptocurrencies have become part of modern fraudulent schemes. The AICPA FLS Fraud Task Force, an international association of certified forensic auditors, emphasizes the importance of knowing the risks and tools associated with

cryptocurrencies (Musiala et al., 2020). The challenge in criminal investigations is to understand the technical process for conducting cryptocurrency transactions. The anonymity, that is, the pseudo-anonymity of cryptocurrencies makes it difficult for investigative bodies to work, which, combined with the rapid transfer of funds, complicates the investigation process itself. External factors that, on the one hand, support the use of cryptocurrencies and, on the other hand, make it difficult to detect traces of funds transfers are: (1) the development of new technologies, (2) cooperation with cryptocurrency exchanges and (3) establishing the real identity of participants in criminal activities (Sandon, 2021).

The first factor is technological and relates to new technologies that criminal groups develop and test to increase anonymity. As part of new technologies for anonymity, technological solutions have been developed, that makes it challenging to detect exchange or digital wallet storage service providers, in order to reduce the risk of revealing identity when converting cryptocurrencies into *fiat* money. In order to conceal traces of funds, mixing services are used. Mixing service is a service that mixes potentially recognizable cryptocurrencies to increase anonymity. This service works by having the cryptocurrency owner transfer that cryptocurrency to the mixing service provider, who then mixes it with the other owner's cryptocurrencies and transfers the mixed cryptocurrencies to the desired addresses. This activity reduces the possibility of establishing a link between the original transaction and the address. Shapeshifter is a type of mixing service that goes a step further by exchanging funds for another cryptocurrency and thus increasing anonymity. Special feature of shapeshifter is chain hopping, which exchanges one cryptocurrency for another in quick succession in order to lose track as soon as possible. A special mixing service is CoinJoin, which connects the payments of different participants in one transaction, which makes it difficult to determine the individual participant, the value of each payment and the recipient of funds (Sandon,

2021, p. 7). The technological challenge are also hidden addresses - *stealth addresses*. *Stealth addresses* are one-time randomly selected addresses for each outbound transaction, automatically created in the sender's digital wallet. The hidden address never appears in the chain of blocks and cannot be linked to other recipient addresses. VPN (Virtual Private Network) and TOR (The Onion Router) are also used to conceal traces, allowing to hide identities and transactions using a different IP address or geographic location. Digital wallets also can be used to increase anonymity: one of them is the *Wasabi* privacy-oriented wallet, which has built-in features of TOR and CoinJoin. Furthermore, some private cryptocurrencies, such as Monero, in the protocol have built-in features that increase privacy, such as hidden addresses, CoinJoin services or the use of TOR (Sandon, 2021, pp. 9-10).

Another challenge in establishing the identity of participants in criminal activities is cooperation with the exchange. Exchanges are required to conduct in-depth customer analyses to protect the financial system from money laundering and terrorism financing. One of the key elements of customer analysis is the identification process through a personal identification number before cryptocurrency payments. However, in some cases, exchanges do not operate in accordance with the law or are not obliged to apply it, and when cashing out cryptocurrencies, they do not carry out the process of identifying the client. Also, in situations when they have information about personal identification numbers, they do not want to cooperate with investigating bodies in revealing the identity of their clients. Some exchanges use a P2P (*Peer to Peer*) network that operates without intermediaries, which further complicates investigations since there is no contact point for cooperation in obtaining information (Sandon, 2021, p. 13).

The third challenge in conducting investigations is to establish the real identity of participants in criminal activities, as criminal groups very often use techniques for concealing the identity. Namely, even if the exchanges operate in accordance with the

legal regulations, the identity of the suspect cannot be revealed during the in-depth analysis if they have used false identification documents. Another way of hiding identity refers to the use of a VPN network that conceals an IP address or imitates an IP address from countries that are not obliged to apply legislation. There is also the use of the technique of "peer-to-peer-trading", where the identity of third parties is used in the exchanges on behalf of someone else (Sandon, 2021, p. 15).

4. The Theoretical Perspective of Cybercrime with an Emphasis on Cryptocurrencies

The aim of this paper is to present the misuse of cryptocurrencies in cyberspace, so it is first necessary to analyse the position of cryptocurrencies within the taxonomy of cybercrime. However, as cryptocurrencies first appeared in late 2008, the emphasis will be on papers published after 2008 that analyse the taxonomy of cybercrime. Alkaabi, Mohay, McCullagh and Chantler (2011) state two types of cybercrime. The first type involves committing criminal offences where computers, computer networks, or electronic devices are the targets of criminal activities. This type of crime consists of criminal offences of unauthorized access, such as hacking, malicious programmes such as viruses, criminal offences that lead to the interruption of services, such as *botnet*, and fraud and abuse of services. The second type of cybercrime consists of crimes that include computers, computer networks and electronic devices as a tool for committing crimes. These include, for example, content-related offences, unauthorized alteration of data or programmes for personal or organisational gain, and improper use of telecommunications channels (Alkaabi et al., 2011). Within their taxonomy, it is not possible to clearly determine which type of cybercrime could be classified as cryptocurrency-related

criminal activity, as awareness of the potential misuse of cryptocurrencies arises later, with the emergence of cases such as *Mt. Gox* and *Silk Road.*

Chandra and Snowe (2020) studied cybercrime taxonomies, focusing on the period between 2001 and 2018, and found that most typologies were based on internal threats, which according to them, represent only one of the significant risks. The authors believe that the taxonomy should be representative and that it should identify changes in the categories of cybercrime that occur due to the rapid change in its nature and scope. Therefore, they base the taxonomy structure on the FBI's *Criminal Justice Information Services Division*. Chandra and Snowe (2020) classify cybercrime as *pure technology crime* and *cyber-advanced crime*. In their taxonomy, cryptocurrencies are classified as a *cyber-advanced crime*. Namely, it is about the use of computer technology with the aim of victimisation of individuals, public bodies, business entities or property.

Interpol Darknet and Cryptocurrency Task Force also have developed a cryptocurrency taxonomy (Darknet and cryptocurrency taxonomy, n.d.). Cryptocurrency-related crimes are classified into the following categories: fraud - *scam,* sexual extortion - *sextortion,* network identity theft - *phishing,* illegal access to computers - *hacking,* blackmailing computer programme - *ransomware* and the Ponzi scheme (Interpol, 2022). Europol in cybercrime also includes criminal acts - online fraud and money laundering (Cybercrime, n.d.).

4.1 *Cryptocurrencies and Cyber-Enabled Crimes*

Considering the theoretical aspects of cybercrime and taxonomies developed within the scientific community and law enforcement bodies, in order to achieve transparency and coherence, the role of cryptocurrencies in cyber-enabled crimes will be presented separately from cyber-dependent crimes. Cyber-enabled crimes refer to the traditional crimes that can be committed using computers, computer networks, or other forms of

information technology communications (ICT). Unlike cyber-dependent crimes, which are not possible to commit without the use of ICT (McGuire & Dowling, 2013). In the context of cyber-enabled crimes, the role of cryptocurrencies in money laundering, terrorism financing and trafficking of illicit goods and services will be analysed. The role of cryptocurrencies in white-collar crime as a traditional crime will be shown separately.

4.1.1 Money Laundering

Money laundering through cryptocurrencies is an umbrella illegal activity of both *online* and *offline* criminal offences as an integral part of the process of "legalization" of illicit profits. Money laundering has a precise definition that should be adapted to the context of cryptocurrencies. The Treasury's Financial Enforcement Network defines money laundering as a three-step process to make illegal money - *dirty money* - gain legal: (1) entry of *dirty money* into the legal financial system, (2) *layering* - additional transactions conceals its true origin and (3) integration within the financial system to achieve the legality of funds (Fanusie & Robinson, 2018). A special feature of money laundering that includes cryptocurrencies is a shorter laundering cycle. Namely, in this case, there is no separate financial system within which the laundering of *dirty cryptocurrencies*, unless they cash in *fiat* money. Fanusie and Robinson (2018) uses the term "Bitcoin laundering" when individuals move Bitcoins from an address associated with illegal activities to new addresses by concealing the real source of funds or cashing it into *fiat* money (Fanusie & Robinson, 2018, p. 3). The research conducted by Custers, Oerlemans and Pool has shown that cryptocurrency laundering does not include all steps, and it recommends abandoning the traditional three stages model for money laundering involving cryptocurrencies (Custers, Oerlemans & Pool, 2020).

Exchanges maintain liquidity within the cryptocurrency ecosystem and act as a kind of "bridge" between *fiat* money and the cryptosystem. Criminals intentionally seek

exchanges that are not licensed or are located in states that have poor compliance. However, Chainalysis, analysing "Bitcoin laundering", found that in 2019, almost 50% of funds were "cleared" through the two largest exchanges, namely Binance and Huobi. The question is how this is possible since they operate in accordance with the law. Further analysis found the inflow of "dirty Bitcoin" through OTC (*over the counter*) brokers who have open accounts on the Binance and Huobi exchanges. OTC brokers make buying and selling easier for individuals who cannot or do not want to trade directly. OTC brokers are independent of exchanges and conduct looser client assessments and regulatory requirements (Chainalysis, 2020b). It should also be noted that the real identity of persons involved in illegal activities can be disguised through "money mules", i.e., individuals who transfer or move illegally acquired money on behalf of others.

The next channel for "Bitcoin laundering" is *Peer to Peer* (P2P) *Platforms*, which allow direct conversion of *fiat* money and cryptocurrencies. Depending on national regulations, P2P platforms may not be subject to regulation in the future, and thus the identification of participants in the transfer of funds will continue to be avoided. In 2020, one of the most exciting areas in the development of cryptocurrencies were DeFi (*Decentralized finance*) platforms. Innovators use the Ethereum network to provide DeFi platforms lending, market forecasting or DEX (*Decentralized exchange services*) services. Unlike P2P platforms, which are basically network sites, DEX uses the Ethereum network to make real-time cryptocurrency exchanges, based on *smart contracts*. DEXs are suitable for criminal activities as they offer the possibility of avoiding compliance control, and there is no need for an intermediary who would actively control the accounts, sources of funds or identity. A special advantage of DEX is that it allows hiding Ethereum transactions since it uses *Tornado Cash mixing services* (Elliptic, 2020).

As part of the cryptocurrency laundering channel, it is also necessary to mention ATMs (*Automated teller machine*) or cryptocurrency ATMs that enable the transfer of cryptocurrencies to *fiat* money and *vice versa*. However, in many countries, ATMs for cryptocurrencies are not regulated. Additionally, it should be mentioned that cryptocurrency gambling services are recording a growing trend, enabling their clients to use cryptocurrencies. Thus, a study conducted by Elliptic found that about twenty per cent of "Bitcoin laundering" from the Alphabay *dark web market* was conducted through gambling services (Elliptic, 2020, p. 23).

4.1.2 Terrorism Financing

The number of reliable and confirmed cases of using cryptocurrencies to finance terrorism is relatively small compared to other cryptocurrency money laundering activities (Elliptic, 2020, p. 46). Publications and analyses of information on terrorism financing are sensitive, as they represent a threat to national security. Analyses of cryptocurrency terrorism financing in 2019 and 2020 have shown an increase in abuse, finding new methods of using cryptocurrencies, looking for additional ways to cover their tracks and that terrorism financing often involves a small amount of funds.

In 2021 were discovered terrorism organisations that have financed their activities with cryptocurrencies. For example, in the spring of 2021, Al-Qassam Brigades, Hamas military wing, raised a donation worth over $100,000. In July 2021, the Israeli government seized most of the related MSB (*Money service business*). The seized assets included not only Bitcoin but other cryptocurrencies such as Ethereum and Tether. In 2021, the U.S. Office of Foreign Assets Control sanctioned Farrukha Furkatovitch Fayzimatov for material aid and support to Hay'at Tahrir al-Sham, a militant organisation involved in the Syrian civil war. Fayzimatov used social media to promote, recruit new members and obtain donations to purchase equipment for Hay'at Tahrir al-Sham. It

received funds directly from centralized and P2P exchanges that did not apply regulatory requirements, and donors actively concealed their identities when sending funds. Fayzimatov forwarded the funds to high-risk exchanges located in Russia (Chainalysis, 2022).

4.1.3 Illicit Trade

Illicit trade in *darknet* markets is considered an initiator of organised crime in the European Union. It is estimated that about two-thirds of illicit sales in *darknet* markets are related to drug sales. During 2010, the first anonymous *darknet* markets or *cryptomarkets* appeared, which include the encryption of e-mail via the TOR network, which guarantees anonymity to users. *Darknet* markets consist of websites that are very similar to online trading platforms like eBay or Amazon, however, the key difference relates to the anonymity of access to *darknet* markets. There are different ways of access, and the most used are surface web pages that provide a list of *onion* addresses, i.e., *mirror sites* that contain hyperlinks to hidden pages or through the so-called "Invitation-only" markets that are accessed only through the recommendation of current users (European Monitoring Centre for Drugs and Drug Addiction and Europol, 2017).

In order for the anonymous service to be fully implemented, the financial side of the transaction also needs to be anonymous, which allows the use of cryptocurrencies and the use of various techniques to conceal identity. Tumbling/mixing is a popular way to blur bitcoin traces on the *darknet.* Many *darknet* markets offer users additional security in the form of *escrow* services. Basically, the *escrow* system works so that when a customer places an order, the fee is retained by a third party until the customer acknowledges receipt of the order. After confirmation by the buyer, the fee is forwarded to the seller (European Monitoring Centre for Drugs and Drug Addiction and Europol, 2017, p. 25).

The reasons for the closure of the *darknet* markets may be various. Based on the conducted analysis, it was found that the most common reason for closing the market is an *exit scam*. In this case, market administrators suddenly close the website and take money deposited in *escrow* accounts without fulfilling orders. The next most common reason is the *voluntary exit*, when the market closes voluntarily, by mutual agreement of the parties involved. Markets can also be closed due to the activities of law enforcement bodies and seizures. It should be mentioned that the reason for the closure of the *darknet* market may also be computer attacks or theft. According to available data, *darknet* markets have been operating for about eight months on average. The Valhalla, Dream Market and Outlaw Market had the longest period of operation, i.e., more than four years on average (European Monitoring Centre for Drugs and Drug Addiction and Europol, 2017, p. 16). According to a Chainalysis report, in 2021, many *darknet* markets were closed by agreement, and administrators allowed participants to withdraw funds. This is unusual since so far, the most common reason for closing was an *exit scam*. One of the possible reasons is avoiding the investigation of law enforcement bodies, which led to a change in the business strategy of market organisers (Chainalysis, 2022).

4.2 *Cyber-Dependent Crimes*

Different concepts of cybercrime appear in the literature, but the general approach is to differentiate cyber-enabled crimes from cyber-dependent crimes. Cyber-dependent crime cannot be committed without information technology and a certain level of knowledge about its application in cyberspace. This category of cybercrimes includes website attacks - *hacking*, malicious computer programmes - *malware*, or a blackmailing computer programmes - *ransomware*. In addition to this key difference in the context of the use of information technology, there is also a difference in the motivation. The motive for committing criminal acts dependent on information technology is not primarily financial

gain, as in the case of white-collar crime, but motives are mostly a challenge, acquiring new knowledge, curiosity or fun (Weulen Kranenbarg, 2018). Within the framework of cyber-dependent crimes will be explained the connection between cryptocurrencies and ransomware, malware, and theft of cryptocurrencies.

4.2.1 Ransomware

Ransomware is one of the methods of cybercrime in which attackers, i.e., hackers, insert a malicious computer programme - *malware* into the user's computer with the purpose of file encryption. Attackers ask for a ransom from users, most often in cryptocurrencies, to allow them to re-access the files. *Phishing* fraud, as a type of social engineering aimed at collecting confidential data, is one of the most used methods. It is estimated that 1.5 million new phishing sites are designed each month (Chainalysis, 2020a).

According to cybersecurity research, there are two types of ransomware attack offenders. The first type consists of offenders who are part of organised criminal groups. These attacks are characterized by a large scale, and a large number of organisations are attacked, and a low ransom is demanded because the offenders believe that the victims will be willing to pay a ransom. The second type of offenders are state actors who organize much bigger attacks. Recorded Future and Crowstrike research state that in 2017, North Korea supported the so-called *WannaCry* attack. The *WannaCry* attack is known for its enormous scale of infection, and during this attack, two hundred thousand computers were infected in one hundred and fifty countries and caused damage of $4 billion. In some cases of attacks committed or supported by states, the ransom is a secondary motive as the real goal is to cause chaos in the target groups of victims (Chainalysis, 2020a, p. 27).

The average duration of attacks by malicious computer programmes used to be two years, but in 2021 it was shortened to only two months. A Chainalysis study found

the reason for this shortening in rebranding. For example, at least 140 active ransomware attacks were launched by the same criminal group, although the public sought to give the impression that it was being carried out operationally by different criminal groups. Ransomware attacks can have also political motives, and an example of such an attack is the ransomware attack carried out on the night of 22 January 2022, on several Ukrainian state agencies, which was initiated by tensions between Ukraine and Russia (Chainalysis, 2022, p. 49). A relatively new form of a ransomware attack is *DarkSide* ransomware, which first appeared in August 2020. This attack is connected to the *DarkSide* group and is used as a threat to very high-income organisations. The attack includes encryption, theft of sensitive data and the threat that sensitive data will be made publicly available if no ransom is paid (Patil, 2021).

4.2.2 Malware

Malware is the umbrella name for various malicious software programmes. Offenders can use malware programme for different types of attacks such as spying, destroying data and resources, causing system errors, or slowing down information system. The use of malware to steal or extort cryptocurrencies is nothing new, as ransomware attacks on victims' devices and cryptocurrencies have also been carried out using malware. However, these attacks require more careful planning and stronger implementation skills, especially when carrying out attacks on organisations. There are also malware attacks that are not so sophisticated and have a *spray-and-pray* approach. In this case, it is about sending spam to millions of users and stealing small amounts (Chainalysis, 2022, p. 56).

The following types of malwares are used to steal cryptocurrencies: *Info stealers*, *Clippers*, *Cryptojackers* and *Trojans*, and most of them can be purchased quite cheap on specialized forums. Info stealers are a type of malicious programme that collects data on an infected computer to pass it on to an attacker, such as cryptocurrency data. Clippers

are a malicious programme that “hijacks” a cryptocurrency transaction by exchanging the address with the one owned by the attacker, and in this case, the cryptocurrency payment ends up in the attacker's account instead of the desired recipient (Chainalysis team, 2022). Cryptojackers are a malicious programme that allows the computer power of the victim's computer needed to mine cryptocurrencies could be used without permission. The Trojan is a virus that at first glance looks like the legal programme, however, when inserted into the victim’s computer, it interferes with the operation of the computer, causing theft or other forms of damage to the victim’s computer (Chainalysis, 2022, p. 57).

4.2.3 Stolen Funds

It can be said that 2021 was a “top-notch” year for the theft of cryptocurrencies, since $3.2 billion worth of cryptocurrencies were stolen (Chainalysis, 2022, p. 70). With this in mind, one can get the impression that hackers have exceptional computer knowledge and skills, however, social engineering is most commonly used to steal cryptocurrencies, and hackers, in most cases, have tried to blackmail users or employees of exchanges with malware programmes that allow them access to their cryptocurrencies. Once the malware programme gives them access, hackers can wait months and observe cash flows so they can steal as much as possible (Chainalysis, 2020a).

The technique of social engineering is implemented in a way that hackers set up a fake company, use fake websites and are active on social networks. Most often it is about advertising platforms for automated trading, the so-called “trading bot”, and on the site leave the possibility to download a free trial version. If a trial version is downloaded, the malware programme helps hackers gather information about the digital key and wallet. According to Chainalysis, in 2021, in 51% of cases, the final destination of stolen cryptocurrencies was on DeFI platforms (Chainalysis, 2022, p. 74).

5. The Dark Side of Crypto-Assets in White-Collar Crime

The cryptocurrency market, despite instability and volatility, is attracting the attention of investors and entrepreneurs. The remarkable growth in the value of Bitcoin, as well as other cryptocurrencies, is a magnet for manipulative techniques and various types of frauds. Trozze et al. (2020) have identified twenty-nine types of cryptocurrency-related frauds and found that the Ponzi scheme and high-yield investment programmes were subject to 44.4% of all academic research on frauds. These data indicate the need to understand the role of cryptocurrencies in the implementation of financial frauds, in order to protect investors and entrepreneurs.

Financial frauds related to cryptocurrencies, considering the characteristics of the offender and the motive for committing the crime, can be viewed as part of white-collar crime. Although the term white-collar crime leads to certain disagreements and debates among criminologists, there is consensus that it appears in the context of occupation, that the basic motive of the offender is financial gain or business success and that it does not include direct violence. White-collar crime is considered illegal or unethical conduct that violates the entrusted responsibility and is committed by an individual or an organisation of high or respectable social status, most often during a professional activity, with the aim of achieving a personal or organisational gain (Schneider, 2020). A key element in white-collar crime is a breach of trust, which is also strongly shown in cryptocurrency-related frauds.

The main categories of criminal activities within white-collar crime are corruption, corporate fraud, money laundering, securities and commodities fraud, financial institution fraud, fraud against the government and health care fraud. Within the category of securities and commodities fraud, the Federal Bureau of Investigation lists the following criminal activities: investment fraud, Ponzi schemes, pyramid schemes,

market manipulation, broker embezzlement, and commodities fraud such as gold (White-Collar Crime, n.d.).

5.1 *The Role of Cryptocurrencies in Financial Fraud and in the Context of White-Collar Crime*

According to Reurink (2018), the phenomenon of financial fraud has not been sufficiently investigated, although there is awareness of its shift from the margins of financial market activity towards the wider financial industry. The conceptual definition of financial fraud is complex not only from a legal point of view but also due to different understandings of fraudulent activities within certain segments, such as financial institutions, markets, or insurances (Reurink, 2018). Although different can be attributed to fraud meaning, fraud should be viewed in the context of the prohibited use or manipulation of financial information (Fligstein & Roehrkasse, 2013).

Financial information forms the basis of market transactions and significantly affects the climate in financial markets. In order to ensure the availability of financial information, to protect the integrity of such information and to protect participants who do not have the necessary expertise in understanding financial information, regulatory authorities should provide a legal framework to protect market participants. There are several objectives to be achieved by regulation: the first objective is the problem of market asymmetry, and therefore regulatory authorities require the timely publication of relevant information so that all market participants are on an equal footing. The second goal is aimed at protecting all participants who do not have the necessary expertise, and therefore financial advisors are committed to providing clients with the necessary information when deciding on financial transactions. The third goal is to prevent deceptive behaviours that mislead participants in financial markets (Reurink, 2018, p. 1294).

When some market participants knowingly and willingly mislead other participants by providing them with false, incomplete, or manipulative information and thus violate any of the above three regulatory objectives, then we enter the realm of financial fraud. The specific actions taken in the implementation of financial fraud may be different, as they depend on the market segment in which they are implemented, the type of financial instruments and the characteristics of fraud offenders. Therefore, according to Reurink (2018), there is a conceptual difference between financial frauds, and these can be divided into false financial disclosures, financial scams, and fraudulent financial mis-selling. False financial disclosure refers to giving false statements about capabilities and financial health of a business entity to market participants who then make investment decisions based on such information. Unlike false financial disclosures, financial scams are fraudulent schemes in which individuals voluntarily cooperate with offenders and hand over their financial resources or sensitive personal information to them. The third type of financial fraud refers to fraudulent financial mis-selling, where offenders provide the end user with false information about a financial product, knowing in advance that the product is unsuitable for him (Reurink, 2018, p. 1294). Below it will be presented the role of cryptocurrencies in financial scams and in breach of trust in the context of white-collar-crime.

5.1.1 Crypto-Assets and Ponzi Scheme

Understanding the Ponzi scheme is necessary as this is the most commonly used investor fraud. The Ponzi scheme is a type of fraud in which investors are promised high rates of return with little or no risk. The organizers of the fraud and the first investors are paid out with the resources of later investors when in reality there is little, or no income generated from the business project. The Ponzi scheme works as long as there is an arrival of new investors or as long as investors do not require a refund (Ponzi scheme, n.d.).

Chainalysis states that 2019 was the year of the biggest cryptocurrency frauds worth $4.3 billion, with millions of victims (Chainalysis, 2020a). Most of this fraudulent income was generated on the basis of the Ponzi scheme. Although no significant presence of Ponzi schemes with cryptocurrencies was recorded in 2020, in 2021 the Finiko Ponzi scheme was discovered, which was mainly present in Eastern Europe, and the victims lost more than $1.1 billion (Chainalysis, 2022). Below it will be shown how some of the largest cryptocurrency-based Ponzi schemes operate.

The PlusToken project started in April 2018 and was presented to investors as *a high-yield investment programme* and attracted the most investors from China and South Korea. This investment programme, which attracted about three million victims, was suddenly closed in June 2019, and a notice was posted on the official website that read "Sorry, we have run". The fraudulent investment scheme offered investors a monthly return ranging from 9% to 18%, similar to the 2018 BitConnect fraudulent Ponzi scheme. The illusion of investment was maintained by the development of projects related to cryptocurrencies and the PlusToken digital wallet. However, typical for the Ponzi scheme, newer investments were used to return to older investors (Michael, 2022). PlusToken fraud scheme was presented to victims with an outstanding marketing strategy, and the target group were individuals without knowledge of cryptocurrencies.

The anatomy of the PlusToken scheme is presented in *The 2020 State of Crypto Crime*, in which Chainalysis followed the trail of stolen 800,000 Ethereum (ETH) and 45,000 Bitcoin (BTC). In the initial phase of the fraudulent scheme, the fraudsters paid the victims the expected return on investment in order to create the illusion of a responsible business entity. By analysing the trace of ETH, it was found that 10,000 ETHs were cashed in, and the remaining 790,000 ETHs were forwarded to digital wallets and kept there for months. Tracking the stolen 45,000 BTC was more complex. Chainalysis found that 25,000 BTCs were cashed, and the remaining 20,000 BTCs were forwarded to

over 8,700 crypto addresses, indicating a significant effort by the fraudsters to cover their tracks. Further investigation found that the fraudsters moved the BTC about 24,000 times using *Wasabi* digital wallets and the CoinJoin protocol, using more than 71,000 different addresses. It is important to note that the investigation found that the offenders had used the *peel chains* money laundering technique. This money laundering technique is carried out by the fraudsters by forwarding the funds in quick succession through several digital wallets, allocating smaller amounts to be cashed in at each step, and passing most of the funds to the next wallet. Eventually, the remaining funds were forwarded to OTC broker addresses. Chinese media reported that the fraud attracted cryptocurrencies worth more than $3 billion (Chainalysis, 2020b).

BitConnect, a famous Ponzi cryptocurrency scheme launched in 2016, also used complex investment programmes. Fraud victims were introduced to the lending programme, by trading Bitcoin for a *BitConnect* token in exchange for paying interest with the ability to freeze the current value of the token for a certain period of time while earning interest was calculated on a daily basis. The most controversial part of the fraud was the "trading bot" algorithm for calculating interest rates. In January 2018, the authorities issued an order to close the company (OneCoin, n.d.). In February 2022, the U. S. Department of Justice announced that were filed charges against the founder of *BitConnect* for a $2.4 billion global fraud scheme (Department of Justice, 2022).

The next example *is OneCoin*, a centralised cryptocurrency that became operational in 2014. Its founder Ruža Ignatova promoted *OneCoin* as a cryptocurrency that operates in the same way as other cryptocurrencies, which are used for payment and have their digital wallet. However, in reality, there was no background technology to support *OneCoin* or the payment model. The company noted the sale of trading training materials as the core of its business and actually operated as a multi-level marketing scheme. Investors were offered rewards for bringing in new participants (Frankenfield,

2022). Ruža Ignatova escaped in 2017 and was put on the list of most wanted persons by Europol, offering a reward of €5,000 for information that would lead to her arrest (OneCoin, n.d.).

The Ponzi schemes described above confirm the successful integration of cryptocurrencies into financial frauds. The Security Exchange Commission has published "red flags" common to Ponzi schemes based on virtual currencies: high investment returns with little or no risk, overly consistent returns, unregistered investments, unlicensed sellers, complex strategies investments that are difficult to understand, the inability to obtain detailed information about the investment, problems in paying the return on investment and encouraging the organisers to reinvest the realised return on investment (Securities and Exchange Commission, 2013).

5.1.2 Frauds Based on Tokens

The distributed ledger technology has created the possibility of relatively fast, cheap, and easy obtaining of funds for entrepreneurial projects or *Initial Coin Offerings* (hereinafter: ICO). The initial offer allows investors to acquire tokens in exchange for *fiat* money or other cryptocurrencies over a period of time. Tokens make it easier for investors to access the issuer's services but do not give them ownership. It is the right of ownership that makes the difference between an ICO and an Initial public offer (hereinafter: IPO). There are also some differences between ICO and *Crowdfunding* that allows a relatively large number of individuals to participate with small amounts in financing an entrepreneurial venture without the usual presence of intermediaries (Tiwari, Gepp & Kumar, 2019).

ICO brings several advantages to the issuer, such as bypassing financial intermediaries such as banks and stock exchanges, thus speeding up the bidding process and reducing costs, the required technology is relatively simple and accessible, and due to increased interest in cryptocurrencies, the amount of funds that can be raised is larger

than, for example, through *Crowdfunding* or a traditional IPO (Delivorias, 2021). The fundamental shortcoming of the ICO is the possible problem of information asymmetry. Namely, ICOs have not been subject to special regulation so far, so ICO the *white paper* is inconsistent in terms of content. Even when the content of the *white paper* is detailed enough, it cannot be compared to the prospectus required for securities. It is important to highlight the weak legal protection of investors in the case of bankruptcy or liquidation of such entities. Also, unlike shareholders in traditional corporate infrastructure who have the right to vote, investors in tokens do not possess any form of supervision. And finally, ICO is characterised by high volatility, which makes the investment itself uncertain (Delivorias, 2021, p. 5).

The euphoria of investing in ICO and the lack of *due diligence* in the projects creates an environment suitable for various types of financial frauds, which is confirmed by the fact that more than 10% of the funds invested in ICO were lost through various forms of fraud. Hornuf, Kück and Schwienbacher (2022) conducted research on ICO-related frauds and identified the following types of fraud: *exit fraud*, securities fraud, Ponzi scheme and *pump and dump*, *phishing*, and *hacking*. According to Chainalysis, the latest fraudulent innovation is *rug pull*. His importance could be seen in the fact that in 2021, *rug pull* accounted for 37% of fraudulent revenue, and in 2020 it accounted for only 1% (Chainalysis, 2022). Generally speaking, *rug pull* is a type of fraud where organisers artificially increase the value of a token before running away with the funds while leaving investors with worthless assets. *Rug pull* fraud represents the form of *exit fraud* (Puggioni, 2022).

5.1.3 Cryptocurrencies and Market Manipulation Techniques

Two manipulation techniques that are most used in the cryptocurrency markets are *pump and dump* and *wash trade.* The *pump and dump* manipulation technique is common in the

cryptocurrency markets, as opposed to regulated financial markets, where it is prohibited by law. The modus operandi of this manipulation technique in the cryptocurrency markets is slightly different from that used in traditional financial markets. Organisers of *pump and dump* manipulation use social networks such as Reddit, Discord or Telegram, where participants are organised into groups (Barnes, 2018). These groups have different numbers of members, so smaller groups have about 2,000 members, and some large ones have more than 200,000 members. The subject of manipulation of these groups are less popular cryptocurrencies with low market capitalisation, and low trading volume. The growth of cryptocurrency values during the *pump* phase can be over 950% and can last from just a few minutes to a few hours, followed by a collapse phase, or *dump* (Kamps & Kleinberg, 2018).

Wash trading is one of the common manipulation techniques in traditional financial markets, and its aim is to create the illusion of trading volume, which then reduces the integrity and confidence in financial markets. The basic feature of the *wash trading* technique is that individuals or groups enter into business arrangements by agreement and at the same time appear as buyers and sellers of a particular financial instrument. The implementation of this manipulation technique does not change the actual ownership of the object of trading but only creates the illusion of increased market activity of a particular trading instrument and thus misleads other market participants (Cao, Li, Coleman, Belatreche & McGinnity, 2016).

Wash trading is also present in the cryptocurrency markets, which is confirmed by the expertise in the actual presentation of the volume of cryptocurrency trading. Bitwise Asset Management published the results of a 2019 survey showing that about 95% of the volume of cryptocurrency trading was fake (Hougan, Kim & Lerner, 2019). The strategy of creating the illusion of demand in the cryptocurrency market, unlike traditional financial markets, is implemented in several ways: (1) false publication of

transactions, so that cryptocurrency exchanges simply publish transactions that did not happen in reality; (2) exchanges that trade cryptocurrencies also participate in buying and selling on their own platform, thus increasing the volume of trading; (3) exchanges pay the so-called *wash trade* directly to a third party involved in increasing the trade volume; or (4) some exchanges provide certain benefits to other exchanges in the cryptocurrency markets that generate higher trading volumes (Hougan et al., 2019, p. 36).

6. Conclusion

The emergence of crypto-assets in cyberspace supports a relatively favourable climate for the implementation of criminal acts. Necessary conditions for criminal acts are privacy, anonymity, authentication, hidden exchange, and secure payment (European Monitoring Centre for Drugs and Drug Addiction and Europol, 2017). Cryptocurrencies play a key role in achieving relatively secure payment terms, as they reduce the risk of detecting traces through a cryptographic protection mechanism when conducting transactions. Based on the study of criminal acts related to cryptocurrencies, its presence in the implementation of traditional criminal acts based on information communication technology, but also cyber-dependent crimes, was found. Cryptocurrencies represent a sophisticated money laundering mechanism, regardless of whether they are *online* or *offline* criminal acts in the process of legalizing illicit profits.

The expansion of crypto-assets related criminal acts has been extended to financial frauds. This paper analyses the misuse of crypto-assets within white-collar crime. Crypto-assets based financial fraud is a more complex scheme; however, a key element is the breach of trust and the ambition of victims to be involved in *get-rich-quick-schemes* (Eurojust, 2021). Because of the characteristics of financial frauds based on crypto-assets, investors should pay attention to *red flags* when evaluating investment

projects: high investment return with little or no risk, unregistered investments, unlicensed sellers, complex investment strategies and difficulties in receiving a return on investment.

It is important to emphasize that cryptocurrencies are a promising technology. However, like all new technologies, it needs to go through different stages of adaptation. Depending on the perception and interests of individuals, its use also arises. In addition to the direct financial damage to victims, the misuse of cryptocurrencies also creates indirect damage, given the negative perception of cryptocurrencies. The international cooperation of regulatory bodies should support this global innovative technology by enabling safe implementation on the one hand, and protection of all participants in cyberspace on the other.

References

Alkaabi, A., Mohay, G., McCullagh, A., & Chantler, N. (2011). Dealing with the Problem of Cybercrime. In I. Baggili (Ed.), *Digital Forensics and Cyber Crime. ICDF2C 2010. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering* (pp. 1–18). Berlin, Heidelberg: Springer.

Barnes, P. (2019). Crypto Currency and its Susceptibility to Speculative Bubbles, Manipulation, Scams and Fraud. *Journal Of Advanced Studies In Finance*, ***9***(2), 60-77. doi:10.14505//jasf.v9.2(18).03

Cao, Y., Li, Y., Coleman, S., Belatreche, A., & McGinnity, T. M. (2016). Detecting Wash Trade in Financial Market Using Digraphs and Dynamic Programming. *IEEE Transactions on Neural Networks and Learning Systems*, *27*(11), 1-13. doi:10.1109/TNNLS.2015.2480959

Chainalysis. (2020a). *Cryptocurrency Typologies: Our Guide to Who's Who on the Blockchain*. Retrieved from https://go.chainalysis.com/2020-typologies-report.html

Chainalysis. (2020b). *The 2020 State of crypto crime. Everything you need to know about darknet markets, exchange hacks, money laundering and more*. Retrieved from https://ag-pssg-sharedservices-ex.objectstore.gov.bc.ca/ag-pssg-cc-exh-prod-bkt-ex/257%20-%20001%20Appendix%20A%20-%202020-Crypto-Crime-Report%20Chainanalysis.pdf

Chainalysis. (2022). *The 2022 Crypto Crime Report. Original data and research into cryptocurrency-based crime.* Retrieved from https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf

Chainalysis team. (2022, January 19). Meet the Malware Families Helping Hackers Steal and Mine Millions in Cryptocurrency [Blog post]. Retrieved from https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-malware/

Chandra, A. & Snowe, M. J. (2020). A taxonomy of cybercrime: Theory and design. *International Journal of Accounting Information Systems*, 38(C). doi:10.1016/j.accinf.2020.100467

Coelho, R., Fishman, J., & García Ocampo, D. (2021). Supervising cryptoassets for anti-money laundering. *FSI Insights on policy implementation*, Nr. 31, April, available at: https://www.bis.org/fsi/publ/insights31.pdf

Custers, B., Oerlemans, J. - J., & Pool, R. (2020). Laundering the Profits of Ransomware: Money Laundering Methods for Vouchers and Cryptocurrencies. *European Journal of Crime, Criminal Law and Criminal Justice*, 28, 121-152. doi:10.1163/15718174-02802002

Cybercrime. (n.d.). Retrieved from https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime

Darknet and cryptocurrency taxonomy (n.d.). Retrieved from https://www.interpol.int/en/How-we-work/Innovation/Darknet-and-Cryptocurrencies

Delivorias, A. (2021). *Understanding initial coin offerings: A new means of raising funds based on blockchain*. Retrieved from https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/696167/EPRS_BRI(2021)696167_EN.pdf

Department of Justice. (2022). *BitConnect Founder Indicted in Global $2.4 Billion Cryptocurrency Scheme* [Press release]. Retrieved from https://www.justice.gov/opa/pr/bitconnect-founder-indicted-global-24-billion-cryptocurrency-scheme

ECB Crypto-Assets Task Force. (2019). *Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures*. Retrieved from https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf

Elliptic. (2020). *Financial Crime Typologies in Cryptoassets. The Concise Guide for Compliance Leaders*. Retrieved from https://www.elliptic.co/hubfs/Financial%20Crime%20Typologies%20in%20Cryptoassets%20Guides%20(All%20Assets)/Typologies_Concise%20Guide_12-20.pdf

Eurojust. (2021). *Eurojust Guidelines on How to Prosecute Investment Fraud.* Retrieved from https://www.eurojust.europa.eu/sites/default/files/assets/eurojust_guidelines_how_to_prosecute_fraud_07_2021.pdf

European Banking Authority. (2019). *Report with advice for the European Commission. On crypto-assets.* Retrieved from https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA%20Report%20on%20crypto%20assets.pdf

European Monitoring Centre for Drugs and Drug Addiction and Europol. (2017). *Drugs and the darknet: Perspectives for enforcement, research and policy*. Retrieved from https://www.europol.europa.eu/sites/default/files/documents/drugs_and_the_darknet_-_td0417834enn.pdf

Europol. (2021). *Europol Spotlight - Cryptocurrencies: Tracing the Evolution of Criminal Finances*. Retrieved from https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Sp

otlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf

Fanusie, Y. J., & Robinson, T. (2018). *Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services*. Retrieved from https://info.elliptic.co/whitepaper-fdd-bitcoin-laundering

Fligstein, N., & Roehrkasse, A. F. (2013). *All the Incentives Were Wrong: Opportunism and the Financial Crisis*. Retrieved from https://www.law.berkeley.edu/files/csls/Fligstein_Paper_CSLS_23_Sep13(1).pdf

Frankenfield, J. (2022). *OneCoin*. Retrieved from https://www.investopedia.com/terms/o/onecoin.asp

Hornuf, L., Kück, T., & Schwienbacher, A. (2022). Initial coin offerings, information disclosure, and fraud. *Small Business Economics*, 58, 1741-1759. doi:10.1007/s11187-021-00471-y

Houben, R., & Snyers, A. (2020). *Crypto-assets - Key developments, regulatory concerns and responses*. Retrieved from https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU(2020)648779_EN.pdf

Hougan, M., Kim, H., & Lerner, M. (2019). *Economic and Non-Economic Trading In Bitcoin: Exploring the Real Spot Market For The World's First Digital Commodity*. Retrieved from https://www.sec.gov/comments/sr-nysearca-2019-01/srnysearca201901-5574233-185408.pdf

Interpol. (2022). *INTERPOL-Innovation-Centre/DW-VA-Taxonomy*. Retrieved from https://github.com/INTERPOL-Innovation-Centre/DW-VA-Taxonomy/commit/df6b0026ba9b174140a109e51410ebf015fe53c1

Kamps, J., & Kleinberg, B. (2018). To the moon: defining and detecting cryptocurrency pump-and-dumps. *Crime Science, 7*, 18. doi:10.1186/s40163-018-0093-5

McGuire, M., & Dowling, S. (2013). *Cyber crime: A review of the evidence*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf

Michael. (2022, May 15). Plus Token (PLUS) Scam – Anatomy of a Ponzi [Blog post]. Retrieved from https://boxmining.com/plus-token-ponzi/

Musiala, R. A., 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*. Retrieved from https://cointhinktank.com/upload/eye-on-fraud-cryptocurrency-202003.pdf

OneCoin. (2022). Retrieved March 22, 2022, from Wikipedia: https://en.wikipedia.org/wiki/OneCoin

Patil, Y. (2021, June 9). DarkSide Ransomware [Blog post]. Retrieved from https://blog.qualys.com/vulnerabilities-threat-research/2021/06/09/darkside-ransomware

Ponzi scheme. (n.d.). Retrieved from https://www.law.cornell.edu/wex/ponzi_scheme

Puggioni, V. (2022, February 6). Crypto rug pulls: What is a rug pull in crypto and 6 ways to spot it. *Cointelegraph*. Retrieved from https://cointelegraph.com/explained/crypto-rug-pulls-what-is-a-rug-pull-in-crypto-and-6-ways-to-spot-it

Reurink, A. (2018). FINANCIAL FRAUD: A LITERATURE REVIEW. *Journal of Economic Surveys*, *32*(5), 1292-1325. doi:10.1111/joes.12294

Sajter, D. (2018). Financijska analiza kriptovaluta u odnosu na standardne financijske instrumente. In D. Koški, D. Karačić & D. Sajter (Eds.), *Financije – teorija i suvremena pitanja* (pp. 277-301). Osijek: Ekonomski fakultet u Osijeku.

Sandon, T. (2021, November 3). Keeping up With Financial Investigations in the Crypto Age [Blog post]. Retrieved from https://www.cognyte.com/blog/keeping-up-with-crypto-financial-investigations-cognyte/

Schneider, S. G. (2020). The Gray Area of White-Collar Crime: It Isn't Black or White. *FAU Undergraduate Law Journal*, 7-36. Retrieved from https://journals.flvc.org/FAU_UndergraduateLawJournal/article/view/121968

Securities and Exchange Commission. (2013). *Ponzi Schemes Using Virtual Currencies*. Retrieved from https://www.sec.gov/files/ia_virtualcurrencies.pdf

Tiwari, M., Gepp, A., & Kumar, K. (2020). The future of raising finance - a new opportunity to commit fraud: a review of initial coin offering (ICOs) scams. *Crime, Law and Social Change, 73*(4), 417-441. doi:10.1007/s10611-019-09873-2

Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S.D. (2020). Cryptocurrencies and future financial crime. *Crime Science, 11*, 1. doi:10.1186/s40163-021-00163-8

Weulen Kranenbarg, M. (2018). *Cyber-offenders versus traditional offenders: An empirical comparison* (Doctoral dissertation, Vrije Universiteit, Amsterdam). Retrieved from http://dare.ubvu.vu.nl/handle/1871/55530

White-Collar Crime. (n.d.). Retrieved from https://www.fbi.gov/investigate/white-collar-crime