

Edyta Żyła-Kania*

Use of Virtual Currencies for Financing Terrorism

DOI: [10.58183/pjps.01032023](https://doi.org/10.58183/pjps.01032023)

Abstract

Given the dynamic development of new technologies, it is becoming necessary to improve the system of counteracting and combating the financing of terrorism. In particular, this concerns virtual currencies. The use of them by the criminal world is encouraged by decentralisation of that market, anonymity of users and broad opportunities for functioning on the darknet, which is frequently beyond control of any services. In February 2020, the value of the cryptocurrency market was estimated at US\$300 billion. In Poland, the first legal regulations on counteracting the financing of terrorism with the use of virtual currencies were adopted as late as in 2018, and under the 2021 amendment the legislator introduced several other regulations relating to that area.

Keywords

virtual currencies, cryptocurrencies, new technologies, counteracting the financing of terrorism, combating financing of terrorism

* e-mail: edyta.zyla77@gmail.com,
<https://orcid.org/0000-0002-7531-6320>

Introduction

The rapid development of new technologies results in many areas associated with their functioning remaining outside of any legal framework. It was so for many years in the case of virtual currencies, which came about in 2009, whereas the first regulations were introduced to the Polish legal order in 2018. The anonymity of users guaranteed by the virtual currency trading systems encourages the criminals to use these solutions in carrying out their illegal operations. Growing terrorist threats caused that the majority of states implemented a number of restrictions aimed at counteracting terrorism financing. Those solutions significantly impeded the acquisition of funds by terrorist organisations for their activities, including not only terrorist attacks as such, but also enrolment and propaganda initiatives. In order to circumvent those impediments, criminal groups seek other forms of collecting and transferring funds that seem to be safer from their point of view. Owing to considerable anonymity of virtual currencies and lack of experience of the enforcement authorities in investigating crimes with their use, those cryptocurrencies may become a convenient tool in conducting criminal activities.

The aim of this publication is to determine to what extent the existing legal and institutional solutions in Poland effectively counteract using virtual currencies for financing terrorism, what does the international legal environment in this respect look like and what is the specificity of threats associated with financing terrorism with the use of virtual currencies. In the course of the research, the method of analysis was used, which allowed for specifying major concepts in the context of the outlined problem situations, as well as identifying legal acts and ways of functioning of the institutions taking part in the system of counteracting financing of terrorism. The method of synthesis, in turn, made it possible to draw general conclusions as regards the investigated issues. The hypotheses were verified also with the use of the method of examination of documents, including scientific studies and statistical analyses. In addition, research results were presented using expert interviews. Invited were six experts specialising in the subject of counteracting and combating financing of terrorism, including representatives of the academic community, practitioners and officials. Researched was the system of counteracting and combating financing of terrorism in Poland in the years 2000-2019, after the new regulations concerning that area had come into force. On the basis of the collected data, a hypothesis was put forward that the system of counteracting and combating financing of terrorism in Poland in the years 2000-2019 did not take into consideration all identified forms of terrorism financing (including virtual currencies) and failed to counteract them satisfactorily. Also after 2018,

that is after the new regulations concerning the system of counteracting financing of terrorism had come into force, the system required further improvements.

International regulations concerning virtual currencies

Legal regulations concerning virtual currencies, including their definition, are to be found in the so-called 5th AML Directive. According to the Directive, virtual currencies are “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.”¹ The Directive also defines a custodian wallet provider, which is “an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies.”² In the preamble to the Directive, it has been found that there is a possibility that virtual currencies could be used for money laundering and financing terrorism. Therefore, individual states should have the possibility of monitoring transfers of virtual currencies, while legal regulations should be extended so as to include providers engaged in exchange services between virtual currencies and fiat currencies as well as custodian wallet providers.³ The EU Directive also indicates that web users using virtual currencies enjoy a considerable degree of anonymity. It has been stressed that in order to contain the risks related to the anonymity, legal mechanisms should be established thanks to which financial intelligence units should be able to obtain information needed to identify the owner of virtual currency.⁴

References to virtual currencies are found also in FATF Recommendations. In one of them, FATF points out that states and financial institutions should identify and assess the risks of money laundering and financing terrorism associated with the use of new technologies. In the case of financial institutions, such analysis should be performed before a product is marketed.⁵ Moreover, FATF expects that individual states will undertake measures against natural or legal persons providing money or other assets transfer services aimed at registration or licensing of such services as well as monitoring their quality.⁶ In July 2019, FATF published an interpretive note to Recommendation 15, in which it specified to what extent it refers to virtual currencies in the context of their potential use for money laundering or financing of terrorism. The institution also issued a guidebook concerning those issues, in which it was specifically indicated how individual recommendations refer to the problem of virtual currencies.⁷

1. Article 1(d)(18) of the 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, and amending Directives 2009/138/EC and 2013/36/EU, OJ L 156/43, 2018, p. 43–74.

2. Ibidem.

3. Ibidem, Preamble (8).

4. Ibidem, Preamble (9).

5. Urząd Komisji Nadzoru Finansowego, *Międzynarodowe Standardy Przeciwdziałaniu Praniu Pieniądzy i Finansowaniu Terroryzmu oraz Proliferacji; Rekomendacje FATF*, https://www.knf.gov.pl/knf/pl/komponenty/img/Rekomendacje_FATF_40223.pdf, p. 3, (access 10.03.2019).

6. Ibidem.

7. Financial Action Task Force, *Guidance for a risk based approach. Virtual assets and virtual asset service providers*, FATF 2019, pp. 19–22.

The research results show that cryptocurrency trading is not illegal in the majority of states (including Poland), though certain countries see the development of this technology as an opportunity for making themselves independent from Western financial systems. Russia is working on the development of the Ethereum currency and is preparing its own national cryptocurrency system. Similar work is carried out in China, whereas North Korea steals cryptocurrencies and uses them for money laundering in order to strengthen that country's economy.⁸ Also the US central bank is considering the introduction of its own cryptocurrency.⁹

The new currencies are also scrutinised by the European Union and in this connection work is carried out on a virtual euro. The European Central Bank (ECB) informs that the digital euro would be an electronic form of the central bank's money available to all citizens and businesses, just like banknotes though in a digital form. The European Central Banks assures that the digital euro is to be protected and regulated by the EBC, and it will differ from the cryptocurrencies that are now functioning on the market primarily by the centralisation of the system and its being based on a banking institution.¹⁰

8. J. Konieczny, R. Prabucki, R. Wielki, *Kryptowaluty. Perspektywa kryminologiczna i kryminalistyczna*, Instytut Wydawniczy EuroPrawo 2018, p. 106.

9. W. Nowakowski, *Czy rok 2020 będzie przełomowy dla kryptowalut?*, "Człowiek i Dokumenty", 2020, No. 58, p. 65.

10. *European Central Bank*, www.ecb.europa.eu, (access 23.11.2020).

Legal regulations associated with the functioning of virtual currencies in Poland

As regards Polish regulations, a definition of virtual currencies is found in the *Act on Counteracting Money Laundering and Financing of Terrorism* and pursuant to its Art. 2(2)(26) virtual currencies mean "a digital representation of value which is not:

- a) legal tender issued by the National Bank of Poland, foreign central banks or other public administration bodies;
- b) an international unit of account established by an international organisations and accepted by individual countries affiliated in this organisation or cooperating therewith;
- c) electronic money within the meaning of the Act of 19 August 2011 on Payment Services;
- d) a financial instrument within the meaning of the Act of 28 July 2005 on Trading in Financial Instruments;

e) a bill of exchange or a cheque – and is convertible in business transactions into legal tender and is accepted as a means of exchange, and also may be electronically kept or transferred or may be subject to electronic trading.”¹¹

Moreover, the Act defined the concept of a wallet in the context of virtual currencies stating that it is “a set of ID data kept in an electronic form, which ensures for the authorised persons a possibility to use units of virtual currencies, including carrying out exchange transactions.”¹² Until the coming into force of the *Act on Counteracting Money Laundering and Financing Terrorism* of 1 March 2018, which introduced the said regulations, institutions of the Polish state had used the definition of the European Banking Authority which provides that virtual currencies are “a digital representation of value not issues by a central bank or a public authority, not necessarily linked with the currency of a given country, but accepted by natural and legal persons as legal tender, which may be transferred, kept or electronically traded.”¹³

In the context of virtual currencies, it should be noted that they are not legal tender and are functioning in the decentralised system as they are not issues by any public authority. In light of the *Personal Income Tax Act*¹⁴ income from virtual currency trading is subject to taxation. The 2018 amendment of that Act introduced provisions regulating the rules for taxation of income from virtual currency defined in the *Act on Counteracting Money Laundering and Financing of Terrorism*. It is worth noting that the amendment covered both Personal Income Act and Corporate Income Act. In its substantiation it was raised that incomes from trading in virtual currencies are recognised as income from financial capital or capital gains. The sources of income from virtual currency trading do not include revenues of operators engaged in virtual currency exchange or exchange intermediation. Taxable is income from the exchange of virtual currencies into legal tender and income from the sale of virtual currencies at the exchange, while the use of virtual currencies to pay for goods, services or regulate other obligations is treated on a par with their selling.¹⁵

When discussing virtual currencies, a distinction needs to be made also between this concept and cryptocurrencies, despite the fact that these terms are generally used interchangeably, also by the EU institutions or FATF. Some experts notice, however, that cryptocurrency is a type of virtual currency, though treating them as same may lead to far-reaching simplifications, first of all due to the fact that cryptocurrency has no issuer, while virtual one does.¹⁶

11. Artykuł 2 (2)(26), ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, Dz.U. 2021 poz. 1132, [Article 2 (2)(26) of the Act of 1 March 2018 on Counteracting Money Laundering and Financing Terrorism, Journal of Laws 2021, item 1132].

12. Ibidem, Article 2 (2)(17e).

13. Narodowy Bank Polski, Komisja Nadzoru Finansowego, *Komunikat Narodowego Banku Polskiego i Komisji Nadzoru Finansowego w sprawie “walut wirtualnych”*, https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_NBP_KNF_w_sprawie_walut_wirtualnych_7_07_2017_57361.pdf, (access 24.11.2020).

14. See: Ustawa z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych, Dz.U. 2021 poz. 1128, [Personal Income Tax Act of 26 July 1991, Journal of Laws 2021, item 1128].

15. Rządowe Centrum Legislacji, *Uzasadnienie nowelizacji przepisów podatkowych obejmujących m.in. Ustawę z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych oraz Ustawę z dnia 15 lipca 1992 r. o podatku dochodowym od osób prawnych*, RCL 2018.

16. S. Bala, T. Kopyściański, W. Srokosz, *Kryptowaluty jako elektroniczne instrumenty płatnicze bez emitenta*, Wydawnictwo Uniwersytetu Wrocławskiego 2016, p. 114.

Virtual currency functioning principles

In order to ensure efficient functioning of the cryptocurrency market there is a need to implement legal regulations in many areas of law, including civil law (ownership, obligations), financial law (marketing, regulation of trading, licencing, customer authentication, payment services, electronic money), foreign exchange law, banking law, commercial law or administrative law.¹⁷

The functioning of virtual currencies is based on blockchain technology, which is a ledger consisting of a list of transactions carried out in a given cryptocurrency.¹⁸ According to Wojciech Nowakowski, elements of a blockchain are block comprising information on transactions or other events that are linked together and constitute an integral whole (each subsequent block contains a compilation of the previous one).¹⁹ Quoting after Paweł Opitek and Kamil Góral: “Their chain, in which the chronological sequence of transactions performed is recorded, constitutes a decentralised record and may be shared and confirmed by anybody who has relevant authorisations.”²⁰ Describing the mechanism of operation of the most popular cryptocurrency – bitcoin, it should be noted that a user with a certain IP address, similar to the number of a bank account, initially generated 50 blocks of data, that is bitcoins. In the course of successive operations subsequent tranches allocated to that address are created. The previously created block of data, called *coins*, also remain in that user’s wallet. Each of the subsequent sets of data has a limited capacity, which is why the demand for transactions is greater than the technical capabilities of the system, which in consequence means that some of the transactions take long to be validated. The pace of adding them depend on the value of so-called transaction fee; the larger it is, the greater is the change for the quick adding of a transaction to a block. The fee is also paid in bitcoins.²¹ Individual transactions are carried out by so-called miners, that is computers owned by people belonging to the bitcoin community. The greater the computing power of the hardware, the greater the chance to generate new bitcoins. That is why such an important role in the process of virtual currency trading is played by performance of hardware, especially cryptographic cards.²² Each bitcoin is divided into 100 million units, i.e. so-called satoshi. The blockchain contains all records. The average time for the creation of another block in case of a bitcoin blockchain is 10 minutes. Access to information contained in public blockchains is open, which means that it can be checked by anybody. Therefore, there is a theoretical possibility to ascertain both the addresses from which transactions are carried out as well as their course. In practice, however, blockchains are used which make it impossible to check the transaction, while the user themselves operate under pseudonyms.²³

17. W. Michalczyk, *Bariery rozwoju Bitcoina jako nowej formy pieniądza międzynarodowego*, “*Ekonomia XXI wieku*”, 2018, 1 (17), pp. 53–54.

18. K. Brzeziński, A. Bubieli, K. Jaczewski, et al., *Podstawy korzystania z walut cyfrowych*, Wydawnictwo Instytut Wiedzy i Innowacji 2017, p. 15.

19. W. Nowakowski, *Hybrydowe łańcuchy bloków. Hyperledger*, “*Człowiek i Dokumenty*”, 2020, No. 56, p. 55.

20. P. Opitek, K. Góral, *Analiza kryminalna transferów kryptowalutowych w pracy prokuratora (cz. I)*, “*Prokuratura i Prawo*”, 2020, No. 4–5, p. 80.

21. K. Brzeziński, A. Bubieli, K. Jaczewski, et al., *Podstawy...*, op. cit., pp. 14–18.

22. G. Sobiecki, *Bitcoin: globalna alternatywna waluta*, in: *Kryzys finansowy – przebieg i skutki społeczno-gospodarcze w Europie Środkowej i Wschodniej*, ed. S. Partycki, Wydawnictwo KUL 2010, pp. 56–70.

23. K. Brzeziński, A. Bubieli, K. Jaczewski, et al., *Podstawy...*, op. cit., p. 17.

The specificity and extent of threats associated with the use of virtual currencies for financing terrorism

Virtual currencies may be used for criminal activities, mainly due to the decentralisation of the underlying databases as well as the absence of a concrete specified issues. There is no entity that supervises their functioning, whereas the society is not sufficiently knowledgeable to use them efficiently and safeguard itself against their potential misuses.²⁴ The scope of criminal activities involving virtual currencies is steadily growing. Over the last three years it was a leap growth.²⁵ It follows from the 2018 research conducted by an Australian-Latvian research team that almost one-fourth of bitcoin users were engaged in illegal operations, and almost one-half of the transactions carried out in that currency were associated with criminal activities. Bitcoin value is related to the fact of its being used by the criminal world, which is confirmed by the exchange rate volatility as a response to the operations of law enforcement agencies. The researchers found that the proceeds from illegal operations linked with the use of the bitcoin system amount to around US\$ 76 billion per annum, which is the amount similar in scale to the US and European drug market. Moreover, the use of bitcoin is waning upon emergence of less transparent currencies.²⁶ In the context of the risk of money laundering and financing terrorism, noteworthy are also P2P platforms. Those tool make it possible e.g. to exchange electronic money for digital currencies, or digital currencies for traditional money. Officially, they should be subject to the rules associated with counteracting money laundering and financing terrorism, but in practice it is not so, whereas the services they offer are available on social media or the darknet.²⁷

The possibility of using cryptocurrencies for financing terrorism is also shown by the 2014 Al-Qaida manifesto encouraging their use for the struggle against the infidel. The manifesto stressed that transferring money in the tradition form encountered many barriers, and first of all those transfers were controlled by the governments of individual states, so a solution to this situation was to use virtual currency – bitcoin. The terrorist message described the system and provided the rudiments of its functioning, and then emphasised its advantage over other payment systems such as PayPal or eBay (mostly owing to its decentralisation). Also shown was the possibility of making completely anonymous transactions, thanks to which it became also possible to raise donations in virtual currency and then convert it into any traditional currency. “This system has the potential to revive the lost Sunnah of donating to the mujahedeen, it is simple, easy, and we ask Allah to hasten it’s usage for us.” – appealed the manifesto.²⁸

24. Ibidem, p. 57.

25. P. Opitek, K. Góral, *Analiza kryminalna...*, op. cit., pp. 74–96.

26. S. Foley, J.R. Karlsen, T. Putniņš, *Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?*, “Review of Financial Studies”, 2019, 32 (5), pp. 1798–1853.

27. P. Opitek, *Pranie pieniędzy i finansowanie terroryzmu z wykorzystaniem walut wirtualnych*, Instytut Kościuszki 2020, pp. 10–12.

28. T. Munthir, *Bitcoin wa Sadaqat al Jihad: Bitcoin and the Charity of Violent Physical Struggle*, <https://krypt3ia.files.wordpress.com/2014/07/btccedit-21.pdf>, (access 24.11.2020).

Jerzy Konieczny, Rafał Prabucki and Rafał Wielki emphasise in order to use cryptocurrencies for criminal activities one has to be well prepared technologically, which means they become attractive to those organisations that have such skills. Moreover, their use involves risks, which may discourage terrorists, e.g. unpredictable volatility of exchange rates or interest taken in them by law enforcement bodies. However, as the researchers underline, terrorist organisations are able to manage the risk, which is an inherent part of their operation. Although not many cases of using cryptocurrencies for financing terrorism have been identified, the possibility of escalation of such threats must not be ignored and that area should remain in the domain of interest for researchers.²⁹ From the 2020 Europol report it follows that virtual currencies are used for financing terrorist activities mostly to cover minor expenses, purchases on illegal darknet platforms, as well as to pay for counterfeit documents or air tickets.³⁰ Maciej Kędzierski supposes that in the future state virtual currencies may be created, which will contribute to the emergence of state terrorism. Cryptocurrencies provide an opportunity to make darknet payments for financial services, the activities of secret agents or the functioning of associations for the benefit of militants.³¹

29. J. Konieczny, R. Prabucki, R. Wielki, *Kryptowaluty...*, op. cit., p. 91.

30. EUROPOL, *European Union Terrorism Situation and Trend report 2020*, https://www.europol.europa.eu/cms/sites/default/files/documents/european_union_terrorism_situation_and_trend_report_te-sat_2020_0.pdf, p. 22, (access 23.11.2020).

31. M. Kędzierski, *Przeciwdziałanie i zwalczanie finansowania terroryzmu w Polsce*, Wydawnictwo Adam Marszałek 2019, p. 95.

32. Article 8 of the Directive (EU) 2018/843..., op. cit.

33. 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, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, OJ L 141/73, 2015, p. 73–117.

34. Article 8 of the Directive (EU) 2018/843..., op. cit.

Counteracting and combatting the use of virtual currencies for financing terrorism

The regulations aimed at counteracting the financing of terrorism with the use of cryptocurrencies were introduced into the legal order as late as in 2018. The 5th AML Directive provided not only the definition of virtual currencies, but also the list of measure to be taken by individual states in order to counteract the practice of financing terrorism with the use of those technologies. In the Preamble it was stated that “Providers engaged in exchange services between virtual currencies and fiat currencies (that is to say 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) as well as custodian wallet providers are under no Union obligation to identify suspicious activity. Therefore, terrorist groups may be able 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.”³² With a view to those threats it was decided that it was necessary to extend the scope of the 4th AML Directive (Directive 2015/849)³³ “(...) so as to include providers engaged in exchange services between virtual currencies and fiat currencies as well as custodian wallet providers. For the purposes of anti-money laundering and countering the financing of terrorism (AML/CFT), competent authorities should be able, through obliged entities, to monitor the use of virtual currencies. Such monitoring would provide a balanced and proportional approach, safeguarding technical advances and the high degree of transparency attained in the field of alternative finance and social entrepreneurship.”³⁴

Those principles have become binding for the EU Member States, which have been obligated to update their national regulations in accordance with the recommendations laid down in the Directive. Combatting crime associated with trading in virtual currencies is a challenge for law enforcement agencies in all states worldwide. None of them has either an effective tested methodology for combatting this type of crime, or experience in this area. J. Konieczny, R. Prabucki and R. Wielki emphasise that working out certain solutions in this respect requires using various sources of information, including open sources, information from the darknet and data collected in the course of operational and exploratory activities.³⁵ As regards the problems in carrying out procedure associated with cryptocurrency offences, the Polish experts point to, among others: difficulties in defining that crime owing to its interdisciplinary nature, anonymity of the perpetrators and lack of their direct contact with the victims, the possibility of operating in any place in the world and attacking many victims at the same time, as well as the long time the investigations take, which as a matter of fact does not favour their effectiveness. Combatting cybercrime is also impeded by the need to make constant updates of the expensive systems.³⁶

Experts on counteracting the financing of terrorism with the use of virtual currencies – presentation of research results

In order to evaluate to what extent the Polish system of counteracting the financing of terrorism with the use of virtual currencies was effective, six experts were interviewed. The question was: *Is the existing system of counteracting the financing of terrorism capable of effectively preventing the financing of terrorism with the use of new technologies, including virtual currencies?* All experts indicated that the existing system was able to prevent those threats only partially. Responding to the subsequent question, in which they were asked to indicate what measures should be taken to improve the system, the experts first of all stressed that seeking the possibilities of using new technologies terrorist organisations ever more often showed interest in virtual currencies. One of the experts said that it did not involve solely placing information online encouraging the entities dependent on terrorist organisations to use virtual currencies, but also their activities on the darknet and social media. Offences were also committed against holders of bitcoins and other virtual currencies. In this situation, the state institutions, in particular the General Inspector of Financial Information (GIIF) should undertake measures allowing for more stricter control of the functioning of virtual currencies. According to the expert, entities involved in virtual currency trading should assess what disadvantages they saw in their relationships with GIIF. Moreover, it would be needed to set the framework for a financial analysis concerning those entities – currently (as at the time of the interview, i.e. October 2019) it was limited to analysing their bank accounts. The expert also saw the need for training the

35. J. Konieczny, R. Prabucki, R. Wielki, *Kryptowaluty...*, op. cit., pp. 106-107.

36. Ibidem, pp. 108-109.

staff of the Financial Information Department of the Ministry of Finance as regards analysing the data of wallets owned by users of virtual currencies. He believed that the existing system was only partially capable of counteracting the financing of terrorism with the use of virtual currencies.³⁷ Also another expert acknowledged that the existing system was partially capable of counteracting the threat associated with the financing of terrorism with the use of virtual currencies, whereas the difficulties were due to their very specificity guaranteeing a high degree of anonymity. In the practice of financing terrorism, criminals world are also encouraged to reach out for those instruments by absence of close international collaboration.³⁸

Conclusions

Virtual currencies are not yet an instrument which is commonly used for perpetrating crimes of the terrorist nature, but remain in the area of interest of terrorist organisations. This is demonstrated not only by cases of raising funds with the use of cryptocurrencies, but also the Al-Qaida manifesto addressed to its followers, which points out the advantages of virtual currencies.

The research results presented above allow for stating that:

- the use of them by the criminal world is encouraged by decentralisation of that market, anonymity of users and broad opportunities for functioning on the darknet, which is frequently beyond control of any services;
- the virtual currency market is all the time on the rise, whereas the value of transactions performed with the use of only bitcoins for criminal purposes for criminal purposes becomes comparable to the scale of the US and European drug market;³⁹
- detecting and combatting crime with the use of virtual currencies is very difficult and time consuming, both owing to the specificity of the underlying technology as well as the absence of an adequate methodology and insufficiently effective international collaboration;
- not all states abide by the rules of financial security laid down in the FATF Recommendations, which encourages dishonest virtual wallet users to locate their activities in those states.

37. Expert interview on 1 October 2019. Author's private archive.

38. Expert interview on 27 November 2019. Author's private archive.

39. S. Foley, J.R. Karlsen, T. Putniņš, *Sex, Drugs...*, op. cit., pp. 1798–1853.

The a hypothesis put forward in the introduction that the system of counteracting and combating the financing of terrorism in Poland in the years 2000-2019 did not take into consideration all identified forms of terrorism financing (including virtual currencies) and failed to counteract them satisfactorily has been confirmed. Those threats were perceived both by the international community and the Polish lawmaker, though the measures that have been undertaken seem to be belated and insufficient. Although the virtual currency market had been developing since 2009, the first legal regulations in this regards were introduced 9 years later. Earlier, only the threats associated with investing in virtual currencies has been signalled, the manifestation of which was *inter alia* the information campaign launched in 2017 by the Polish Financial Supervisory Authority and the National Bank of Poland. Meanwhile, the virtual currency market has been dynamically developing, and the absence of any control encouraged criminal organisations, including terrorist ones, to function in it. Changes in this respect have been the matter of the last few years. Almost all experts, whose opinions have been presented above, assessed that the Polish system of counteracting the financing of terrorism with the use of virtual currencies was only partially adapted to the existing threats. To improve this situation, it will become necessary not only to revise the regulations, but also equip Polish services with adequate IT and analytical instruments, and also strengthen international collaboration.

Moreover, on the basis of the above presented research results it should be acknowledged that the legal regulations and institutional solutions concerning counteracting and combatting the financing of terrorism with the use of virtual currencies will be subject to further amendments. As pointed out by the experts, whose opinions have been quoted above, the new Act on Counteracting Money Laundering and Financing Terrorism of 1 March 2018 perceived the threats associated with the development of virtual currencies though failed to prevent them sufficiently. It was only in the 2021 amendment that the legislator introduced a number of regulations related to that area.

Those regulations significantly order the virtual currency market, as before the amendment it had operated in a large measure outside the law. These changes are certainly not yet adequate, and in the forthcoming years there will be a need to pass further legal regulations.⁴⁰

40. The research results presented herein come from: E. Żyła, *System przeciwdziałania i zwalczania finansowania terroryzmu w Polsce wobec istniejących zagrożeń*, Akademia Sztuki Wojennej 2022.

Bibliography

Bala S., Kopyściański T., Srokosz W., *Kryptowaluty jako elektroniczne instrumenty płatnicze bez emitenta*, Wydawnictwo Uniwersytetu Wrocławskiego 2016.

Brzeziński K., Bubieli A., Jaczewski K., Piech K., Piwko J., Rykowska J., Sobiecki G., Wiśniewski Ł., *Podstawy korzystania z walut cyfrowych*, Wydawnictwo Instytut Wiedzy i Innowacji 2017.

European Central Bank, www.ecb.europa.eu, (access 23.11.2020).

EUROPOL, *European Union Terrorism Situation and Trend report 2020*, https://www.europol.europa.eu/cms/sites/default/files/documents/european_union_terrorism_situation_and_trend_report_te-sat_2020_0.pdf, (access 23.11.2020).

Expert interview on 1 October 2019. Author's private archive.

Expert interview on 27 November 2019. Author's private archive.

Financial Action Task Force, *Guidance for a risk based approach. Virtual assets and virtual asset service providers*, FATF 2019.

Foley S., Karlsen J.R., Putniņš T., *Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?*, "Review of Financial Studies", 2019, 32 (5), pp. 1798–1853.

Kędziński M., *Przeciwdziałanie i zwalczanie finansowania terroryzmu w Polsce*, Wydawnictwo Adam Marszałek 2019.

Konieczny J., Prabucki R., Wielki R., *Kryptowaluty. Perspektywa kryminologiczna i kryminalistyczna*, Instytut Wydawniczy EuroPrawo 2018.

Michalczyk W., *Bariery rozwoju Bitcoina jako nowej formy pieniądza międzynarodowego*, "Ekonomia XXI wieku", 2018, 1 (17), pp. 41–67.

Munthir T., *Bitcoin wa Sadaqat al Jihad: Bitcoin and the Charity of Violent Physical Struggle*, <https://krypt3ia.files.wordpress.com/2014/07/btcredit-21.pdf>, (access 24.11.2020).

Narodowy Bank Polski, Komisja Nadzoru Finansowego, Komunikat Narodowego Banku Polskiego i Komisji Nadzoru Finansowego w sprawie "walut" wirtualnych, https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_NBP_KNF_w_sprawie_walut_wirtualnych_7_07_2017_57361.pdf, (access 24.11.2020).

Nowakowski W., *Czy rok 2020 będzie przełomowy dla kryptowalut?*, "Człowiek i Dokumenty", 2020, No. 58, pp. 63–67.

Nowakowski W., *Hybrydowe łańcuchy bloków. Hyperledger*, "Człowiek i Dokumenty", 2020, No. 56, pp. 50–59.

Opitek P., Góral K., *Analiza kryminalna transferów kryptowalutowych w pracy prokuratora (cz. I)*, "Prokuratura i Prawo", 2020, No. 4–5, pp. 74–96.

Opitek P., *Pranie pieniędzy i finansowanie terroryzmu z wykorzystaniem walut wirtualnych*, Instytut Kościuszki 2020.

Rządowe Centrum Legislacji, *Uzasadnienie nowelizacji przepisów podatkowych obejmujących m.in. Ustawę z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych oraz Ustawę z dnia 15 lipca 1992 r. o podatku dochodowym od osób prawnych*, RCL 2018.

Sobiecki G., *Bitcoin: globalna alternatywna waluta*, in: *Kryzys finansowy – przebieg i skutki społeczno-gospodarcze w Europie Środkowej i Wschodniej*, ed. S. Partycki, Wydawnictwo KUL 2010, pp. 56–70.

Urząd Komisji Nadzoru Finansowego, *Międzynarodowe Standardy Przeciwdziałaniu Praniu Pieniędzy i Finansowaniu Terroryzmu oraz Proliferacji; Rekomendacje FATF*, https://www.knf.gov.pl/knf/pl/komponenty/img/Rekomendacje_FATF_40223.pdf, (access 10.03.2019).

Żyła E., *System przeciwdziałania i zwalczania finansowania terroryzmu w Polsce wobec istniejących zagrożeń*, Akademia Sztuki Wojennej 2022.

Legal acts

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, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, OJ L 141/73, 2015, p. 73–117.

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, and amending Directives 2009/138/EC and 2013/36/EU, OJ L 156/43, 2018, p. 43–74.

Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, Dz.U. 2021 poz. 1132, [Act of 1 March 2018 on Counteracting Money Laundering and Financing Terrorism, Journal of Laws 2021, item 1132].

Ustawa z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych, Dz.U. 2021 poz. 1128, [Personal Income Tax Act of 26 July 1991, Journal of Laws 2021, item 1128].