TEME, Vol. XLVII, Nº 4, October – December 2023, pp. 975–990

Review article https://doi.org/10.22190/TEME220701060D
Received: July 1, 2022 UDC 343.3/.7
Accepted: September 19, 2023

CRYPTOCURRENCIES AND CRIME

Darko Dimovski*

University in Niš, Faculty of Law, Judicial Research Center, Niš, Serbia

Abstract

In the introductory part of the paper, the author briefly explores the emergence of the first cryptocurrency (Bitcoin), which was initially devised for the purpose of securing easier transactions without intermediaries. Criminals soon realised that cryptocurrencies, due to their inherent characteristics, could provide them with anonymity. As other cryptocurrencies (altcoins) emerged, it was necessary to define their conceptual framework. While cryptocurrencies were initially used in illegal sales of narcotics, their application soon spread to a number of other criminal activities. In that context, the author first presents the reasons that led criminals to turn to cryptocurrencies in their financial transactions, and then explains the possible uses of cryptocurrencies in the commission of crime. The central part of the paper provides examples of criminal activities committed by using cryptocurrencies. It is reasonable to expect that, in the future, the use of cryptocurrencies will extend to other criminal activities, which are still unaffected by the trend that has existed for the last ten years.

Key words: cryptocurrencies, Bitcoin, crime.

КРИПТОВАЛУТЕ И КРИМИНАЛИТЕТ

Апстракт

Аутор рада на почетку излаже када је настала прва криптовалута - биткоин, уз образложење шта је била сврха његовог креирања. Како су се после биткоина јавиле и друге криптовалуте било је неопходно одредити његов појам. Иако су замишљене с циљем олакшавања трансакција без посредника, криминалци су убрзо схватили да криптовалуте захваљући својим карактеристикама могу да им обезбеде анонимност. Мада су првобитно коришћене зарад продаје наркотика, употреба криптовалута се убрзо проширила на бројне друге криминалне активности. С тим у вези, аутор представља разлоге због којих су се криминалци определили да се окрену криптовалутама, те у другом делу рада наводећи примере образлаже у којим криминалним активностима се развила учестала употреба криптовалута. Са разлогом се може очекивати да употреба криптовалута буде проширена и на друге криминалне активности, које су још увек незахваћене трендом који постоји последњих десетак година.

Кључне речи: критповалуте, биктоин, криминалитет.

* Corresponding author: Darko Dimovski, University in Niš, Faculty of Law, Judicial Research Center, Trg kralja Aleksandra 11, 18105 Niš, Serbia, darko@prafak.ni.ac.rs

INTRODUCTION

Bitcoin is a type of cryptocurrency created by the mysterious Satoshi Nakamoto in 2009. It was created for the purpose of facilitating cashless transactions without any compensation. Unlike standard currencies managed by state governments worldwide, it is the first digital currency and payment system managed by decentralised governance (by all Bitcoin holders). Bitcoin can be sent from user to user without the need for any intermediaries; the transaction is verified on the so-called network nodes, via cryptography, and recorded in a publicly distributed ledger of transactions called a blockchain (Investopedia, 2022).

In order to explain what is meant by a blockchain, we should look at the common transaction methods. The problem of mistrust, quite common in transactions, was solved by involving an intermediary, which was often embodied in the intermediary role of a bank. In order to limit the power of banks, states became involved in mediation. Yet, it did not prevent some banks from becoming even more powerful than some states. In this regard, there was a desire to liberalise the standard business transactions model. This aspiration is reflected in the creation of blockchain technology which enables transition from the centralised to the so-called peer-to-peer (P2P) model. Blockchain technology is structured as a single linked body of data given in chronological order and organised in a digital chain of blocks containing information about each transaction (Investopedia, 2022). It enables transactions without any intermediaries; transaction data is recorded in blockchain nodes, while data protection is ensured by cryptographic methods. Blockchain nodes store the data of all recorded transactions; they serve as infrastructure because they constantly communicate with each other, synchronise, and exchange and verify the latest data. In case individual data blocks do not pass verification by certain nodes in charge of verifying the authenticity of records in the chain, the proposed data blocks are rejected. In other words, the network cannot be compromised by placing false data (Minović, 2017, p. 22).

Other cryptocurrencies, known under the generic name *altcoins*, were created soon afterwards. To ensure better understanding, we should first define this concept. The term *cryptocurrency* refers to digital or virtual currency that is protected by cryptography, which makes it almost impossible to counterfeit or double-spend. In other words, cryptocurrency is a form of network-based digital assets, distributed across a large number of computers (Investopedia, 2022).[1] The basic feature of all cryptocurrencies is the fact that it is almost impossible for state authorities to control them; as a result, they only have to accept or reject cryptocurrencies as a legitimate means of trading (Milutinović, 2018, p. 107).

---

[1] Investopedia (2022): Cryptocurrency, J. Frankenfield (updated January 11, 2022); Retrieved 28 March 2022 from: https://www.investopedia.com/terms/c/cryptocurrency.asp

Although designed to facilitate transactions without intermediaries, cryptocurrencies provided an ideal opportunity for criminals around the world to engage in illegal activities by using blockchain technology, which provides absolute anonymity and thus makes it impossible for government agencies to seize cryptocurrencies. Access to cryptocurrencies is provided only to persons who have the appropriate key (code). In 2011, Ross Ulbricht made a 'pioneering endeavour' to use cryptocurrencies in criminal activities. Along with creating the website called *Silk Road*, he started the production of psychedelic mushrooms, with the goal of selling them through the site by using Bitcoin. He used the Tor browser, which allows users to surf the web anonymously, without revealing their identity and location. In this case, the identity of the buyer could possibly be revealed by referring to the postal address where the mushrooms would be delivered, but this problem was solved by using an anonymous *post restante*. Soon, other illegal products began to be sold through this website (Poper, 2017, pp. 89-91). The presented example illustrates the unlimited possibilities of using cryptocurrencies in the commission of illegal activities, while the identity of the perpetrator remains undiscovered. In this context, the paper analyses the reasons for using cryptocurrencies, examines their possible uses in different criminal activities, provides examples of crimes committed by using cryptocurrencies, and discusses future trends concerning the use of cryptocurrencies in criminal activities.

WHY DO CRIMINALS LIKE CRYPTOCURRENCIES?

There are five reasons why criminals have turned to cryptocurrencies. Although all transactions are recorded on the blockchain, which is a public record, the identities of the creators of transactions remain unknown. In this way, criminals can engage in completely anonymous criminal activities, such as drug trafficking, trading weapons, or child pornography. At the same time, anonymity makes it much easier for terrorist organisations to raise funds for attacks.

The second reason for the growing use of cryptocurrencies in criminal activities is the lack of any links between participants. Those participating in criminal activities do not need to know one another; the transfer of cryptocurrencies occurs in a virtual space, without any intermediaries.

The third reason is twofold – ease of access and speed of transactions. To make use of cryptocurrencies, one only needs to have an Internet connection and use the appropriate application. Since cryptocurrencies are digital assets, there is no need for transactions to be validated by third parties (e.g. banks, exchanges, brokers). Consequently, cryptocurrencies are transferred within just a few minutes, with no possibility of cancelling transactions (Cognyte, 2021). In order to illustrate the advantage of cryptocurrency trading in relation to the traditional transfer of money through

a bank, we can note that in the traditional banking environment it is not possible to transfer money at all times. There are several reasons for a delayed transfer of money between banks. Among other things, delays may occur due to non-working hours, weekends, holidays, and many other reasons, such as natural disasters, different time zones, lack of validation/certification/verification, different currencies, inaccurate transfer data, and inadequate fraud prevention procedures (Statrys, 2021). On the other hand, there are no such problems in a cryptocurrency transaction, which is automatic and fully decentralised.

Easier storage and transfer are the fourth reason criminals have turned to cryptocurrencies. Namely, cryptocurrencies are easy to store (in digital wallets) because no physical space is needed to store information about them. In this way, the attention of thieves is not attracted, but neither is the attention of the authorities. Transactions with cryptocurrencies are easy because there are no borders/restrictions preventing their trade, which also implies that they cannot be seized. For example, the Lazarus Group, a cybercrime organisation linked to North Korea, is estimated to be responsible for stealing cryptocurrencies worth over 1.75 billion US dollars. A major theft was recorded in 2020, when 275 million US dollars of cryptocurrency disappeared from the KuCoin stock exchange as cybercriminals hacked private keys to the exchange's hot wallets (Chainalysis, 2021).[2] Another example is the hacking of the blockchain-based Poly Network website in August 2021, when more than 600 million US dollars' worth of different cryptocurrencies were stolen, which is considered to be one of the largest cryptocurrency thefts in history so far (CoinDesk, 2021).[3]

The lack of borders is the fifth reason for criminals' willingness to turn to cryptocurrencies. From all of the above, we can conclude that cryptocurrency transactions can be made even in spite of existing borders. To illustrate the ease of the global transfer of cryptocurrencies, we may refer to an example of cryptocurrency money laundering worth 16 million US dollars, committed by a Swedish citizen, who was subsequently sentenced to 15 years' imprisonment (Cognyte, 2021).

THE USE OF CRYPTOCURRENCIES IN CRIMINAL ACTIVITIES

Before we turn to a detailed analysis of the use of cryptocurrencies in criminal activities, it is important to note that the criminal use of crypto-

[2] Chainalysis (2021): Lazarus Group Pulled Off 2020's Biggest Exchange Hack and Appears to be Exploring New Money Laundering Options, 2/9/2021, Retrieved 01 April 2022 from: https://blog.chainalysis.com/reports/lazarus-group-kucoin-exchange-hack/

[3] CoinDesk (2021): Cross-Chain DeFi Site Poly Network Hacked; Hundreds of Millions Potentially Lost, E. Gkritsi, M.Shen, 9/ 10/2021; Retrieved 1 April 2022 from: https://www.coindesk.com/markets/2021/08/10/cross-chain-defi-site-poly-network-hacked-hundreds-of-millions-potentially-lost/

currencies is no longer primarily limited to cybercrime activities. In other words, the criminal use of cryptocurrencies refers to all criminal activities that require a monetary transaction. Based on the above, we can conclude that the possibilities of using cryptocurrencies in criminal activities are unlimited. Although there are estimates of relevant national and foreign bodies regarding the criminal use of cryptocurrencies, it should be emphasised that the 'dark figure' of crime is quite high because the possibilities of detecting such activities are rather narrow. Yet, we should be cautious when making estimates because criminals still like cash, and the use of cash for criminal activities is still significantly higher than the criminal use of cryptocurrencies. We may conclude that cryptocurrencies have given criminal offenders more opportunities to engage in their activities. At the same time, the largest obstacle to a greater use of cryptocurrencies in criminal activities is high volatility, i.e. the range and the speed of movement of cryptocurrency values (Europol, 2021, p. 2).

According to the private sector estimates, the illegal use of cryptocurrencies makes up a small part of their overall use. Namely, only 0.34% of cryptocurrency transactions are related to illegal use. According to the academic community estimates, 23% of total transactions pertain to the illegal use of cryptocurrencies, which is a significantly higher share compared to the private sector estimate. The reason for this discrepancy in estimates should be partly sought in different approaches to conducting research. Even though the share of illegal use of cryptocurrencies in criminal activities has decreased compared to their legal use (because the share of legal use is growing much faster than the share of illegal use), it should be noted that the tendency of illegal use of cryptocurrencies is growing (Europol, 2021, pp. 4-5).

Members of organised crime soon realised all the advantages of using cryptocurrencies in their activities. Cryptocurrencies are used to facilitate criminal activities in the context of drug trafficking, human trafficking, and the import and export of illicit products, fraud and money laundering. Members of state authorities realised that it was necessary to take additional steps to prevent the activities of criminal groups in a newly established field. In this regard, for example, the Italian politician Lucrezia Ricchiuti started a discussion about the mafia's connections with gambling and cryptocurrencies. She claimed that the mafia launders illegal money through gambling sites by using digital currencies that are anonymous and often cannot be tracked. Therefore, it is necessary to work on preventing such activities, because the lack of control and the absence of criminal liability inevitably leads to gambling being a safe place for money laundering by the mafia (Jones, 2018, p. 2).

According to the report of the blockchain data company Chainalysis, criminals laundered 8.6 billion US dollars (6.4 billion pounds) of cryptocurrency in 2021, which is 30 % more than the previous year. One of the

reason for the significant increase in money laundering should be sought in the fact that criminal networks specialising in large-scale money laundering have adopted cryptocurrencies and offer their services to other criminals (Chainalysis, 2022, p. 2). In addition, Europol has seen an increase in the use of cryptocurrencies in money laundering schemes, especially during the COVID-19 pandemic. Criminals used the so-called ransomware, a type of malicious software that restricts access to a computer system or stored data, and demands ransom from the victim in order to obtain cryptocurrencies from the victim. However, money earned from trafficking in psychoactive substances and converted into cryptocurrencies for the purpose of laundering is not included in the report, which suggests that the volume of money laundering by using cryptocurrencies is significantly higher. This claim may be supported by the example of a criminal group from Northern England that distributed drugs to dealers. The money laundering scheme operated as follows: first, a courier would take cash from the dealer and take it to a broker; then, the broker would buy certain cryptocurrency, and send it to an address previously designated by the criminal group. Notably, the broker's fee was 4%, which is fairly low when compared to a broker's fee in more traditional forms of money laundering. It shows that money laundering based on cryptocurrencies has a great profit-making potential. Consequently, we may reasonably fear that such criminal activity will increase in the period to come. Another reason for the expected increase is the quick and easy conversion of one cryptocurrency into another, which makes it impossible to monitor cash flows (BBC, 2022).

In addition to money laundering, there are a number of scams involving cryptocurrencies. Namely, according to Europol's estimates, fraud related to cryptocurrencies is the most common crime committed in the illegal use of cryptocurrencies. Cryptocurrency investment fraud schemes have been identified in several countries across the European Union. Fraudsters create fake websites intended for investments in cryptocurrencies, or advertise lucrative investments and encourage investors to create accounts on online trading platforms. At the same time, victims of fraud are convinced that they can track their investments thanks to the platform they used to invest money. On the platform itself, cryptocurrency trading is simulated in order to gain the investors' trust, including the inevitable use of social engineering techniques by brokers. There have been cases of fraudsters using social networks to advertise their Internet platforms by using fake messages from public figures. For example, the Australian mining magnate Andrew 'Twiggy' Forrest filed a criminal complaint against Facebook because it "failed to prevent false cryptocurrency advertisements that used his image" (Independent, 2022). Fraudsters also ask investors to invest money in order to launch a new cryptocurrency, which is expected to bring huge profits in the future but which does not actually exist. Another technique for extracting money is the so-called pyramid scheme, where in-

vestors are promised high returns which will come from new investors they are expected to bring into the game; thus, while "the increase in value promised to investors is just an illusion, any disbursements to investors are merely funds transferred from investors who are further down the pyramid structure" (Europol, 2021, pp. 13-15).

The best evidence of the dangers of cryptocurrency fraud are examples from practice. In July 2021, an interesting case was recorded in the Republic of Serbia. More than a dozen of Serbian hackers were suspected of and charged with cryptocurrency-related fraud. Although they were citizens of several states (Serbia, Montenegro, Australia and the Philippines), they all had their place of residence in the City of Niš (Južne vesti, 2020). They were suspected of targeting people around the world, urging them to invest money in fake cryptocurrency mining. They launched more than 20 fake cryptocurrency investment and trading platforms. They advertised themselves as world leaders in the binary options market, claiming that investors could expect a profit of as much as 80% of the amount of invested money. They created fake profiles of fake companies' personnel, fabricated trade activities, and held online conference meetings in order to convince potential investors that the company was legitimate. In case a person decided to invest money, he/she was instructed to transfer money via an international bank account, and was directed to monitor the investment via a fake online investment platform, which showed a positive return on investments. It is assumed that they managed to collect over 70 million dollars. All these facts indicate that their fraudulent scheme was well-established (Sloboden pečat, 2021).

Drug trafficking is another crime which has undergone certain changes in terms of *modus operandi*. At the beginning of discussing possible uses of cryptocurrencies in criminal activities, we presented the example of the Silk Road platform and its founder Ross Ulbricht, but other drug traffickers soon realised all the advantages of using cryptocurrencies. Thus, in order to provide a better insight into the prevalence of this form of trading in narcotics, we should explore some other examples as well. First of all, we may refer to the estimates of the US Government Accountability Office (GAO), which reported that between 80 and 90% of all illegal sales on the so-called dark web (part of the Internet network that can be accessed only by using specific software, configuration or permission) are related to illegal drugs, while all transactions are performed by using cryptocurrencies (Forbes, 2022). At the same time, it should be pointed out that many drug traffickers do not use the dark web because the use of cryptocurrencies provides them with sufficient security that their transactions are very difficult to track. For example, a Bitcoin millionaire Aaron Shamo, started 'mining' in 2009, soon after Bitcoin was created, and the value of his property soon grew to 10 million dollars. Yet, state authorities suspected that part of his wealth was generated by illegal activities. In 2016, he was ar-

rested and accused of trafficking the deadly opioid fentanyl from China, financing operations with Bitcoins, and funding a vast underground drug trafficking organisation that distributed more than a half million counterfeit pills on the dark net. Shamo and five of his friends were considered to be part of a new generation of 'entrepreneur' criminals who buy and sell drugs online, covering their tracks by using cryptocurrencies. Procuring drugs from China, which entered the United States through the post office at the JFK airport in New York, they turned the Internet into one of the main arteries for fentanyl travel in the United States. In the fiscal year 2016, the volume of fentanyl trade was evidenced by the fact that customs officers detected seven shipments of fentanyl at the airport; in 2017, the number rose to 86 shipments and, in 2018, they seized 146 shipments. Drug addicts soon realised that it was possible to get drugs delivered to a home address via US postal services, which resulted in 20,000 people dying from fentanyl overdose in 2016 alone (CNBC. 2018). In 2019, Shamo was found guilty and sentenced to life imprisonment (US Department of Justice, 2020).

In addition to trafficking in psychoactive substances, criminals have begun to use cryptocurrencies in human trafficking. It was only in the last decade of the 20th century that the international community took the first systematic steps to combat this form of crime (Konstantinović Vilić, Nikolić Ristanović, Kostić, 2012, p. 205). Two decades later, additional efforts are needed to fight human traffickers because the contemporary tech-savvy generations use cryptocurrencies to make it even more difficult for competent state authorities to track these illicit activities and take appropriate measures.

It is estimated that trafficking in human beings generates about 150 billion dollars per year, which makes it one of the most profitable criminal activities. In this regard, an international body called the Financial Action Task Force (FATF), based in Paris, estimated that about 24.9 million people are subjected to forced labour and sexual exploitation at any given time, which indicates the great possibilities of using cryptocurrencies in human trafficking (FATF, 2018, p. 9). Thus, the Financial Crimes Enforcement Network (FinCEN) pointed out that members of organised criminal groups involved in human trafficking are increasingly using 'alternative' payment mechanisms, including cryptocurrencies (GAO, 2021). At the same time, according to the US GAO estimates, in the period between 2017 and 2020, transactions in cryptocurrencies related to human trafficking quadrupled. During the same four-year period, the tax administration identified six investigations involving virtual currency that were linked to human trafficking (GAO, 2021, pp. 27-28). In the future, a real explosion of human trafficking that includes the use of cryptocurrencies can be reasonably expected to occur.

Cryptocurrencies have also found their application in child pornography. During 2019, a non-governmental organisation called the Internet Watch Foundation (IWF) confirmed the existence of 132,676 URLs or websites with child sexual abuse content on 4,956 domains traced to 58 countries, which constitutes an increase of 27% when compared to the year 2018. In 2019, there was a new increase in the number of websites on the dark net as the IWF identified 288 new dark web sites with child pornography. In 2018, the IWF identified a significantly smaller number of such websites (85). Comparing the number of websites on the dark net in these two years, an increase of 238% can be noted. Interestingly, 197 of the 288 sites identified in 2019 accepted only cryptocurrency payments to allow the users access to their content. This is precisely an indication of how cryptocurrencies can be used for another illegal purpose. The true extent of using cryptocurrencies to provide access to the contents of child pornography websites may be illustrated by the available data. In 2019, Chainalysis tracked payments (in the total amount of slightly less than 930,000 US dollars) effected in cryptocurrencies to web addresses related to child pornography. Thus, in 2019, there was an increase of 32% when compared to 2018; in turn, in 2018, there was an increase of 212% when compared to 2017 (ICMEC, 2021, p. 4).

In order to illustrate how criminals use cryptocurrencies in child pornography, we may refer to a case from judicial practice. In October 2019, the US Department of Justice filed an indictment against a 23-year-old South Korean citizen, Jong Woo Son, who was accused of running a dark web site exclusively dedicated to child pornography. He founded the site in 2015, and only three years later, he had over 200,000 video files on his server. He allowed its users to create free accounts on the site and download the contents by using points. The site users purchased points with Bitcoin, or earned points by recommending the website to new users and by posting videos with child pornography, which only increased the number of users and the hours of video recordings. During its three-year operation, the website received 420 Bitcoins and had over 7,300 transactions worth over 370,000 US dollars at the time of the respective transactions, which means that the profit increased over time as the value of Bitcoin grew. Jong Woo Son was identified by an undercover investigator who sent Bitcoins to the Bitcoin addresses listed on the website. Within a few days, Son transferred the cryptocurrencies to another address that was linked to his account at an online exchange office. The indictment also covered more than 337 users living in the United States and 11 other countries. As a result, over 250,000 videos were removed from the website (ICMEC, 2021, pp. 6-7).

Another interesting case occurred in the United States in March 2020, when 32-year-old Dutch citizen Michael Rahim Mohammad was indicted for running a website, *DarkScandals*, featuring child pornography on the dark net (since 2012). Users could access the website content either

by paying in cryptocurrencies or by uploading their videos of sexual abuse of children. The scale of the illegal activity may be illustrated by the fact that the site contained over 2,000 videos and images of sexual exploitation of children, and received 188.6 Bitcoins worth approximately 1.6 million US dollars at the time, as well as 26.7 Etheriums worth approximately 5,730 US dollars. Many of the virtual currency addresses linked to this site were primarily used for paying for the website's content, but many of them were also used for paying for other illegal activities on the dark net, such as purchasing narcotics, stolen data, and other illicit products. The site founder was identified because he made a mistake; namely, he instructed the site users to send payments in cryptocurrencies to specific crypto addresses, and then he used his identification data to create bank accounts in order to convert cryptocurrencies into money (ICMEC, 2021, pp. 9-11). All these transactions clearly illustrate the social danger of activities committed by using cryptocurrencies.

The US judicial practice illustrates that cryptocurrencies have also been used as a means of paying a hired hit-man to commit murder. The first suspicion that Biotcoin was used for these purposes was related to Ross Ulbricht, the founder of the Silk Road website; the investigators retrieved private messages from the server about paying hit-men a total of 650,000 US dollars to kill several people, but the prosecution could not prove the execution because the victims' bodies were never found (Wired, 2015). Soon, there were several other cases where cryptocurrency was used to pay the hit-men. In 2016, Kristy Lynn Felkins (aged 37) used the dark web *Besa Mafia* platform to order the murder of her ex-husband. She paid 12 Bitcoins, worth 5,000 US dollars, for the hit-man's services, provided precise information about the target's whereabouts, and even suggested that the hit-man could stage it as a robbery (while she was out of town). The case was discovered when federal investigators received information that a person named "KBGMKN" (who turned out to be Felkins) commissioned a murder. This platform offered various illegal services (including murder, kidnapping and assault) in exchange for cryptocurrency payments, but it should be noted that the platform was designed by fraudsters to entice as many people as possible to pay them in cryptocurrencies, while the services were never performed (Oxygen, 2022). In another similar case, a US citizen, Nelson Replogle, hired a hit-man to kill his wife and sent a Bitcoin to the potential killer, together with a description of his wife's car and the time when she would be out of the house. The murder was not committed because the FBI investigators reacted in time. They analysed the Bitcoin blockchain, established that the Bitcoin was stored in the Coinbase platform, and obtained information from Coinbase about the account, transaction history, Replogle's name, photo and internet address, but they could not locate the hit-man (Decrypt, 2021).

The greatest danger of using cryptocurrencies in illegal activities is related to terrorism. The use of cryptocurrencies by terrorist groups enables them to expand the scope of activities which do not necessarily have to be confined to one territory, particularly in terms of providing logistics and finances, so that their activities may be performed in other territories. Namely, the use of cryptocurrencies enables a rapid distribution of funds to other regions, while facilitating the recruitment process and reducing the role of intermediary terrorist organisations. It may be reasonably assumed that the traditional methods of financing terrorism will always exist; however, the digitalisation of money, and particularly the increasing use of cryptocurrencies, will significantly complicate the work on preventing terrorist attacks (Hassan, Nafees, 2022). To illustrate the difficult task of preventing terrorism when digital money is used as a financial tool, we may refer to some examples. As shown in the research on the financing of 40 Jihadi terrorist cells in Europe, in the period between 1994 and 2014, terrorists raised money from territories under their control (e.g. the Islamic State), from their own resources (self-financing), and by illegal trade in drugs, weapons and other goods. The results show that that terrorist acts in Europe were inexpensive in a large number of cases, as it was estimated that one attack cost less than 10,000 US dollars (Oftedal, 2015, p. 45). In the past years, many terrorist groups have adapted to greater state control and a greater use of digital money. Now, they raise funds through legal sources and methods that are difficult to associate with terrorism. The use of digital currency makes both legal and illegal financial transaction harder to detect. Moreover, money kept in personal digital currency accounts does not raise much suspicion from government agencies (Dimovski, 2021, pp. 230-231). Starting from the fact that state authorities are powerless in the prevention of terrorist acts financed with digital money, counteracting terrorism is further frustrated when terrorist groups use cryptocurrencies. Terrorist groups always endeavour to develop strategic advantages in relation to state authorities. In the future, one of these advantages will be cryptocurrencies, as a 'lucrative alternative mode of financing' their activities, particularly given the anonymity in financial transactions, lack of regulations, and insufficient control of the state apparatus. In that context, the Philippine Institute for Peace, Violence and Terrorism Research (PIPTVR) reported that a local terrorist group, supported by the Islamic State, carried out the first cryptocurrency transaction in May 2020 in order to fund its activities in the conflict-stricken region of Mindanao in the southern Philippines (Hassan, Nafees, 2022).

At the same time, there are platforms on the dark net, such as *Finance Islamic Fight without leaving a trace*, through which one can transfer cryptocurrencies to jihadists in order to finance their terrorist activities. Interestingly, one extremist published a book called *Bitcoin wa Sadaqat al Jihad,* where he explains how to make the transfer of North American and

Western European Bitcoin to jihadists. In June 2015, an American teenager admitted that he taught members of the Islamic State how to use Bitcoin, by giving them guidelines on how to make Bitcoin wallets for potential donors. Shortly afterwards, terrorist organisations started using cryptocurrencies to finance terrorist attacks. Bahrun Naim, the organiser of the terrorist attacks in Jakarta in 2016, used Bitcoin for virtual payments, transfer of funds to armed units, and financing terrorist activities (Wang, Zhu, 2021, p. 2330). It was also revealed that members of the Islamic State demanded payment in Bitcoin as a ransom for the kidnapped people, and they used the collected funds to further finance their terrorist activities. Studies have shown that whenever traditional ways of raising money to finance terrorist activities were in jeopardy, terrorists always turned to cryptocurrencies. Although the Islamic State, Al Qaeda and Hezbollah continue to dominate traditional ways of raising money, cryptocurrencies are increasingly being used for financing terrorist activities. Thus, the use of cryptocurrencies for these purposes may be reasonably expected to increase in the future, provided that the *status quo* is preserved in terms of the characteristics of cryptocurrencies and their (currently high) values. In addition, it is essential to improve the existing infrastructure of ATMs (automated teller machines for withdrawing money) where users can exchange cryptocurrencies for cash, because the existing ATM infrastructure is particularly bad in areas where terrorist groups operate in the Middle East (Wang, Zhu, 2021, pp. 2333-2334).

CONCLUSION

The analysed criminal law areas indicate that all comparative advantages of cryptocurrencies have started to be used in the commission of many forms of crime. It should be noted that it is necessary to conduct organised and systematic criminological research which should provide a broader and more detailed picture of the actual scope of the use of cryptocurrencies in criminal activities. Once the cryptocurrency market was established, some criminals saw the advantages of cryptocurrencies and their profit-making potential. The owner of the Silk Road platform, Ross Ulbricht, who earned over one billion dollars from drug trafficking, was discovered because he made a mistake when creating the site – he left a job ad using an IP address instead of using the Tor browser, which ensures anonymity and makes transactions almost impossible to detect (BBC, 2013).

Following this case, there has been a rapid increase in the use of cryptocurrencies, not only in drug trafficking but also in many other criminal activities. Organised criminal groups started using cryptocurrencies in activities such as human trafficking, kidnapping, and gambling. The situation was further aggravated when cryptocurrencies started being used by

terrorist groups; the intrinsic characteristics of cryptocurrencies (anonymity, ease of access, speed of transactions, easy storage and transfer, and lack of control) have made it much more difficult for competent authorities to fight against criminal activities involving the use of cryptocurrencies. To this effect, it is essential to start coordinated operations in countries throughout the world as soon as possible. It is the only way to preclude the expansion of the use of cryptocurrencies in criminal activities. Another issue of particular concern is the fact that cryptocurrencies facilitate the commission of the most serious crimes by individuals, including murder, because one may easily hire a hit-man who is paid in cryptocurrencies. As shown in this paper, these financial transactions are rather difficult to trace, and the competent state authorities encounter many challenges, not only in terms of crime detection but also in prosecuting the perpetrators and other responsible persons.

There is no doubt that the Republic of Serbia is also facing the problem of criminal activities committed by using cryptocurrencies. In many countries, including Serbia, the use of cryptocurrencies is still under-regulated and insufficiently controlled. Although cryptocurrency has been legally recognised under the Digital Property Act (2020) as digital property, which may be used as a means of exchange for investment purposes (BBC News, 2021), this Act does not regulate a range of criminal offences that may be committed by using cryptocurrencies. In the future, we may reasonably expect a further increase in the use of cryptocurrencies in the commission of criminal activities. Therefore, competent state authorities should prepare and adjust their activities in order to adequately face the great challenges in the fight against the use of cryptocurrencies for criminal purposes.

ACKNOWLEDGEMENTS. This research was funded by the Ministry of Education, Science and Technological Devlopment of the R. Serbia (project ref. no. 451-03-68/2022-14/200120).

REFERENCES

BBC (2013). Silk Road: How FBI closed in on suspect Ross Ulbricht**,** D. Lee**,** 2 October 2013; Retrieved 10 April 2022 from: https://www.bbc.com/news/technology-24371894

BBC News (2021). Kriptovalute i Srbija: Šta donosi Zakon o digitalnoj imovini (Cryptocyrencies in Serbia: the Digital Property Act), S. Maksimovic, BBC News na srpskom, 1 jul 2021; Retrieved 10 April 2022 from: https://www.bbc.com/serbian/lat/srbija-57681737

BBC/British Broadcasting Corporation (2022). Crypto money laundering rises 30%, report finds, 26 Jan. 2022; Retrieved 2 April 2022 from: https://www.bbc.com/news/technology-60072195

Chainalysis (2021): Lazarus Group Pulled Off 2020's Biggest Exchange Hack and Appears to be Exploring New Money Laundering Options,9/2/2021, Retrieved 01 April 2022 from: https://blog.chainalysis.com/reports/lazarus-group-kucoin-exchange-hack/

Chainalysis (2022): The 2022 Crypto Crime Report, Chainalysis, UK, https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/

CNBC (2018). How bitcoin is fueling America's opioid crisis, April 13, 2018; Retrieved April 3, 2022 from: https://www.cnbc.com/2018/04/13/how-bitcoin-and-cryptocurrencies-are-fueling-americas-opioid-crisis.html

Cognyte (2021): **5** Reasons Why Criminals & Terrorists Turn to Cryptocurrencies, T. Sadon, 2 /11/ 2021, Retrieved 30 March 2022 from: https://www.cognyte.com/blog/5-reasons-why-criminals-are-turning-to-cryptocurrencies/

CoinDesk (2021): Cross-Chain DeFi Site Poly Network Hacked; Hundreds of Millions Potentially Lost, E.Gkritsi, M.Shen, 9/10/2021; Retrieved 01 April 2022 from: https://www.coindesk.com/markets/2021/08/10/cross-chain-defi-site-poly-network-hacked-hundreds-of-millions-potentially-lost/

Decrypt (2021). Man Used Coinbase to Pay Hitman in Bitcoin for Wife's Murder, FBI Says, May 10, 2021; Retrieved 7 April 2022 from: https://decrypt.co/70420/man-used-coinbase-hitman-bitcoin-fbi

Dimovski, D., (2021). Prevencija kriminaliteta putem digitalizacije [Crime Prevention through Digitalization], *Zbornik radova Pravnog fakulteta u Niš*u, vol. 60, br. 91/2021, str. 227-242.

Europol (2021). Cryptocurrencies: tracing the evolution of criminal finances, Europol Spotlight Report series, Publications Office of the European Union, Luxembourg, https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf

FATF/Financial Action Task Force (2018). Financial Flows from Human Trafficking, FATF Report, Paris; https://www.fatf-gafi.org/media/fatf/content/images/Human-Trafficking-2018.pdf

Forbes (2022). Crypto Increasingly Used In Human/Drug Trafficking Says GAO, Ted Knutson, Jan 10, 2022; Retrieved 03 April 2022 from: https://www.forbes.com/sites/tedknutson/2022/01/10/crypto-increasingly-used-in-humandrug-trafficking-says-gao/?sh=cfdebe8637eb

GAO/US States Government Accountability Office (2021). Virtual Currencies: Additional Information Could Improve Federal Agency Efforts to Counter Human and Drug Trafficking, (2021). US Government Accountability Office; Retrieved 04 April 2022 from: https://www.gao.gov/products/gao-22-105462; https://www.gao.gov/assets/gao-22-105462.pdf

Hassan, A.M., Nafees, S.N. (2022). Cryptocurrency and Terrorist Financing in Asia, *The Diplomat*, Feb. 4, 2022; Retrieved 8 April 2022 from: https://thediplomat.com/2022/02/cryptocurrency-and-terrorist-financing-in-asia/

ICMEC/International Centre for Missing & Exploited Children (2021). Cryptocurrency and the Trade of Online Child Sexual Abuse Material, the International Centre for Missing & Exploited Children; https://cdn.icmec.org/wp-content/uploads/2021/03/Cryptocurrency-and-the-Trade-of-Online-Child-Sexual-Abuse-Material_03.17.21-publish-1.pdf

Independent (2022). Australian billionaire launches criminal case against Facebook over false crypto ads, 03 February 2022; Retrieved 2 April 2022 from: https://www.independent.co.uk/tech/facebook-australian-billionaire-forrest-crypto-b2006597.html

Investopedia (2022): What Is Bitcoin? J. Frankenfield (updated June 13, 2022); Retrieved 28 March 2022 from: https://www.investopedia.com/terms/b/bitcoin.asp; https://www.investopedia.com/terms/c/cryptocurrency.asp

Jones, J. (2018). Digital Currencies and Organised Crime Update, Faculty of Business and Law, University of the West of England, Bristol

Konstantinović Vilić, S., Nikolić Ristanović, V., Kostić, M. (2012). Kriminologija [Criminology], Pravni fakultet u Nišu, Niš

Milutinović, M. (2018). Cryptocurrency [Cryptocurrency], Ekonomika, Niš, Vol. 64, 2018, № 1

Minović, M. (2017). Blockchain tehnologija: mogućnosti upotrebe izvan kripto valuta [Blockchain Technology: possible use outside cryptocurrencies], Fakultet organizacionih nauka, Beograd

Oftedal, E. (2015). The Financing of Jihadi Terrorist Cells in Europe, Norwegian Defence Research Establishment (FFI), 6 January 2015, https://www.ffi.no/en/publications-archive/the-financing-of-jihadi-terrorist-cells-in-europe

Oxygen (2022). Woman Pleads Guilty to Paying a Dark Web Hitman Ii Bitcoin to Murder Her Ex-Husband, March 18, 2022; Retrieved 7 April 2022 from: https://www.oxygen.com/crime-news/kristy-felkins-guilty-bitcoin-murder-for-hire

Poper, N. (2017). Digitalno zlato [Digital Gold], Laguna, Beograd

Sloboden pečat (2021). A prison awaits them in Texas: A group of Serbian hackers shook America, made a global fraud worth $70 million, 4. Feb.2021, Sloboden pečat/Free Press; Retrieved 2 April 2022 from: https://www.slobodenpecat.mk/en/gi-cheka-zatvor-vo-teksas-grupa-srpski-hakeri-ja-zatresoa-amerika-napravija-globalna-izmama-teshka-70-milioni-dolari/

Statrys (2021): 8 Reasons Why Your Bank Transfer is Delaye, B. Ozanne, 27/9/2021; Retrieved 30 March 2022 from: https://statrys.com/blog/delayed-bank-transfer

US Department of Justice (2021). Shamo Sentenced To Life In Prison After Conviction For Organizing, Directing Drug Trafficking Organization, US Attorney's Office, District of Utah, Press release, October 15, 2020: Retrieved 3 April 2022 from: https://www.justice.gov/usao-ut/pr/shamo-sentenced-life-prison-after-conviction-organizing-directing-drug-trafficking

Wang, S., Zhu, X. (2021). Evaluation of Potential Cryptocurrency Development Ability in Terrorist Financing, Policing, Oxford University Press, Oxford, Volume 15, Number 4

Wired (2015). Read the Transcript of Silk Road's Boss Ordering 5 Assassinations, February 2, 2015, Retrieved 7 April 2022 from: https://www.wired.com/2015/02/read-transcript-silk-roads-boss-ordering-5-assassinations/

Zakon o digitalnoj imovini (Digital Property Act), Službeni glasnik RS, br. 153/2020

КРИПТОВАЛУТЕ И КРИМИНАЛИТЕТ

Дарко Димовски
Универзитет у Нишу, Правни факултет, Правосудни истраживачки центар, Ниш, Србија

Резиме

Биткоин, створен 2009. године од стране Сатошиа Накамота, је прва криптовалута чија се сврха огледа у обављању трансакција без икаквих надокнада, при чему њоме не управља нека централна власт. Како бисмо боље разумели шта се

подразумева под биткоином, али и другим криптовалутама које су убрзо након тога креиране, неопходно је одредити шта се под криптовалутама подразумева. Може се рећи да су криптовалуте дигитална или виртуелна валута која је заштићена криптографијом, што фалсификовање или дупло трошење чини готово немогућим. Криминалци су схватили да је криптовалуте могуће користити за обављање нелегалних активности. Наиме, постоје одређени разлози из којих се криминалци опредељују за што чешћу употребу криптовалута. Ти разлози се огледају у постојању анонимности, непостојању посредника, могућности вршења преноса у било које време, лакшем складиштењу и преносу, и непостојању граница. С тим у вези, криминалци широм света су почели да користе криптовалуте за обављање криминалних активности. Стога криптовалуте се користе за олакшавање криминалног пословања у оквиру трговине наркотицима, трговине људима, и увоза и извоза недозвољених производа. Поред тога криптовалуте се користе за прање новца, што је нарочито интензивирано за време трајања пандемије вируса ковид-19. До експанзије употребе криптовалута дошло је и код кривичних дела преваре, при чему се штета мери у више десетина милиона долара. Исто тако, употреба криптовалута је знатно олакшала трговину наркотицима, али и трговину људима. Уједно, корисницима дечије порнографије су криптовалуте омогућиле знатно већи степен анонимности, што је довело до повећања броја интернет сајтова са дечијом порнографијом. Криптовалуте су коришћене и као начин исплате зарад извршења убистава. Највећи степен друштвене опасности забележен је код извршења терористичких аката, јер употреба криптовалута омогућава брзу дистрибуцију финансија у друге регионе. На основу изложеног, може се очекивати даљи пораст употребе криптовалута у наведеним активностима, али и њена употреба и у другим активностима криминалаца, што ће захтевати даље прилагођавање државних органа у борби против нелегалне употребе криптовалута.