The Impact of Misuse of Cryptocurrencies in Combating Money Laundering and Terrorist Financing

Dr. Zoran S. Pavlovic*
Nikola Paunovic*

Abstract

Cryptocurrencies are designed as a secure form of financial transaction via the Internet. However, the development of information and communication technology has created new space for their misuse in criminal purposes, especially in the area of money laundering and terrorist financing. Bearing in mind the complexity in conducting financial transactions via the Internet, the paper in the first part deals with most important legal challenges regarding the misuse of cryptocurrencies through money laundering and terrorist financing. Furthermore, in the second part of the paper, the most relevant crime detection methods are considered. Finally, the practical challenges at the level of the protection of financial transactions against their misuse in criminal purposes, have created a need for normative regulation of cryptocurrencies, which is why last part of this paper includes the analysis of the relevant legal framework in this area at international, European or national level. In the concluding remarks, the key recommendations for better legal protection of the cryptocurrency transactions are provided, since it is noticed that although the cryptocurrency financial transaction system has created opportunities for relatively secure financial operations in a digital environment, there is still space for improvement.

Keywords: *cryptocurrencies, money laundering, terrorist financing, detection, phenomenological forms, legal framework*

I. Introduction

Cryptocurrency is the latest topic of discussion in the financial world[1]. The term cryptocurrency refers to currencies, which rely upon cryptogenic algorithms to ensure network and transactional validity, and are distributed over the Internet, but are not issued by any centralized source. The first decentralized cryptocurrency created in 2009 was Bitcoin. Since then, numerous other cryptocurrencies have been created. All

* Professor of Criminal law, Chairman of the Department for Criminal Law, Faculty of Law University Business Academy Novi Sad, Ombudsman of the Autonomous Province of Vojvodina, Republic of Serbia. Contact: zoran.pav@hotmail.com.

* Research Assistant, Attaché at Ministry of Foreign Affairs, Republic of Serbia, Ph.D. Student, The University of Belgrade, Faculty of Law. Contact: dzoni925@gmail.com.

[1] K., Sontakke, A., Ghaisas, „Cryptocurrencies: A Developing Asset Class“, *International Journal of Business Insights & Transformation*, No. 2, 2017, 10.

of these currencies are distinguished from other virtual currencies such as e-Gold, Amazon, Tokens that are exchanged solely through the Internet, but are also issued and controlled from a centralized source[2]. Foremost type of decentralized cryptocurrencies is Bitcoin. The issuance of this currency is computer-programmed and limited, based on peer-to-peer technology and data encryption technology, which practically eliminates the possibility of double-spending, counterfeiting and similar abuses. At the same time, this is one of the main reasons why this currency is considered safe, even though there is no central issuing institution[3].

On the other side, cryptocurrencies such as bitcoin allows criminals to generate, transfer, launder, and steal illicit funds with anonymity. Accordingly, the first fact that disables as well as makes it difficult to detect the misuse of cryptocurrencies is variety of obliged entities included in the cryptocurrencies transactions. Thus, there is a *cryptocurrency user* which means a natural person or legal entity who obtains coins either to use them to purchase real or virtual goods or services, as well as to make peer-to-peer payments, or to hold them for investment purposes i.e. in a speculative manner. Second player is the so-called *cryptocurrency exchanger* which means the person or entity who offer exchange services to cryptocurrency users, usually under payment of a certain fee (i.e. a commission), allowing them to sell their coins for fiat currency or buy new coins with fiat currency. In this regard, it should be mentioned coin inventors and offerors. *Coin inventors* are individuals or organizations who have developed the technical foundations of a cryptocurrency and set the initial rules for its use. Moreover, there are *coin offerors* meaning individuals or organizations that offer coins to cryptocurrency users. Another player is *wallet provider* who provides cryptocurrency users digital wallets or e-wallets which are used for holding, storing and transferring coins. In this sense, there are two types of wallet providers. On the one hand, there is *hardware wallet provider* which provides cryptocurrency users with specific hardware solutions to privately store their cryptographic keys (e.g. Ledger Wallet). On the other side, exists *software wallet provider* which provides cryptocurrency users with software applications allowing them to access the network, send and receive coins and locally save their cryptographic keys. Furthermore, there is *custodian wallet providers* who takes online custody of a cryptocurrency user's cryptographic keys. Finally, there is *miner* who participates in validating transactions on the blockchain technology by solving a cryptographic puzzle[4].

Furthermore, the second thing that disables as well as makes it difficult the detection is reflected in fact that there are a lot of phenomenological forms in which perpetrators can misuse the cryptocurrency transactions. In other words, the misuse of cryptocurrency transactions may involve various forms of fraud, corruption crimes, as well as organized crimes[5]. However, taking into account the fact that all mentioned forms could not be analyzed in this article, the focus should be put on the most

---

[2] T. Bierer, „Hashing It Out: Problems And Solutions Concerning Cryptocurrency Used As Article 9 Collateral", *Journal Of Law, Technology & The Internet*, Vol. 7, 2016, 81.

[3] V. Dinić, „Bitcoin as a decentralized currency", *Bankarstvo* No. 2 2014, 135.

[4] R. Houben, A. Snyers, *Cryptocurrencies and blockchain, Legal context and implications for financial crime, money laundering and tax evasion*, European Parliament, Brussels, 2018, 25-28.

[5] Z., Pavlović, „Institutional Capacities of the Republic of Serbia for Opposing Organized Criminal, Terrorism and Corruption", *Proceedings from scientific conference Financial Crime (Ed. J. Kostić, A. Stefanović)* Institute of Comparative Law and Institute of Criminological & Sociological Research, Zrenjanin, 2018, 58.

prevalent examples of criminal offenses by which it is manifested the misuse of the cryptocurrencies transactions. In that context, in the following lines it will be analyzed two criminal offences: money laundering and terrorist financing focusing the legal challenges regarding the qualification of alleged criminal activities.

Finally, the last thing that disables as well as makes it difficult the investigation of the cases concerning the misuse of cryptocurrencies is a lack of comprehensive normative regulation at international, European as well as national level. However, bearing in mind some achievements in this field in recent period in this article it will be considered the legal framework concerning the misuse of cryptocurrencies through money laundering and terrorist financing.

II. Legal Challenges Regarding the Misuse of Cryptocurrencies Through Money Laundering and Terrorist Financing

One of the major goals of every criminal investigation is to provide a proper qualification of alleged criminal activities to corresponding provisions of substantive criminal law, i.e. to define the elements of crime. Some new forms of criminal activity such as misuse of virtual currencies may call for the need to re-think and re-adjust currently available substantive criminal law options to real-life cases. Cybercrime aspects of the misuse of virtual currencies can manifest themselves in a multitude of ways. Standalone offences of cybercrime that are connected with virtual currencies, may not be, at a first glance, particularly relevant for the investigations focusing on laundering of crime proceeds. On the other side, reality shows that such offences which involve money-laundering by use of virtual currencies may be connected to criminal proceeds derived from forms of cybercrime such as computer-related identity offences, or computer-related fraud or forgery. Therefore, cybercrime offences may be deemed as predicate offences to money-laundering. In this case, investigations will be relying on cybercrime elements of crime to construct the offence of money-laundering. In this regard, it is important to understand the nature of specific cybercrime offences, including illegal access, system interference, data interference and misuse of devices[6]. Cybercrime offences concerning the misuse of cryptocurrencies dominantly represent the predicate offenses of money laundering and terrorist financing.

Money laundering is a process of concealing the illicit origin of money or assets acquired through crime[7]. Precisely, it means the process of conversion or transfer of illegally derived property, by concealing or disguising the illicit origin of that property, as well as eliminating traces of its acquisition, possession or use in order to integrate laundered proceeds into legal financial flows[8]. This crime has three essential stages. During the first stage, so-called *the investment* phase, the perpetrator breakdowns the

---

[6] United Nations Office on Drugs and Crime, Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies, United Nations Office on Drugs and Crime, 2014, 78-81.

[7] N. Važić, *„Pranje Novca- Materijalni I Procesni Aspektu Međunarodnom I Domaćem Zakonodavstvu", Bilten sudske prakse Vrhovnog suda Srbije, No. 2, 2008, 121-122.* See also, L., Cvitanović. et.al., *Kazneno pravo-posebni dio*, Pravni fakultet Sveučilišta u Zagrebu, 2018, 381-389.

[8] Z. Pavlović, „Fighting money laundering and control of real estate transactions*", Proceedings from scientific conference Financial Crime and corruption (Ed. J. Kostić, A. Stefanović) Institute of Comparative Law and Institute of Criminological & Sociological Research*, Vršac, 2019, 79-81.

direct link between money and the illegal activity through it has acquired, introducing the illegally acquired money into the financial system most often in the form of some legal activity in which payment is made in cash. After the money had entered the legal financial system in the second *concealment* stage it is transferred from the account to which it is placed on other accounts in order to hide the link between money and criminal activity from which it originates. Finally, in the context of the last *integration* stage, laundered money appears as money from some legal activity[9].

Furthermore, terrorist financing means providing or collecting funds, by any means, directly or indirectly, with the intention that they be used, or in the knowledge that they are to be used, in full or in part, to commit, or to contribute to the commission of, either terrorist offences or offences related to terrorist activities. The link between money laundering and terrorist financing is reflected in the fact that the second one crime could be the associated predicate offence of the first one. Precisely, financing terrorism is a preparatory action to secure or collect funds or assets, intending to be used or knowing that they can be used, in whole or in part, for the commission of a terrorist act by a terrorist or by terrorist organizations[10].

Like money laundering, terrorist financing also has several stages. The first phase includes the acts of the *collection of funds* derived either from the clandestine legitimate business of the entity that is connected or even guided by terrorist organizations or individuals or from criminal activities. A significant source of these funds is donations by individuals who support the goals of terrorist organizations, as well as charities funds that raise funds and channel them to terrorist organizations. In the second phase, the collected funds are *stored* in various ways, including banks accounts opened by intermediaries, individuals or companies. The third phase is the *transfer of these funds* to terrorist organizations or individuals for operational use, through the use of fund transfer mechanisms, such as international electronic transfers between banks or money remittances, the use of charity organizations, alternative systems or money transfer networks, through couriers or smuggling over state borders[11].

The use of virtual currencies such as bitcoin for money-laundering or terrorist financing purposes is going to highlight distinction between objective elements of crime (an act in itself, as well as objects and tools of crime) and subjective (intent, purpose, complicity etc.). The use of virtual currency as objective elements of these criminal offences can be brought down to the following aspects. In terms of placement, when criminally obtained funds are introduced in the financial circulation, the procurement of the virtual currency through an exchanger may be used as a relevant element of crime. In terms of layering (the process in which criminally derived funds are legalized and their ownership and source is disguised), the essential features of virtual currency can be brought forward as an element of money-laundering offence where the prosecution will be willing to prove the case that the virtual currency was selected precisely for these features, in order to conceal the criminal origin of funds. In terms of integration (the process by which the property legalized through layering is re-introduced into the economy), the use of virtual currency may be one of the

[9] B., Sinanović, „Pranje novca", *Bilten sudske prakse Vrhovnog suda Srbije*, No. 2, 2011, 63-64.

[10] D., Bolta „Sprječavanje financiranja terorizma", *Policija i sigurnost*, No. 4, 2010, 420. D., Derenčinović, The Review Of The Harmonisation Of The Croatian Criminal Law With International Legal Documents On Combating Terrorism, *Hrvatski ljetopis za kazneno pravo i praksu*, No. 2, 2003, 959; D., Derenčinović, et. al., *Posebni dio kaznenog prava*, Pravni fakultet Sveučilišta u Zagrebu, 2013, 32.

[11] N., Stanković *Terorizam i finansiranje terorizma*, Evropski Univerzitet Brčko, Brčko, 2014, 63-64.

elements, for instance if the laundered proceeds are re-invested into the virtual currency market, this may be an additional element of offence that can be used. On the other hand, in terms of proof of intent, as a subjective element of crime, which is an essential feature of money-laundering offences, focus should be on the following aspects of bitcoin. Firstly, anonymity and general lack of face-to-face interaction may be a valid proof of intent to commit offence related to illegal use of virtual currencies. Secondly, difficult traceability, including lack of paper/document trail can be specifically noted as element of intent. Finally, reliance on cryptography overall lack of regulation can be proven as a deliberate choice[12].

III. Crime Detection Methods of Money Laundering and Terrorist Financing Concerning the Misuse of Cryptocurrencies

In the context of the issue regarding virtual currencies, it should be noted that the development and widespread use of the Internet, personal computers, mobile devices, and related platforms and services, has had a vast impact on financial transactions[13]. The ability of new financial innovations to enable rapid cross-border payments presents elevated money laundering as well as terrorist financing risks. For that reason, financial institutions should identify the money laundering as well as terrorist financing risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products[14].

The anonymity of virtual currencies is considered the main risk in connection with the misuse of cryptocurrencies through money laundering or terrorist financing. In addition, international investigations, especially those involving advanced technology, can create challenges for law enforcement with respect to gathering evidence and information. The uncertain or non-existing legal instruments to trace, freeze and seize illicit virtual currencies that are related to illicit funds, can create an obstacle for law enforcement. Even though most virtual currencies leave a digital footprint, it might, in some cases, be challenging if not impossible to link the digital footprint to a physical person, especially if a person has extensive knowledge regarding covering key evidences[15]. While this means that law enforcement can utilize transaction monitoring technology, it again means many people using Bitcoin and cryptocurrencies already know that, and have driven the development of more anonymous currencies known as altcoins in response, or use techniques to further enhance their anonymity. This includes technology that masks identifying information on transaction ledgers, as well as the use of software like The Onion Router (Tor), known for its association with the Dark Web and online marketplaces like Silk Road, to anonymize a person's IP address[16].

---

[12] United Nations Office on Drugs and Crime, *op. cit.,* 85-86.

[13] T., Keatinge, D., Carlisle, F., Keen, *Virtual currencies and terrorist financing: assessing the risks and evaluating responses*, European Parliament, Brussels, 2018, 21.

[14] Financial Action Task Force, *International Standards On Combating Money Laundering And The Financing Of Terrorism & Proliferation- The FATF Recommendations*, Paris, 2016, 17.

[15] Office for Prevention of Laundering of Proceeds Derived from Criminal Activity, *Virtual currencies – Risks of Money Laundering and Financing of Terrorism*, Riga, 2019, 8-9.

[16] How Law Enforcement Catches Cryptocurrency Crimes, https://www.iannfriedman.com/blog/2019/february/how-law-enforcement-catches-cryptocurrency-crime/, Accessed 09.05.2020.

However, the truth is that cryptocurrencies like Bitcoin are not entirely anonymous. Bitcoin transactions are visible to all who use the network. Through the use of monitoring technologies that track transaction ledgers, there can be significant visibility of activity. The fact that Bitcoin transactions leave a trace is not enough to deter criminals since law enforcers are not able to immediately identify the parties involved in a Bitcoin transaction, but they can spot and study patterns in the movement of cryptocurrency to profile and de-anonymize suspects[17]. For example, no matter what cryptocurrency or concealment technology is used, a suspected criminal will need to eventually exchange their digital currency for real money. This can allow law enforcement to implement two main things: to **de-anonymize suspects** by stripping down of anonymity as well as to **detect unusual patters** by identifying unusual or suspicious behavior[18]. Therefore, the abovementioned has shown that, although difficult, the investigation of the ownership of digital currencies is not impossible.

Moreover, concerning the detection of the misuse of cryptocurrencies, it should be noted that digital currency networks usually record transactions in a distributed public ledger, which can be subjected to analytical monitoring tools capable of highlighting suspect transactions[19]. In this regard, the application of blockchain technology is required since it allows to make a link between bitcoin transactions and individual users taking into account the fact that these ledgers are public or open sourced, meaning that anybody can access or maintain these ledgers[20]. However, in some cases even where bitcoin, keeps an open, transparent ledger of all transactions available as open-source information, linking a specific transaction to individual users may require additional indicators from other sources such as i.e. virtual currency administrator or virtual currency exchange company located in one country but holding accounts in other countries where it does not have a significant customer base or the volume and frequency of cash transactions conducted by the owner of a virtual currency administrator or virtual currency exchange company do not make economic sense[21].

IV. Legal Framework Concerning the Protection Against Misuse of Cryptocurrencies Through Money Laundering and Terrorist Financing

1. Money laundering and counter-terrorism financing risks concerning criptocurrencies at the international level

In that regard, in 2014, the FATF took up the specific topic of virtual currencies linking cryptocurrencies with the anonymity risks because customer identification features such as name and address are not attached to a user's Bitcoin address, and because the system has no central service provider that has oversight of transactions and can be held accountable. According to the FATF's assessment, suspicious activity

[17] How Law Enforcement Catches Cryptocurrency Criminals, https://thenextweb.com/hardfork/2019/12/26/bitcoin-cryptocurrency-criminals-law-enforcement/, Accessed 09.05.2020.

[18] How Law Enforcement Catches Cryptocurrency Crimes, https://www.iannfriedman.com/blog/2019/february/how-law-enforcement-catches-cryptocurrency-crime/, Accessed 09.05.2020.

[19] International Centre For Asset Recovery, *Tracing Illegal Assets – A Practitioner's Guide*, Basel 2015, 115.

[20] K., Sontakke, A., Ghaisas, *op. cit.,* 11.

[21] United Nations Office on Drugs and Crime, *op. cit.,* 148-149.

may therefore not only be more difficult to detect, but the source of payments may be blurred in contrast to traditional credit or debit cards, or payment systems such as PayPal and Western Union. Since the existence of the anonymity risks in relation to cryptocurrencies, there are increasing concerns about the use of virtual currencies by terrorist organizations, especially with evidence of websites connected to terrorist organizations seeking Bitcoin donations or providing instructions of how to purchase weapons using Bitcoin[22]. For that reason, financial institutions should identify the money laundering as well as terrorist financing risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products[23].

2. Money laundering and counter-terrorism financing risks concerning criptocurrencies at the EU level

Directive (EU) 2018/843 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing constitutes the main EU legal instrument in the context of the detection and investigation misuse of virtual currencies through money laundering and terrorist financing[24]. This Directive introduces the definition of the following terms: 1) virtual currencies, 2) fiat currencies and 3) custodian wallet provider. The adoption of this Directive represents a significant step forward in the area of the protection of EU financial interests against misuse of cryptocurrencies for criminal purposes, bearing in mind the fact that providers engaged in exchange services between virtual currencies and fiat currencies as well as custodian wallet providers were under no Union obligation to identify suspicious activity, enabling terrorist groups to transfer money into the Union financial system or within virtual currency networks by concealing transfers or by benefiting from a certain degree of anonymity on those platforms. It was therefore essential to extend the scope of Directive (EU) 2015/849 so as to include providers engaged in exchange services between virtual currencies and fiat currencies as well as custodian wallet providers[25]. Namely, according to article 2 paragraph 1 of the amended Directive (EU) 2018/843 anti-money laundering and counter-terrorism financing framework has been extended so as to include providers of virtual as well as fiat currencies, and custodian wallet providers as the

---

[22] N., Paunović, Terrorist Financing As The Associated Predicate Offence Of Money Laundering In The Context Of The New Eu Criminal Law Framework For The Protection Of The Financial System, EU and Member States – Legal and Economic Issues, ed. (Duić, D, Petrašević, T., Novokmet, A.), Faculty of Law, Josip Juraj Strossmayer University of Osijek, Osijek, 2019, 670-671.

[23] Financial Action Task Force, *International Standards On Combating Money Laundering And The Financing Of Terrorism & Proliferation- The FATF Recommendations*, Paris, 2019, 15.

[24] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, Official Journal of the European Union, L 141/73 of 5 June 2015, (hereinafter: Directive (EU) 2015/849).

[25] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, Official Journal of the European Union, L 156/43 of 19 June 2018, (hereinafter: Directive (EU) 2018/843).

new obliged entities[26]. Precisely, amended Directive (EU) 2018/843 shall apply to the following obliged entities: a) providers engaged in exchange services between virtual currencies and fiat currencies; b) custodian wallet providers. For the purposes of this Directive, *virtual currencies* means a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically. On the other side, *fiat currencies* mean coins and banknotes that are designated as legal tender and electronic money, of a country, accepted as a medium of exchange in the issuing country. Finally, *custodian wallet provider* means an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies[27].

3. Money laundering and counter-terrorism financing risks concerning criptocurrencies at the national level

In the context of accession and negotiations process to EU, the Republic of Serbia has recently adopted the new framework concerning money laundering and terrorist financing, introducing new obliged entities of the importance against misuse of virtual currencies through money laundering and terrorist financing[28]. Thus, amended Serbian Law on money laundering and terrorist financing *in Article 4 point 17* recognizes as obliged entities *providers of virtual currencies* defining as persons providing the services of purchasing, selling or transferring virtual currencies or exchanging of such currencies for money or other property through internet platform, devices in physical form or otherwise, or which intermediate in the provision of these services[29]. However, it should be mentioned that Serbian law does not contain any further provision which defines virtual currencies. In that regard, the Serbian law should be amended, according to the meaning of virtual currencies referred to in Directive (EU) 2018/843, since it is incomprehensible that it recognized as obliged entities persons providing the services of purchasing, selling or transferring virtual currencies, but that did not include the definition of virtual currencies in the list of terms used in this Law. Moreover, comparing to the amended provisions of the Directive (EU) 2018/843 concerning virtual currencies, Serbian Law does not recognize the term of custodian wallet provider as an obliged entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies. To conclude, it should be noted that Serbian law is incompletely harmonized with EU *acquis* in this area and in the context of *de lege ferenda* amendments it would be necessary to include these solutions[30].

---

[26] L., Haffke, M., Fromberger, P., Zimmermann *Virtual Currencies and Anti-Money Laundering – The Shortcomings of the 5th AML Directive (EU) and how to Address them*, 9-12. Available at SSRN: https://ssrn.com/abstract=3328064 or http://dx.doi.org/10.2139/ssrn.3328064 Accessed 09.05.2020.

[27] T., Keatinge, D., Carlisle, F., Keen, *op. cit.,* 50-53.

[28] Law on the prevention of money laundering and the financing of terrorism, Official Gazette of the Republic of Serbia, No. 113/17 and 91/2019.

[29] T., Lukić, „Borba Protiv Pranja Novca I Finansiranja Terorizma U Republici Srbiji", *Zbornik radova Pravnog fakulteta u Novom Sadu*, No. 2, 2010, 202.

[30] N., Paunović, *op. cit.,* 676.

V. Conclusion

The analysis of the impact of misuse of cryptocurrencies in combating money laundering and terrorist financing has shown that although use of virtual currencies has created opportunities for relatively secure financial operations in a digital environment, there is still space for improvement. Variety of obliged entities included in the cryptocurrencies transactions, a lot of phenomenological forms in which perpetrators can misuse virtual currencies, as well as a lack of comprehensive normative regulation at international, European and national level, had influence on some achievements in this field in recent period. Thus, EU framework is enriched with the Directive (EU) 2018/843 which introduced three new types of obliged entities of significance for the effective fight against misuse of virtual currencies through money laundering and terrorist financing. The main contribution of the Directive (EU) 2018/843 in the respect of the amended provisions is related to the fact that providers engaged in exchange services between virtual currencies and fiat currencies as well as custodian wallet providers are under Union obligation to identify suspicious activity concerning money laundering and terrorist financing.

Moreover, following the adopted framework at the EU level, the Republic of Serbia has recently adopted the new framework concerning money laundering and terrorist financing, introducing new obliged entities of the importance against misuse of virtual currencies through money laundering and terrorist financing. However, since incompletely harmonized with EU *acquis* in this area, national framework should be amended by introducing the definition of virtual and fiat currencies as well as custodian wallet provider.

To conclude, bearing in mind, emerging new trends, in particular regarding the way organized criminal groups conduct their operations regarding the misuse of virtual currencies through money laundering and terrorist financing it is extremely important to apply training programs, through appropriate channels of international cooperation and exchange of relevant information in the process of development of the skills and capabilities of persons and entities involved in the suppression of this type of crimes to enable them to be prepared for all methods and techniques used by criminals.

References

1. Bierer, T. „Hashing It Out: Problems And Solutions Concerning Cryptocurrency Used As Article 9 Collateral“, *Journal Of Law, Technology & The Internet*, Vol. 7, 2016.

2. Bolta D., „Sprječavanje financiranja terorizma“, *Policija i sigurnost*, No. 4, 2010.

3. Cvitanović. L., et.al., *Kazneno pravo- posebni dio*, Pravni fakultet Sveučilišta u Zagrebu, 2018.

4. Derenčinović, D., The Review Of The Harmonisation Of The Croatian Criminal Law With International Legal Documents On Combating Terrorism, *Hrvatski ljetopis za kazneno pravo i praksu*, No. 2, 2003.

5. Derenčinović, D., et. al., *Posebni dio kaznenog prava*, Pravni fakultet Sveučilišta u Zagrebu, 2013.

6. Dinić, V. „Bitcoin as a decentralized currency“, *Bankarstvo* No. 2, 2014.

7. Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, Official Journal of the European Union, L 141/73 of 5 June 2015, (hereinafter: Directive (EU) 2015/849).

8. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, Official Journal of the European Union, L 156/43 of 19 June 2018, (hereinafter: Directive (EU) 2018/843).

9. Financial Action Task Force, *International Standards On Combating Money Laundering And The Financing Of Terrorism & Proliferation- The FATF Recommendations*, Paris, 2016.

10. Financial Action Task Force, *International Standards On Combating Money Laundering And The Financing Of Terrorism & Proliferation- The FATF Recommendations*, Paris, 2019.

11. Haffke, L., Fromberger, M., Zimmermann P., *Virtual Currencies and Anti-Money Laundering – The Shortcomings of the 5th AML Directive (EU) and how to Address them*, 9-12. Available at SSRN: https://ssrn.com/abstract=3328064, Accessed 09.05.2020.

12. Houben, R., Snyers, A. *Cryptocurrencies and blockchain, Legal context and implications for financial crime, money laundering and tax evasion*, European Parliament, Brussels, 2018.

13. How Law Enforcement Catches Cryptocurrency Criminals,

14. https://thenextweb.com/hardfork/2019/12/26/bitcoin-cryptocurrency-criminals-law-enforcement/,Accessed 09.05.2020.

15. How Law Enforcement Catches Cryptocurrency Crimes,

16. https://www.iannfriedman.com/blog/2019/february/how-law-enforcement-catches-cryptocurrency-crime/, Accessed 09.05.2020.

17. International Centre For Asset Recovery, *Tracing Illegal Assets – A Practitioner's Guide*, Basel 2015.

18. Keatinge, T. Carlisle, D. Keen, F., *Virtual currencies and terrorist financing: assessing the risks and evaluating responses*, European Parliament, Brussels, 2018.

19. Law on the prevention of money laundering and the financing of terrorism, Official Gazette of the Republic of Serbia, No. 113/17 and 91/2019.

20. Lukić, T., „Borba Protiv Pranja Novca I Finansiranja Terorizma U Republici Srbiji", *Zbornik radova Pravnog fakulteta u Novom Sadu*, No. 2, 2010.

21. Office for Prevention of Laundering of Proceeds Derived from Criminal Activity, *Virtual currencies – Risks of Money Laundering and Financing of Terrorism*, Riga, 2019.

22. Paunović, N., Terrorist Financing As The Associated Predicate Offence Of Money Laundering In The Context Of The New Eu Criminal Law Framework For The Protection Of The Financial System, EU and Member States – Legal and Economic Issues, ed. (Duić, D, Petrašević, T., Novokmet, A.), Faculty of Law, Josip Juraj Strossmayer University of Osijek, Osijek, 2019.

23. Pavlović, Z. „ Institutional Capacities of the Republic of Serbia for Opposing Organized Criminal, Terrorism and Corruption ", *Proceedings from scientific conference Financial Crime (Ed. J. Kostić, A. Stefanović)* Institute of Comparative Law and Institute of Criminological & Sociological Research, Zrenjanin, 2018.

24. Pavlović, Z. „Fighting money laundering and control of real estate transactions*", Proceedings from scientific conference Financial Crime and corruption (Ed. J.Kostić, A.Stefanović)* Institute of Comparative Law and Institute of Criminological & Sociological Research, Vršac, 2019.

25. Sinanović, B., „Pranje novca"*, Bilten sudske prakse Vrhovnog suda Srbije,* No. 2, 2011.

26. Sontakke, K., Ghaisas, A. „Cryptocurrencies: A Developing Asset Class“, *International Journal of Business Insights & Transformation*, No. 2, 2017.

27. Stanković N., *Terorizam i finansiranje terorizma*, Evropski Univerzitet Brčko, Brčko, 2014.

28. United Nations Office on Drugs and Crime, *Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies*, United Nations Office on Drugs and Crime, 2014.

29. Važić, N. „Pranje Novca- Materijalni I Procesni Aspektu Međunarodnom I Domaćem Zakonodavstvu“*, Bilten sudske prakse Vrhovnog suda Srbije*, No. 2, 2008.