https://doi.org/10.4467/27204383TER.23.030.18332

https://orcid.org/0000-0002-4015-5774
https://orcid.org/0000-0002-2761-3144
https://orcid.org/0009-0000-7130-0455

PAWEŁ OPITEK
AGNIESZKA BUTOR-KELER
KAROL KANCLERZ

Selected aspects of crime involving virtual currencies

Abstract

The article consists of two parts. The first discusses issues related to the functioning of the crypto-assets market in Poland and internationally and the planned changes in the regulations governing this market. They concern the legal status of digital tokens and their use in money laundering and terrorist financing, as well as the obligations of obliged institutions in the anti-money laundering system. The second part of the study focuses on procedural and non-procedural issues related to virtual currencies. The status of the digital artefact in criminal proceedings, operational work and the conduct of investigations with a view to combating cryptocurrency crime are discussed. The article concludes with demands addressed to law enforcement and law enforcement agencies. The aim of the article is to provide a comprehensive overview of the issues related to the use of virtual currencies in the commission of crimes, covering in particular AML and terrorist financing issues.

Keywords:

cryptocurrencies, virtual currencies, crime, money laundering, terrorist financing, investigation, digital footprints and evidence

Virtual currencies have become integral to the perpetration of various types of crime - they are the object of an executive action when the perpetrator divests an authorised person of authority over bitcoins and the binary data that constitutes them becomes the object of unauthorised manipulation. It is not uncommon for cryptocurrencies to be used for money laundering, obtaining ransomware or social engineering-based attacks. There is also financial embezzlement using cryptocurrencies and crowdfunding, platforms that operate similarly to the traditional forex market or financial pyramid schemes, whose clients are tempted by the promise of a quick and high profit after investing in tokens. There are also cryptocurrencies being issued which are de facto financial derivatives bypassing capital market regulations. The phenomenon of cryptocurrencies is not only analysed in the context of the modus operandi of the perpetrators of criminal acts. It also raises other important issues, such as the legal status of tokens, the criminal analysis of cryptocurrency transfers, the temporary seizure of movable property and property seizure over bitcoin or other altcoins, procedures for obtaining digital footprints and international legal assistance in this regard, or administrative AML/CFT (Anti-Money Laundering/Counter Financing of Terrorism) procedures. This article provides a snapshot of all these issues, but due to its limited volume only some of them could be discussed in more detail.

At the outset, it is worth asking the question: do Polish law enforcement agencies even need capabilities regarding working with crypto-assets? The answer to such a question is certainly yes, which is due to several reasons. In the most general terms, the contemporary crime picture is too often linked to virtual currencies and the technology creating a system of distributed records for institutions intended to protect the economic interests of the state not to orient themselves in the legal, economic and technical aspects of their operation. But there are also specific cases that oblige, for example, the Internal Security Agency (ISA) to take an interest in cryptocurrencies. They are used for large-scale money laundering, and the ISA is obliged to identify, prevent and detect crimes that harm the economic foundations of the state. Security is also about Poland's compliance with international agreements, as this has a direct impact on Poland's position and reputation on the world stage. In this context, it is worth recalling that the sanctions imposed on Russia and Belarus following the aggression of the Russian Federation in Ukraine also cover crypto-activism and Polish services cannot allow these sanctions to be circumvented using domestic network providers. Anonymous transfers on

blockchain can also be a convenient tool to support terrorist organisations and influence agents that exist in various countries, including Poland. The Internal Security Agency is tasked with controlling this segment of the wider financial market in order to prevent such activities.

The article is based on two research objectives: to analyse the current legal status and actual functionality of cryptocurrencies worldwide, and to determine whether they are associated, and on what scale, with the commission of criminal acts, including money laundering and terrorist financing. In the latter case, in addition to taking a critical look at the international dimension of the crime in question, the topic of law enforcement activities in the fight against cryptocurrency crime, which is close to the authors of the study, is also addressed. The analysis of the crime in question on a micro (national) and macro (global) scale led to the identification of actions that require law enforcement agencies to have knowledge of cryptocurrencies and to use it in practice.

The research methodology used consisted of observing and analysing a variety of online sources related to virtual currencies and establishing the ways in which these currencies operate, as well as the thoughts of the article's authors on the issues considered. Among other things, the authors consulted information from the websites of specialist crypto companies and governmental organisations, including the report of a hearing held in the US Congress by representatives of counter-terrorism services on the activities of extremists in the virtual world. In addition, the authors - on the basis of their own competence and professional experience gained from dealing with criminal cases or carrying out supervisory tasks over the capital market - presented conclusions on cryptocurrency crime and the activities of Polish services in this area. They were confronted with source materials in the form of analyses, reports and other studies of organisations and institutions dealing with digital tokens and blockchain technology. Reference was also made to legal acts in force or in the process of being drafted, which regulate the crypto market. Finally, based on the totality of the information obtained, an inductive method was used to record the observations made in relation to the previously stated dataset.

In the article, the terms: cryptocurrencies, virtual currencies and crypto-assets (digital assets) are used interchangeably as it concerns crime and this terminological arbitrariness is of little relevance to the description of the research topic. However, it should be emphasised that cryptocurrencies are the term with the broadest conceptual scope, although they lack a legal

definition in Polish law. Pursuant to the *Executive Order of the President of the United States of 9 March 2022 on ensuring the responsible development of digital assets*[1], the term digital asset refers to digital money issued by a central bank digital currency (CBDC) regardless of the technology used to issue it, and other representations of value, including securities, financial derivatives and other financial products that are used to make payments, invest, transfer or exchange funds or their equivalent, issued or represented in digital form using distributed ledger technology (DLT) regardless of the product name. The term cryptocurrencies, on the other hand, refers to digital assets that can be a medium of exchange, generated or supported by DLT technology. In the middle of the conceptual scopes of these two terms lie virtual currencies.

Legal status of digital tokens

In terms of regulation, virtual currencies are treated differently around the world. Although they have been recognised as legal tender in some countries, these are exceptional situations, as they are most often denied a position similar to that of fiat money. This is due to the fact that the governments of individual countries rigorously guard their monopoly on the issuance of money, as through it they can shape the monetary policy of the country and influence economic processes. Research by the International Monetary Fund shows that virtual currencies have gained the strongest foothold in sub-Saharan Africa, where 25 per cent of countries have regulated their legal status in detail and more than half of them have decided to lift many restrictions on the operation of cryptocurrencies in the traditional financial market[2]. However, this applies to the regulation of payment tokens, such as bitcoin, which is the simplest in its operation. For example, in October 2021, the Central Bank of Nigeria introduced a virtual

[1] *Ensuring Responsible Development of Digital Assets*, Executive Order 14067 of March 9, 2022, Federal Register. The Daily Journal of the United States Government, https://www.federalregister.gov/documents/2022/03/14/2022-05471/ensuring-responsible-development-of-digital-assets [accessed: 5 IV 2023]. Translations in the article are from the authors (editor's note).

[2] *Living on the Edge*, International Monetary Fund, October 2022, https://www.imf.org/en/Publications/REO/SSA/Issues/2022/10/14/regional-economic-outlook-for-sub-saharan-africa-october-2022 [accessed: 5 IV 2023].

token called eNaira as a back-up to traditional fiat money. The system was developed by Fintech Bitt, and two apps for using eNaira - eNaira Speed Wallet and eNaira Merchant Wallet - are available in the Google and Apple app shops. 500 million eNaira ($1.21 million) have already been issued in 2022, but the Nigerian government has simultaneously banned transactions in its own banking sector with other cryptocurrencies[3].

In contrast, initiatives are being taken in highly developed countries to systematise approaches to advanced digital tokens issued on the basis of blockchain technology and similar in operation to financial derivatives. Work on the tokenisation of such instruments is well advanced in Japan. In October 2021, MUFG, Japan's largest bank, announced the results of a Security Token Research Consortium group (renamed the Digital Asset Co-creation Consortium in 2022) dedicated to building an infrastructure for tokenised securities. It was planned to record their trading on the Corda corporate blockchain. The right to sub-connect to it has been granted to other companies interested in digital financial instruments - securities listed on the Osaka Digital Exchange, which has integrated with the Progmat platform and allows P2P (peer-to-peer) transactions[4] between investors[5]. The platform is expanding its functionality all the time (it has grown from 80 companies to 163 by the end of 2022) and is currently emphasising the development and trading of stablecoin, enabling settlements to be made outside the official banking system[6].

On the other side are countries that have completely banned the possession of virtual currencies, i.e. China, Nepal, Bangladesh, Afghanistan, Morocco, Algeria and Bolivia[7]. In the case of the Middle

---

[3] P. Opitek, *Funkcjonowanie instrumentów finansowych w oparciu o technologię blockchain* (Eng. Functioning of financial instruments based on blockchain technology), Łódź 2022, p. 214.

[4] P2P transactions - transactions between individuals excluding intermediaries, such as shops, and factories and corporations (editor's note).

[5] *MUFG, SBI share roadmap for Japanese security tokens*, Ledger Insights, 7 X 2021, https://www.ledgerinsights.com/mufg-sbi-share-roadmap-for-japanese-security-token-platform/ [accessed: 27 III 2023].

[6] *MUFG's Progmat security token platform to become digital asset joint venture*, Ledger Insights, 22 XII 2022, https://www.ledgerinsights.com/mufg-progmat-security-token-digital-asset-joint-venture/ [accessed: 5 IV 2023].

[7] F. O'Sullivan, *Where Is Crypto Illegal in 2023? The Countries That Ban Cryptocurrency*, Cloudwards, 22 II 2023, https://www.cloudwards.net/where-is-crypto-illegal/ [accessed: 5 IV 2023].

Kingdom, there are several reasons why this has happened. China has a several-year lead over the rest of the developed economies of the globe in the development of the Central Bank's national digital currency, so the government there may have seen decentralised assets as competition threatening the centralised yuan project. Furthermore, China's economic system favours top-down management of the financial market and arguably the existence of a stand-alone bitcoin is not beneficial to it. As a result, the Chinese authorities began to pursue anti-crypto-currency policies and media marketing campaigns discouraging the use of bitcoin and altcoin. Eventually, a ban on cryptocurrency-related search terms on the internet was introduced, as well as the closure of digital platforms[8].

In the United States and European Union countries, ownership of virtual currencies is permitted, and the only obligations involved relate to some form of registration (notification) of business activities conducted using cryptocurrencies. The issue of financial instruments on blockchain protocols is problematic. In Europe, such activities are generally prohibited, while in the United States, the principle of technological neutrality applies and financial instruments can be tokenised, although in practice this is subject to a number of requirements and is generally unprofitable. Recently, the White House published for the first time ever guidelines to comprehensively define a framework for the responsible development of digital assets in the United States. Following an executive order from President Joe Biden, the country's administration made recommendations to protect consumers, investors, businesses, financial stability, national security and the environment in the context of crypto market operations. The 9 March 2022 Executive Order on Ensuring Responsible Development of Digital Assets[9] outlined an innovative approach to addressing the risks and harnessing the potential benefits of digital assets and their underlying technology. Government agencies have developed frameworks and recommendations to support consumer and investor protection, promotion of financial stability and economic competitiveness, and innovation, among others. The US is also recognised as a global leader in the application of anti-money laundering and counter-terrorist financing procedures in the digital asset environment and sets global standards in this sphere. The White House noted that the popularity

[8] P. Opitek, *Funkcjonowanie instrumentów finansowych…*, p. 212.

[9] *Ensuring Responsible Development…*

of cryptoassets has also led to an increase in the number of cybercriminals carrying out, among other things, money laundering and financing illegal activities. In order to counter such practices, there is a need for increased regulation and oversight of the cryptocurrency market, more intensive law enforcement involvement in the fight against the crime in question, and changes to laws, including the key US Bank Secrecy Act (BSA), toughening the penalties provided for the anonymous transfer of crypto assets and making them also apply to providers of online exchanges and non-fungible NFTs (unique tokens that identify a digitised work of art, such as a sculpture or painting). As part of the steps taken, the White House has committed the US Department of Justice to prosecute serious digital asset crimes committed in any jurisdiction and the Treasury to finalise a risk assessment of illicit decentralised finance in 2023[10].

In turn, the European Union lacks, according to the European Commission, uniform rules applicable to crypto-related services, which exposes consumers and institutional investors to a significant risk of loss. Furthermore, the fact that some Member States have introduced relevant regulations at national level and others have not, leads to a fragmentation of common law that distorts competition in the European single market, hinders service providers from expanding their operations across borders and leads to regulatory arbitrage. This is why the European Parliament will soon vote to adopt the Markets in Crypto-assets (MiCA) Regulation. The regulation would establish harmonised rules for such assets at EU level, thus providing legal certainty for crypto-assets not covered by existing EU legislation. This is expected to enhance consumer and investor protection and financial stability, promote innovation and opportunities for DLT-based tokens. The regulation establishes three types of crypto-assets: asset-linked tokens (akin to stablecoins), e-money tokens and crypto-assets not covered by EU legislation. Already in the initial negotiation agreement, very important issues were established, such as, for example, securing the liquidity and redemption of cryptoassets in such a way that they are backed by the value of reference currencies (1:1 rule). The issuer of cryptocurrencies will be obliged to ensure their redemption in the event

[10] *White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets*, The White House, 16 IX 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/ [accessed: 9 IV 2023].

of market turmoil. This is to ensure a high level of consumer and investor protection and the integrity of the crypto ecosystem, and to minimise the risks to financial stability and monetary policy that may arise from the widespread use of cryptoassets and DLT technology in practice[11].

The European Parliament is also working on a new regulation to tighten policy on virtual currencies by closing a regulatory loophole. The tightening is to oblige decentralised organisations such as DAOs[12], NFTs and DeFi platforms[13] to comply with AML rules on the same basis as traditional financial market players. In April 2023, the US Department of the Treasury published the world's first comprehensive risk assessment of illicit DeFi financing. It shows that criminals are keen to use the services of the 'decentralised finance' market primarily to benefit from ransomware attacks, theft, fraud, drug trafficking and proliferation financing, as well as activities in support of terrorism. The key factors facilitating such activities for them stem from DeFi's lack of AML/CFT and KYC procedures[14], the low degree of cyber-security of its protocols and the fact that its administrators often operate in jurisdictions that do not respect international legal

[11] *Proposal for a Regulation of the European Parliament and of the Council on markets in crypto-assets, and amending Directive (EU) 2019/1937*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593 [accessed: 9 IV 2023]; *Markets in crypto-assets (MiCA)*, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)739221 [accessed: 9 IV 2023].

[12] DAO (decentralised autonomous organisation) - a decentralised organisation that makes autonomous management decisions in accordance with the will of governance token holders, i.e. those with voting rights.

[13] DeFi (decentralised finance) - a decentralised financial system designed for an unlimited number of investors, dedicated blockchain platforms, financial products and services and their creators. DeFi uses fiat money, bank accounts or cashless payment systems in various ways, but the most important are cryptocurrencies, innovative distributed ledger protocols and smart contracts reminiscent of bank accounts and deposits, various forms of credit and financial derivatives. Individual and institutional clients provide the capital for the operation of DeFi and look forward to the return on the investments made, especially as the rate of earnings offered is often much higher than in the traditional capital market. On the other hand, investing in DeFi involves a relatively high risk of losing the funds involved or missing out on the benefits promised by the trader. The decentralisation of DeFi means that there is no single, leading organisation or institution that is responsible for the entire system or its individual components. See: P. Opitek, *Funkcjonowanie instrumentów finansowych*..., p. 156.

[14] KYC (Know Your Customer) - the due diligence procedure that financial institutions and other legally defined entities must carry out to identify their customers (editor's note).

assistance mechanisms or cannot be linked to any territory at all[15]. The plan is therefore to oblige credit and financial institutions to apply stringent due diligence rules when executing crypto transactions exceeding €1k, and business relationships with commercial unlicensed entities would be completely prohibited. The same limit of €1k would apply to transfers originating from self-hosted wallets, when identifying the identity of the holder of such a wallet is much more difficult. EU authorities have also proposed the establishment of a new AML authority to oversee and enforce AML rules across all 27 EU countries[16].

In Polish law, the only legal definition relating to blockchain-anchored digital tokens is found in the *Act of 1 March 2018 on countering money laundering and terrorist financing* (hereinafter: AML/CFT Act). It is made up of two elements: it says what virtual currency is not (e.g. legal tender), and it lists its positive characteristics, such as: digital representation of value, exchangeability in business for legal tender, acceptability as a means of exchange, the possibility of electronic storage or transfer, or the possibility of being subject to electronic commerce. Although a detailed legal analysis of this definition[17] is beyond the scope of this article, it should be noted that in practice its interpretation and application poses many difficulties. There is no doubt that it applies to bitcoin and other altcoins, but one gets the impression that the financial market regulators are unable to clearly address the question of whether Article 2(2)(26) of the AML/CFT Act also applies to stablecoins or NFT tokens. One can risk the thesis that the Polish legislator does not intend to take independent steps towards tighter regulation of the crypto market, but instead waits for changes being processed in the European Parliament. This is partly justified by the fact that the common European policy on cryptocurrencies is shaped at the EU level and there is no point in introducing specific national solutions on the eve of the entry into force of regulations such as the MiCA.

[15] *Illicit Finance Risk Assessment of Decentralized Finance*, U.S. Department of the Treasury, April 2023, https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf [accessed: 14 IV 2023].

[16] I. Preiss, *Crypto AML rules passed by MEPs*, The Block, 28 III 2023, https://www.theblock.co/post/223215/crypto-aml-rules-passed-meps [accessed: 6 IV 2023].

[17] Such an analysis was carried out in the article: G. Ocieczek, P. Opitek, *Analiza definicji walut wirtualnych z ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* (Eng. Analysis of the definition of virtual currencies from the Act of 1 March 2018 on the prevention of money laundering and terrorist financing), "Consilium Iuridicum" 2022, no. 3–4, pp. 122–139.

Money laundering using virtual currencies

The offence of money laundering is stipulated in Article 299 of the Criminal Code[18] and presupposes, as an object of protection, the security of economic turnover and the legitimate origin of property values. Of the objects of the executive action described in this provision, such as means of payment, financial instruments, securities, it is virtual currency that will fall within the scope of the property right. This is because the concept of a property right refers to all rights that realise the economic interest of the right holder and comprise their assets[19]. According to Chainanalysis' *Crypto Crime Report*[20], between 2017 and 2022, virtual currencies were used in 'laundering' to the tune of more than $33 billion, with a significant proportion of this value being transferred using online exchanges. In 2021 alone, this volume amounted to almost $9 billion, of which more than 750 million was transferred to DeFi platforms. Observed trends indicate that decentralised finance platforms are becoming an increasingly popular environment for investing illicitly obtained funds, and 2022 was a record year in this respect[21]. This has resulted in the aforementioned work by the European Parliament and the US administration to bring DeFi more tightly under AML regulation.

The professional experience of the article's authors also confirms that virtual currencies are used to commit various types of crimes, including drug trafficking, arms smuggling, fraud, tax evasion, cyber attacks, paying for sabotage and diversion activities, human trafficking and acts of child sexual exploitation. Cryptocurrencies have been seen as a potential source of funding for corruption for some time, but studies of this phenomenon have been general in nature and based more on conjecture than on a convincing methodology[22]. However, the case of Sam Bankman-Fried has shown that such criminality does exist. Bankman-Fried was accused by a US prosecutor of embezzling billions of dollars paid by defrauded

---

[18] *Act of 6 June 1997 – Criminal Code*.

[19] *Prawo cywilne – część ogólna* (Eng. Civil law - general part), M. Safjan (ed.), series: System Prawa Prywatnego, vol. 1, Warszawa 2007, p. 717.

[20] Chainalysis, *The 2022 Crypto Crime Report*, February 2022.

[21] Ibid.

[22] See: M. Alnasaa et al., *Crypto, Corruption, and Capital Controls: Cross-Country Correlations*, International Monetary Fund, 25 III 2022, https://www.imf.org/en/Publications/WP/Issues/2022/03/25/Crypto-Corruption-and-Capital-Controls-Cross-Country-Correlations-515676 [accessed: 4 V 2023].

customers to his cryptocurrency operating company called FTX.com. The investigation found that in a bid to secure favour with politicians, Bankman-Fried made millions of dollars in donations to the election campaigns of both Democratic Party and Republican Party[23]. In addition, in November 2021, he was alleged to have given a bribe of $40 million to at least one Chinese official in exchange for inducing the Middle Kingdom to unblock $1 billion worth of cryptocurrencies seized by Chinese law enforcement authorities[24].

In addition, it appears that transnational criminal organisations are increasingly using digital tokens to transfer and conceal profits from drug trafficking. This is particularly true in Latin American countries, where illicit groups use exchanges operating without KYC and AML procedures to 'launder' billions of dollars a year and, by this means, transfer part of their financial resources to the virtual world in order to avoid prosecutorial detection and confiscation of the 'fruits of the crime'. This includes Mexico's Cártel Jalisco Nueva Generación and Sinaloa Cartel, as well as Central America's Mara Salvatrucha and Brazil's Primeiro Comando da Capital. In the same geographical areas, a growing number of corrupt governments are specifically deregulating the crypto market so that funds invested therein obtained through bribery remain anonymous. Such actions coincide with the interests of Russia, whose allies in South America, such as the Maduro regime in Venezuela, have developed their own cryptocurrency systems to avoid sanctions imposed on the Russian Federation by Euro-Atlantic states and bypass Western currency markets. Venezuela's petro cryptocurrency is used to transfer value between Venezuela and Russia via Russian banks[25]. Such activity was the subject of an indictment filed by the prosecutor in October 2022 in Federal Court in New York. Five Russian nationals were charged therein in connection with illegal purchases of military technology for the Russian Federation (including

[23] *United States of America v. Samuel Bankman-Fried*, https://storage.courtlistener.com/recap/gov.uscourts.nysd.590940/gov.uscourts.nysd.590940.80.0.pdf [accessed: 9 IV 2023].

[24] M. Sigalos, R. Goswami, *Sam Bankman-Fried paid over $40 million to bribe at least one official in China, DOJ alleges in new indictment*, CNBC, 28 III 2023, https://www.cnbc.com/2023/03/28/sam-bankman-fried-paid-over-40-million-to-bribe-at-least-one-chinese-official-doj-alleges-in-new-indictment.html [accessed: 9 IV 2023].

[25] D. Farah, M. Richardson, *The Growing Use of Cryptocurrencies by Transnational Organized Crime Groups in Latin America*, Georgetown University, 20 III 2023, https://gjia.georgetown.edu/2023/03/20/the-growing-use-of-cryptocurrencies-by-transnational-organized-crime-groups-in-latin-america/ [accessed: 6 IV 2023].

advanced semiconductors and microprocessors used in fighter aircraft, missile and space military systems), its smuggling and money laundering using cryptocurrencies. Representatives of Petróleos de Venezuela S.A., Venezuela's state-owned oil company, were also involved in the crime-bearing procedure. The complex criminal scheme involved, among other things, the transfer of millions of dollars' worth of cryptocurrencies, which were used to purchase technology outside the official financial market, as well as to 'launder' the proceeds of illegal activities[26]. In this context, it may be added that on 2 March 2022, the US Attorney General established Task Force KleptoCapture as a law enforcement task force to enforce the extensive sanctions and export restrictions imposed on Russia.

In the European Union and the United States, standards for the regulation of the virtual currency market from an anti-money laundering perspective are shaped by the Financial Action Task Force (FATF)[27]. In 2021, it updated its guidance on a risk-based approach to virtual currency trading and Virtual Assets Service Poviders (VASPs)[28]. The FATF report *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*[29] (September 2020) identifies the technological advantages of crypto-assets and blockchain, but also the risks generated by the new technology. Abuses are fostered by the high anonymity of transfers, the operation of direct P2P value exchange services, 'tumblers' and 'mixers', as well as the different regulation of virtual currencies in different jurisdictions. Indeed, the very concept of a digital token is ambiguous in nature and individual tokens may differ in many respects. This translates into the action of the prosecutor,

---

[26] *Five Russian Nationals and Two Oil Traders Charged in Global Sanctions Evasion and Money Laundering Scheme*, United States Attorney's Office, Eastern District of New York, 19 X 2022, https://www.justice.gov/usao-edny/pr/five-russian-nationals-and-two-oil-traders-charged-global-sanctions-evasion-and-money [accessed: 7 IV 2023].

[27] The Financial Action Task Force was established in 1989 by the International Monetary Fund and currently has 37 member countries. The purpose of the FATF is to define standards and promote legal measures to combat money laundering, terrorist financing and other serious threats to the integrity of the global financial system. Although the FATF does not explicitly decide on the AML/CFT solutions adopted by individual countries, it is de facto instrumental in shaping them.

[28] A Virtual Asset Service Provider is a provider of a virtual platform and other services to manage virtual currencies.

[29] *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*, FATF, https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html [accessed: 7 IV 2023].

who is sometimes faced with the difficult task of determining what the cryptocurrencies revealed in the course of an investigation are.

The role of individual states in combating this crime is highlighted, as well as how they should monitor threats and assess the risks involved. The fight against money laundering on the crypto market remains a constant concern for the EU, and the countries of the Old Continent have either incorporated anti-laundering institutions into their legislation or are in the process of introducing new solutions. These include the *travel rule*, which relates to the transmission and sharing of transaction information by service providers operating in the virtual asset market. Such a solution increases the transparency of transfers and therefore the possibility of identifying those involved in operations and blocking suspicious funds. The implementation of the *travel rule* also reduces the risks associated with money laundering and terrorist financing, especially with regard to transfers of an international nature[30]. A further instrument for tidying up the crypto market relates to the obligation in each EU state to establish a register for virtual currency operators. On Polish soil, this has found expression in Article 129m of the AML/CTF Act. Entities obliged to register have the status of an obliged institution, which will be discussed later in this article. At this point, a question may be asked about the actual benefits of the functioning of the register[31], in which, as of 6 April 2023, there were 705 entities entered declaring the type of services they provide, i.e. exchange between virtual currencies and cash, between virtual currencies themselves, intermediation in such exchange and account maintenance for virtual currencies. In the authors' opinion, such an entry, declaratory in nature, currently serves more for companies to authenticate their activities, as affirmed by the state, than for the actual control of these companies by the authorities authorised under the AML/CFT Act.

Different countries implement AML/CFT policy obligations in different ways, and it is a priority of the FATF that the framework of the global

[30] *Anti-money laundering: Provisional agreement reached on transparency of crypto asset tra*nsfers, Council of the EU, 29 VI 2022, https://www.consilium.europa.eu/en/press/press-releases/2022/06/29/anti-money-laundering-provisional-agreement-reached-on-transparency-of-crypto-asset-transfers/ [accessed: 7 IV 2023].

[31] According to the law, the register is kept by the Minister of Finance and is actually managed by the Chamber of Fiscal Administration in Katowice (the register is located at the following address: https://www.slaskie.kas.gov.pl/izba-administracji-skarbowej-w-katowicach).

AML regime be uniform. The FATF documents recommend a functional approach. According to this, individual countries model the detailed legal solutions according to their internal, specific circumstances, but everywhere the implementation of the essential guidelines should be at a consistently high level. In the European Union, this task is carried out by the Committee of Experts on the Evaluation of Anti-Money Laundering and Terrorist Financing (Moneyval), which is a permanent monitoring body of the Council of Europe. The Committee is entrusted with assessing the compliance of national norms with international AML/CFT standards, the effective implementation of these norms, as well as making recommendations to state authorities on how to improve regulations in this field. The recommendations of the FATF and Moneyval therefore require countries to build efficient AML procedures, including the imposition of specific obligations on crypto-asset market participants, although each government can concretise the solutions adopted on a case-by-case basis[32]. Determinants in the implementation of EU directives include factors such as a country's political system, its economic development, the openness of a given society to innovation and its wealth.

Terrorist financing through cryptocurrencies

Cryptocurrencies have been linked to the activities of extremist organisations - since at least 2015, terrorists have been recorded trying to use bitcoins to create crowdfunding collections to fund their operations[33].

---

[32] P. Opitek, *Przeciwdziałanie praniu pieniędzy z wykorzystaniem walut wirtualnych w świetle krajowych i międzynarodowych regulacji AML* (Eng. Anti-money laundering using virtual currencies in light of national and international AML regulations), "Prokuratura i Prawo" 2020, no. 12, pp. 41–70, Lex, https://sip.lex.pl/komentarze-i-publikacje/artykuly/przeciwdzialanie-praniu-pieniedzy-z-wykorzystaniem-walut-151383722 [accessed: 7 IV 2023].

[33] *Statement of Stephanie Dobitsch, Deputy Under Secretary, Office of Intelligence and Analysis, Department of Homeland Security*, in: *Terrorism and Digital Financing: How Technology is Changing the Threat. Hearing before the Subcommittee on Intelligence and Counterterrorism of the Committee On Homeland Security House of Representatives*, 2021, https://www.congress.gov/117/chrg/CHRG-117hhrg45867/CHRG-117hhrg45867.pdf, p. 8 [accessed: 10 V 2023]. Polish law enforcement services have already discussed the topic of terrorism in 2018, including following a lecture by Paweł Opitek entitled *The use of cryptocurrencies in organised crime and terrorism* presented during a training course for prosecutors of the Department for Organised Crime and Corruption of the National Public Prosecutor's Office and officers

For the most part, these have been organised by groups operating in the Middle East with strong ideological motivations, but illegal activities involving cryptocurrencies and terrorism have also occurred in the United States, Western Europe and, more recently, Ukraine and Poland. US services reports have confirmed that new technologies, such as cryptocurrencies, enable terrorists to further expand and support their efforts to raise funds for illegal activities[34].

Financial support is needed to organise terrorist activities and its beneficiaries can be assisted by crypto-assets. The financing of terrorism through virtual currencies is linked, among other things, to Islamic fundamentalism and the circumvention of economic sanctions by states that do not fully comply with the financial market rules imposed by Western, liberal democracies. There was a debate in Islamic fundamentalist circles as to whether cryptocurrencies were permitted by the Shariah and whether Muslims should use them. Eventually, Al-Qaeda published a manifesto online in the summer of 2014 entitled *Bitcoin wa Sadaqat al-Jihad*[35]. It promoted the use of bitcoin as a convenient means of supporting the fight against infidels bypassing the Western banking system, which restricted donations to the jihad. The manifesto recommended pursuing cryptocurrency transfers for ideological and religious reasons, and described the technical virtues of virtual currencies: resistance to counterfeiting, anonymity of senders and recipients, global reach, and difficulty for law enforcement to detect payments. The superiority of the Bitcoin system over methods such as PayPal or eBay, which are top-down managed and centralised, was highlighted. The manifesto's creators aimed to develop a completely anonymous system for sending donations in bitcoin from the US, the UK, South Africa, Ghana, Malaysia, Sri Lanka or elsewhere in the world to a Mujahideen-managed DarkWallet address. The publication of such a tool has been announced (coming in 2019). In their conclusion, the manifesto's authors said that although the use

of the Central Bureau of Investigation of the Police and the Internal Security Agency, as well as representatives of other bodies, on combating terrorist threats, held in Waplewo on 5-7 November 2018.

[34] *Statement of Chairwoman Elissa Slotkin*, w: *Terrorism and Digital Financing: How Technology is Changing the Threat. Hearing before the Subcommittee on Intelligence and Counterterrorism...*, p. 3.

[35] *Bitcoin wa Sadaqat al-Jihad*, https://krypt3ia.files.wordpress.com/2014/07/btcedit-21.pdf [accessed: 20 I 2019].

of bitcoin faces various obstacles, with most kafirs using it to purchase drugs, the cryptocurrency can be used for a number of useful purposes: from purchasing weapons to donating to the mujahideen. This stance was one of the reasons for the emergence of many social media pages organising cryptocurrency collections for Islamic terrorists from various countries and organisations. The collections are not only conducted by entities directly linked to the criminals, but also by their sympathisers living in the United States or Europe.

Al-Qaeda has used forums and chat rooms on the open Internet since its inception, but after a large-scale service crackdown in 2000 and the arrests of several jihadist supporters, many platforms moved to the Darknet. Today, advanced jihadist forums protect themselves from surveillance by the services with cryptographic encryption, use tools such as Sigaint or TorBox, and access to the platform is verified by the administrator. Forums affiliated with radical movements, such as Shumukh al-Islam oscillating between ISIS and Al-Qaeda supporters, are emerging online[36]. In 2019, the Hamas' military wing (the Izz ad-Din al-Qassam Brigades) posted on social media and on their websites (alqassam.net, alqassam.ps, qassam.ps) a call for contributions in bitcoin for a 'terror campaign'. At the same time, the criminals were learning the rules of cyber security. Izz ad-Din al-Qassam Brigades initially requested that cryptocurrency be sent to a single address hosted on a US exchange, but later developed the technology to generate an individual address for each contribution to make it difficult to trace the origin and transfer of funds. The introduction of new solutions by terrorist groups indicates that they may be adapting to strategies that minimise risk and exploit various technological vulnerabilities[37]. Cyber-terrorist activity is not limited to crowdfunding. In early 2021, Al-Qaeda media offered a reward of 1 bitcoin, worth $60,000 at the time, to the person who murders a police officer in a Western country. Two years earlier, Brenton Tarrant, the perpetrator of attacks on mosques in Christchurch, New Zealand, claimed to have made money from cryptocurrency trading. At the same time, a racially motivated extremist who attempted to carry

[36] B. Berton, *The dark side of the web: ISIL's one-stop shop?*, European Union Institute for Security Studies, June 2015, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_30_The_Dark_Web.pdf [accessed: 23 VIII 2019].

[37] *Risk Assessment. 2022 National Terrorist Financing*, Department of the Treasury, February 2022, https://home.treasury.gov/system/files/136/2022-National-Terrorist-Financing-Risk-Assessment.pdf, p. 22 [accessed: 10 V 2023].

out an attack at a synagogue in Germany testified that he received financial support in bitcoins[38]. There are many indications that the perpetrators of the terrorist attacks carried out on 13 November 2015 in Paris were supported by cryptocurrency transfers during their organisation[39].

The activity of online terrorists has been noticed and dissected by US law enforcement agencies, which have developed the most effective and advanced tools and methods to combat extremism on the Internet. In the United States, one of the main public bodies dealing with counter-terrorism is the Department of Homeland Security (DHS). Its representative stated at a 2021 Congressional hearing that the DHS, along with the Internal Revenue Service (IRS) and the Federal Bureau of Investigation (FBI), conducted a global cyber operation and dismantled the virtual infrastructure of the Izz ad-Din al-Qassam Brigades. Beginning in October 2019, undercover agents of Homeland Security Investigations (HSI), a counter-terrorism service, made bitcoin donations to terrorists in order to unravel the links of entities running online collections for Hamas. These actions enabled investigators to identify supporters of the organisation living in the United States and to carry out further tracking of transferred funds. Sixty-four unique channels of communication (including email addresses) were identified, allowing the donors' bitcoin wallets to be secured. The operation revealed the terrorists' modus operandi on the internet, including how they recruit supporters online, their funding methods, as well as the domains they use and their IT infrastructure, operating in the US, Canada, Russia, Germany and Saudi Arabia, among others. In July 2020, HSI and IRS special agents executed 24 federal search warrants, seizing cryptocurrency and securing data at numerous online exchanges and network service providers - email, VPNs, online payments. Servers were requisitioned and numerous domains and email boxes linked to terrorist activity were shut down. Friendly services around the world joined the cyber operation, allowing the seizure of terabytes of terrorist-controlled data, hundreds of bitcoin wallets, cryptocurrency worth several million dollars and the dismantling of sites designed for bitcoin donations. Another 2020 investigation by the HSI, IRS and FBI had to do with 24 cryptocurrency accounts identified as foreign assets or

[38] *Statement of Stephanie Dobitsch...*, p. 8.

[39] See i.a.: Y.B. Perez, *Bitcoin, Paris and Terrorism: What the Media Got Wrong*, CoinDesk, 6 III 2023, https://www.coindesk.com/bitcoin-paris-and-terrorism-what-the-media-got-wrong [accessed: 10 V 2023].

sources of influence for Al-Qaeda. The cyber operation concerned the use of cryptocurrency to support and finance terrorism, and 60 virtual wallets were seized as a result[40].

Activities targeting terrorist financing using virtual currencies are regarded by the US government as an important front in the fight against international terrorism. This is confirmed by the 2020 *National Strategy for Combating Terrorist and Other Illicit Financing*[41] prepared by the United States Department of the Treasury. It argues that after the attacks of 11 September 2001, the authorities there focused on vulnerabilities in the financial system. At issue are abuses by charities and unlicensed remittances that allowed Al-Qaeda to transfer money internationally to fund terrorist attacks. After the attack on the World Trade Center, some extremist groups abandoned global operations (complex and widespread attacks) and concentrated on the activities of individual terrorists. Radicalised individuals can carry out relatively inexpensive and uncomplicated, but casualty-producing attacks using knives, firearms and cars. Such activities are facilitated by online communication and cryptocurrency transfers made covertly directly to individuals' wallets, reducing the financial footprint[42].

However, the issue of 'cryptocurrencies and extremism' does not only apply to terrorists, but also to other subversive organisations that threaten the stability and security of democratic states. Virtual crowdfunding is also used by neo-Nazi organisations. Extreme right-wing extremists active on the internet use cryptocurrencies, among other reasons, because they are

---

[40] *Statement of John Eisert, Assistant Director, Investigative Programs, Homeland Security Investigations, Immigration and Customs Enforcement, Department of Homeland Security* in: *Terrorism and Digital Financing…*, pp. 14–16. In 2021, the US Department of Justice announced the dismantling of the infrastructure of three campaigns conducted in cyberspace to finance terrorism, involving the Izz ad-Din al-Qassam Brigades. Sophisticated cyber tools were used in these campaigns, including soliciting donations in the form of cryptocurrencies from around the world. The campaign demonstrated, a US government communiqué proclaimed, how various terrorist groups have similarly adapted their terrorist financing activities to the cyber era. US authorities seized millions of dollars linked to the illegal activity, more than 300 cryptocurrency accounts, four websites and four Facebook pages. See: *Global Disruption of Three Terror Finance Cyber-Enabled Campaigns*, The United States Department of Justice, 13 VIII 2020, https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns [accessed: 9 V 2023].

[41] *National Strategy for Combating Terrorist and Other Illicit Financing 2020*, https://home.treasury.gov/system/files/136/National-Strategy-to-Counter-Illicit-Financev2.pdf [accessed: 7 VII 2023].

[42] Ibid, pp. 11–12.

associated with an ideology of deep-seated distrust of financial institutions as those controlled and managed by the 'Jewish finance'. The libertarian origins of the philosophy associated with the rise of bitcoin combining with a distrust of the global establishment also appeals to them. No less important are the purely practical issues surrounding the operation of cryptocurrencies. American neo-Nazis are being roughed out of popular crowdfunding platforms like Patreon, so they are creating alternative sites designed to make donations in the form of decentralised tokens. This is how Hatreon was created. Hosting companies refused to maintain it, so they changed domains to increasingly mask the platform's administrator[43].

Cryptocurrency collection, for example, is carried out by an online US neo-Nazi website called The Daily Stormer. It contains detailed instructions on how to make bitmoney transfers to the address provided there, and the recommended form of deposit is through cryptobanking machines. Andrew Anglin, the site's chief editor, who also publishes a magazine of the same title, is a well-known activist who implements successful crowdfunding campaigns for his organisation. Anglin has repeatedly extolled, including in the pages of The Washington Post, virtual currencies as an excellent tool for raising funds for activities fought by state authorities, and has confirmed that he has received significant donations from people supporting his projects and ideology.

Jihadist recruitment activities on the internet are often closely linked to crowdfunding-based appeals for financial assistance to terrorists. The ease of donating funds and the possibility to donate relatively small amounts can help an extremist organisation materially, while the donor's activity goes unnoticed by the AML system. An example of a completed cryptocurrency crowdfunding carried out for the benefit of militants of the so-called Islamic State was the case of Ali Shukri Amin. The man was born in Africa and emigrated to the United States with his mother when he was a few years old. He settled in Virginia and attended university there. He was interested in science subjects, cyber security topics, encryption and cryptocurrencies. At the same time, Amin radicalised himself and promoted his ideas on social media. Among other things, he set up a Twitter account called @AmreekiWitness, where he posted 7,000 tweets praising

[43] P. Opitek, *Wykorzystanie walut i serwisów wirtualnych do prania pieniędzy i finasowania terroryzmu* (Eng. Use of virtual currencies and services for money laundering and terrorist financing), Warszawa 2019, pp. 43–44 (diploma thesis written during post-graduate studies at the Warsaw School of Economics, unpublished, in the author's possession).

radical Islam and promoting financial support for ISIS through anonymous bitcoin transfers. In addition, he created the blog Al-Khilafah Aridat, where he encouraged the fight against the infidels, as well as producing a series of articles aimed at supporters of the so-called Islamic State. He described in detail how to communicate anonymously online and use encryption during illegal activity on behalf of terrorists. Amin also helped a male acquaintance to reach Syria via Turkey and join the Islamic State militants. In 2015, the prosecutor filed an indictment against him with the court[44], charging him with engaging with other identified and undetermined persons in terrorist activity involving material support and expert advice to foreign ISIS terrorists. The man was sentenced by the court to 11 years' imprisonment.

Obliged institution's responsibilities in the anti-money laundering regime

A pillar of the fight against the crime of money laundering is the AML policy, which must be carried out by obliged institutions. These are entities involved in the broadly defined trading of virtual currencies and, as such, specific obligations have been imposed on them by national governments to counter money laundering. Many of the AML activities relating to crypto-assets are similar to those that have long been associated with cash or e-money payments. However, given the specificity of risk management of transactions involving digital tokens, it is advocated that high requirements for the crypto market must be observed in relation to the activities there, e.g. obtaining a company licence, meeting prudential requirements to hold share capital guaranteeing liquidity, maintaining transparent accounting and periodic audits, holding reserve assets equivalent to the tokens issued. This guarantee fund, which protects investors, provides a financial safety net should, for example, the blockchain protocol be hacked and the underlying value 'stolen'. In view of such cyber threats, obliged institutions must comply with high requirements protecting the assets they hold, including cryptographic keys, and apply, embedded in corporate governance, professional control, risk management and reporting

[44] *United States of America v. Ali Shukri Amin*, CRIMINAL NO. 1:15-CR-164, https://www.investigativeproject.org/documents/case_docs/2826.pdf [accessed: 10 V 2023].

systems. These are accompanied by requirements for the company's internal record-keeping processes, anti-money laundering and countering the financing of terrorism, secure outsourcing, operational resilience of key services (ensuring continuity of the company's operations and high quality of service in the event of a failure of electronic systems or physical events such as fire or interruption of electricity supply). Challenges such as adopting appropriate insolvency and bankruptcy regulations for a company that has placed its assets in cryptocurrencies or provided services and sold products in the crypto market also need to be addressed[45].

The fight against money laundering and counter-terrorism, including virtual currencies, is based on common solutions implemented by the EU into the legal orders of the Union countries. The Fifth Anti-Money Laundering Directive (EU) 2018/843[46], which entered into force in June 2018, played a special role. In Poland, the regulations implementing the solutions contained in this act are effective from May 2021[47]. AML directives issued jointly by the European Parliament and the Council of the EU shape the rights and obligations of professional market participants, public administrations (including FIUs), and indirectly affect state criminal policy. The latter include the possibilities of enforcing obligations against obliged institutions, punishing those responsible for non-compliance, using sources of evidence or securing criminal assets.

In order for law enforcement authorities to take advantage of the opportunities offered by the provisions of the AML/CFT Act in Poland, it is necessary to know the mechanisms governing the AML regime in relation to obliged institutions, including entities engaged in the business of providing virtual currency services (Article 2(1)(12) of the AML/CFT Act). Such entities are obliged to draw up and apply (as well as update and verify) an internal anti-money laundering and counter-terrorist financing

[45] *UK regulatory approach to cryptoassets and stablecoins: Consultation and call for evidence*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950206/HM_Treasury_Cryptoasset_and_Stablecoin_consultation.pdf, p. 20–21 [accessed: 9 IV 2023].

[46] *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*, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32018L0843&from=en.

[47] *Act of 30 March 2021 amending the Act on counteracting money laundering and terrorist financing and certain other acts.*

procedure referred to in Article 50 of the AML/CFT Act. The aforementioned provision enumerates exhaustively what such procedure contains, taking into account the nature, type and size of the entrepreneur's activities, and the entire approach to financial security is based on risk estimation. This risk is the possibility of the actualisation of a threat (including the possibility of committing an offence) in relation to a specific customer of the obliged institution within the framework of the services provided by it. Such risks may be determined as minimal and then no special precautions are required. However, once the risk is assessed as high, enhanced financial security measures are implemented (in-depth investigation of the source of funds, identification of the beneficial owner), including the possibility for the obliged institution to terminate the business relationship with the client. It is already incumbent on the cryptocurrency company to assess the extent and frequency of the measures in question, and further tightening is planned. On 7 December 2022, the Council of the EU agreed on a position whereby a maximum cash payment limit of €10,000 will apply across the Union and, in addition, the anonymity of transfers will be reduced for crypto-asset trading, as all providers of such services will be required to carry out due diligence, i.e. a detailed assessment of the counterparty's current situation and the identification of existing and potential risks associated with the planned financial operation for transactions of €1,000 or more[48]. Already now, an obliged institution should take a closer interest in its client when typical symptoms indicating the possibility of money laundering using cryptocurrencies appear in its activity on the platform. These include the use of multiple accounts registered in the names of different persons, multiple conversions of funds held in accounts or conversions between money and virtual currencies without a specific business purpose, the client's use of ATMs, cash deposit machines cryptobanking machines or other devices that allow anonymous deposits or withdrawals of cash and virtual currencies without a reasonable justification in the person's transaction profile, or the use of non-standard payment methods such as Mistertango, N26, Revolut, Western Union, Wirex, PayPal, MoneyGram for transactions (funds entry or exit)[49]. The identification and assessment of AML/CFT risks

[48] *Fight against money laundering and terrorist financing*, https://www.consilium.europa.eu/en/policies/fight-against-terrorism/fight-against-terrorist-financing/ [accessed: 9 IV 2023].

[49] E. Przewłoka, *Metodyka podstawowych czynności realizowanych przez funkcjonariusza Policji i związanych z przestępstwem „kradzieży" waluty wirtualnej* (Eng. Methodology of basic actions carried out by a police officer and related to the crime of "theft" of virtual currency),

should take into account a number of factors, including those relating to the status of the clients (country of origin, size of the company and profile of its activities), the countries or geographical areas of their origin, the type of products and services offered by the counterparties and the channels of distribution of goods, the type of transactions performed. The catalogue of circumstances examined is not closed and is subject to adaptation to changing internal and external conditions in the environment of the entity involved in cryptocurrency activities.

The first request that ISA or any other special service conducting operations should make to an obliged institution whose activities are of interest to the service is to request the submission of an internal AML and terrorist financing procedure in order to check how the procedure was shaped, whether the document meets the requirements of the law and corresponds to the actual activities of the institution, and then to verify how the procedure was implemented in practice. If the document is sound, it will tell you who was responsible for what in the entity's AML policy, how the risks were estimated, where the metadata collected during remote contacts with counterparties is located and what it contains. In addition, enquiries can be made as to whether a particular client:

1. Concealed real personal data in business relationships?
2. Used an account (e.g. payment, bank, virtual currencies) established in the name of another person or pretended to be someone else in his/her dealings with institution staff?
3. Submitted documents raising concerns as to their authenticity or reliability?
4. Logged on to third-party accounts?
5. Declined to submit certain documents or to state the source of funds at his disposal?
6. In yet another way, he impeded the action of the obliged institution in carrying out its AML obligations?
7. Used ATM deposits or withdrawals with commitment of funds to the stock market[50]?

Other documents which, in accordance with Article 50(2) of the AML/CFT Act, constitute obligatory components of the obliged institution's internal AML procedure, i.e. rules on the application of financial security

Bydgoszcz 2023 (Police internal methodology, in the author's posession).

[50] Ibid.

measures, the retention of documents and information, the performance of duties involving the provision of information on transactions and notifications to the General Inspector of Financial Information (GIFI), the dissemination of knowledge of AML regulations among the obliged institution's employees and the reporting by employees of actual or potential violations of these regulations, internal audit, are also subject to examination.

The obligations enshrined in the AML policy of the obliged institution also apply to the analysis of the transactions made with virtual currencies themselves. The prosecutor may require the exchange to provide, in analytical form, information on the customer's order history (entry and exit of funds), the financial or cryptocurrency services and products (especially unusual ones) used by the customer, to submit an individual (currently in force and in the past if it has changed) assessment of the risk attributed to the person or institution, to verify whether it transferred or attempted to transfer funds to tax havens or sanctioned countries. As of 21 March 2023, cryptocurrencies are subject to sanctions imposed on Russia, i.e. provisions relating to the seizure of assets of certain persons, the prohibition of their sharing by such persons and any economic use. Cryptocurrencies should also not be used to circumvent any sanctions established under EU Council Regulation 833/2014[51]. Union entities are further prohibited from providing services related to the operation or provision of cryptocurrency wallets, accounts or custodial services related to crypto values to both Russian citizens and natural persons residing in the Russian Federation, in addition to legal persons and other entities established there. This means that European service providers should close the crypto accounts of their Russian clients and return the digital assets to them (possibly converting them into money or another category of assets that are not subject to sanctions) and, in the case of sanctioned individuals, freeze their assets. The sanctions provisions should be read in conjunction with the deposit limit set out in Article 5b of the said regulation and, in this respect, the conversion of crypto-assets into fiat deposits would only be possible up to the amount allowed for deposits[52].

---

[51] *COUNCIL REGULATION (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine*.

[52] *Crypto-assets. Relevant provision: Article 5b(2) of Council regulation (EU) NO 833/2014*, https://finance.ec.europa.eu/system/files/2023-03/faqs-sanctions-russia-crypto_en.pdf [accessed: 10 IV 2023].

The question of how effective the sanctions imposed on Russia are in practice remains open. According to a report by renowned analyst firm Inca Digital, based on an analysis of data collected from 163 cryptocurrency trading platforms around the world, including centralised and decentralised exchanges and P2P sites, as well as OTC (Over the Counter) Brokers[53], as many as 79 of them allow Russian citizens to purchase cryptocurrency (notably the P2P stablecoin Tether), and 11 out of 62 international platforms have no requirements for Russians to meet the KYC procedure before trading[54]. The Seychelles-based Huobi and KuCoin exchanges are the most user-friendly and widely used. They have not taken any steps to prevent sanctioned Russian banks from using their platforms and continuously allow transactions with debit cards issued by these banks, including Sberbank. According to Inca Digital, Binance too offers Russians various methods of converting the currency they hold into crypto, including using the OTC system and the P2P market bypassing the KYC procedure up to the equivalent of a $10,000 deposit, but this limit is easy to circumvent. Transactions can be concealed by, among other things, qualifying payments to non-Russian utilities. ByBit, which operates from Singapore, allows users to exchange Russian roubles for cryptocurrencies using a P2P marketplace and a fiat deposit. The situation described is a direct violation of US and European sanctions and confirms that the market under review is a loophole that limits Russia's economic opportunities. Although, due to the sanctions imposed, many exchanges have officially restricted their activities in the country and declare that they are blocking Russian users from accessing the services offered, in reality they continue, in a more or less veiled form, to cooperate with Russian

[53] The name refers to services provided by OTC brokers, which are primarily large cryptocurrency exchanges such as Kraken, Binance, Coinbase, Satstreet, facilitating direct cryptocurrency trading between two parties to a crypto-crypto (e.g. exchange of bitcoin for ethereum) or crypto-fiat money transaction. This is because traders with large amounts of wealth are looking for secure and anonymous channels for the unlimited exchange of wealth, under predetermined conditions, which are not formally listed on centralised exchanges. Negotiating transactions through OTC brokers between sellers and buyers can take place over the telephone or the web, or even provide for an in-person meeting between the parties.

[54] *How Russians Use Tether to Evade Global Sanctions*, Inca Digital, https://inca.digital/intelligence/how-russians-use-tether/ [accessed: 10 IV 2023].

citizens, including by allowing them to benefit from maximum limits on deposits, trading and withdrawals[55].

An immanent feature associated with the trading of virtual currencies is the difficulty of accessing information about the entities involved in the operations, as they usually operate via the Internet. Therefore, there is an emphasis in the legislation to control the digital footprint of such activities. It follows from the wording of Article 76 of the AML/CFT Act that the obliged institution is under a statutory obligation to have information or documents concerning, inter alia, the IP addresses from which the client's connection to the obliged institution's ICT system took place and the time stamps of the connections to the system. The collection of log histories by the prosecutor may allow a number of relevant data to be established about the person of interest, e.g. the geolocation of the electronic devices used and the frequency and time or period of his/her contacts with the obliged institution. Additional analysis of IP addresses in light of the evidence gathered may prove that:

- transactions were carried out from IPs previously used for illegal activities (e.g. fraud, phishing attacks, distribution of ransomware);
- transactions were carried out from sanctioned countries, tax havens or other "exotic" territory or countries supporting international terrorism;
- the person of interest to law enforcement authorities used tools that anonymise network traffic (Tor, VPNs, proxies);
- there are discrepancies between the IP addresses associated with the customer profile and those from which the transactions were initiated (it can be concluded from this that the person under investigation was a so-called 'strawman' and his personal data were used by the actual beneficiary of the transaction)[56].

---

[55] S. Sutton, L. Seligman, *Two major crypto exchanges failed to block sanctioned Russians*, Politico, 24 II 2023, https://www.politico.com/news/2023/02/24/two-major-crypto-exchanges-failed-to-block-sanctioned-russians-00084391 [accessed: 10 IV 2023]; *Crypto exchanges Huobi, KuCoin enabled Russian sanction evasion. Binance also mentioned*, Ledger Insights, 28 II 2023, https://www.ledgerinsights.com/russia-sanctions-crypto-exchanges-huobi-kucoin-binance/ [accessed: 10 IV 2023].

[56] J. Skała, *Uzyskiwanie przez prokuratora informacji i danych od instytucji obowiązanych na podstawie ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* (Eng. Obtaining information and data by the public prosecutor from obliged institutions under the Act of 1 March 2018 on the prevention of money laundering and terrorist financing), "Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury" 2022, n. 3, pp. 92–93. https://doi.org/10.53024/4.3.47.2022.

Crypto transactions should be categorised as higher risk and analysed in detail. In order to increase their transparency, on 29 June 2022 the Council and the EU Parliament reached a preliminary agreement to update the EU Regulation on information accompanying transfers of funds. The new rules will make it mandatory for providers of crypto-asset services to collect and make available certain information about the senders and beneficiaries of transfers. This is to ensure transparency of cryptocurrency transfers in order to better identify suspicious operations and block the funds involved[57]. This increased risk due to the anonymity of crypto transactions extends to other financial market participants (including banks) in addition to typical VASPs, who, although not involved in the trading of virtual currencies, are indirectly exposed to crypto money laundering because, for example, they maintain bank accounts in which funds from the exchange of digital tokens for fiat money are deposited.

An important category of obligations imposed on institutions is the notification to the competent state authorities of events that may constitute an offence or an attempt to commit an offence and notification of a reporting nature. In the latter case, it is a matter of providing the GIFI with information on accepted payments and withdrawals of funds, foreign exchange transactions and transfers exceeding a threshold of a certain monetary value, i.e. on suprathreshold transactions (art. 72 of the AML/CFT Act). Obliged institutions also notify the GIFI of circumstances that may indicate a suspicion that a money laundering or terrorist financing offence has been committed (art. 74 of the AML/CFT Act) and cases where a reasonable suspicion has been obtained that a transfer order or specific property values may be related to money laundering or terrorist financing (art. 86 of the AML/CFT Act). In such a situation, the platform administrator blocks the funds covered by the notification and further decisions on the fate of the assets are taken by the public prosecutor notified by the GIFI. In addition, Article 89 of the AML/CFT Act regulates the obligation to notify the competent public prosecutor on obtaining a reasonable suspicion that the assets transacted or accumulated in the account originate from or are connected to a crime other than the crime of money laundering or terrorist financing or a fiscal crime. The indicated 'blocking' procedures are described in detail in the mentioned articles, but it is worth noting the wording of some of the legal institutions described in the law.

[57] *Fight against money laundering and terrorist financing…*

Determining the status of a digital artefact in criminal proceedings

In the event that any cryptocurrency comes into the interest of a law enforcement agency, its technical and legal status must be established. This is because important issues depend on this, such as the possibility of fulfilling the elements of a crime through the mere possession or issuance of tokens (e.g. prohibited tokenisation of securities), the way in which actual power over digital property is taken (whether the crypto-assets are placed on a public or private blockchain, or perhaps have nothing to do with blockchain techniques at all), the possibility of searching for traces of the crime committed (location of the server). Determining the aforementioned status is not always easy, and although the largest number of cases involve bitcoin or similar altcoins (ethereum or litecoin), there are situations where it is quite challenging to establish all the characteristics of the token. This has happened in the case of parlours running illegal gambling games, where players purchased gaming points for money in the form of a digital representation of their value in a QR code. The research shows that Polish crypto-asset users have sophisticated tokens in their portfolios, the issuance of which on the domestic capital market is subject to numerous legal requirements, subject to supervision by regulatory authorities and often even prohibited. These include such digital assets specific to the DeFi market as PAXGOLD, USDT, COMP[58]. The majority of users further declared that they had used or invested in equity tokens similar to stocks or bonds, derivatives in the form of crypto-assets, and almost half held tokens resembling options, futures or swaps[59].

The centralised and decentralised crypto-asset market is growing and public authorities, not only in Poland but also globally, have great difficulty in navigating it and enforcing the legal obligations imposed on participants in this market. It is to be presumed that criminal acts in the form of financial embezzlement or money laundering carried out in an environment such as DeFi too often remain beyond any control of states and governments. The authors of this article are not aware of a case in which Polish law enforcement or capital market supervisory authorities have carried out sophisticated fraud-related activities in the decentralised finance market. In contrast, the US financial market regulator, The Securities and Exchange Commission (SEC), has been effective in this area. In August

[58] P. Opitek, *Funkcjonowanie instrumentów finansowych…*, p. 235.

[59] Ibid.

2021, it charged the defendants with conducting an unregistered sale of securities to the SEC for more than $30 million using smart contracts and decentralised finance technology, as well as misleading investors about the actual profitability of the products offered. The defendants operated as a company called Blockchain Credit Partners and issued and offered for sale on the DeFi Money Market platform two types of tokens called mTokens with significant returns and DMG tokens giving voting rights in a virtual company (DAO)[60]. The Commodity Futures Trading Commission (CFTC) regulatory agency in March 2023 accused the holding company Binance, the world's largest virtual currency trading platform, and its director Changpeng Zhao of offering digital token derivatives for sale to US citizens without the legally required registration with the CFTC in a civil action in federal court[61].

Another example of the variety of 'digital values' found in the virtual world is computer games, especially those played online. Artefacts in games can represent human characters, weapons (swords, guns), ammunition, parts of armour, objects hiding other things (chests, safes) or more abstract elements whose function represents some kind of value to the users of a given platform. Situations have been known where in-game artefacts have been used for money laundering[62] or have been the subject of assassination[63] or activities in support of terrorism. Where it is suspected that they fall within the modus operandi of the perpetrator of a crime, the legal status of such 'values' must be carefully established. An example of the importance

[60] *SEC Charges Decentralized Finance Lender and Top Executives for Raising $30 Million Through Fraudulent Offerings*, U.S. Securities and Exchange Commission, https://www.sec.gov/news/press-release/2021-145 [accessed: 24 III 2023].

[61] *CFTC Charges Binance and Its Founder, Changpeng Zhao, with Willful Evasion of Federal Law and Operating an Illegal Digital Asset Derivatives Exchange*, CFTC, 27 III 2023, https://www.cftc.gov/PressRoom/PressReleases/8680-23 [accessed: 5 IV 2023].

[62] P. Opitek, *Kryptowaluty w aspekcie czynności dochodzeniowo-śledczych Policji* (Eng. Cryptocurrencies in the aspect of police investigative activities), "Przegląd Policyjny" 2017, no. 2, p. 150. https://doi.org/10.5604/01.3001.0013.6082.

[63] In the verdict of the District Court for Kraków-Krowodrza, II Criminal Division, of 3 August 2012, ref. no. II Ka 776/11/K, the defendant was convicted for the fact that on 6 February 2011 in the city of K., in order to gain financial benefit, without authorisation, he influenced the transfer of information by breaking electronic security in such a way that he changed the access password to the e-mail box named "...@poczta.onet.pl" belonging to T. K., and took over his character in the game "Metin 2", named "Joker 78", thus leading T. K. to a disadvantageous dispossession of property in the amount of at least PLN 500, i.e. an act under Article 287 § 1 of the Criminal Code.

of properly assessing the nature of an artefact, and how a mistake can discredit a prosecutor, is the case concerning so-called 'skins' that is pending before the court. The defendant was found guilty by the District Court in Przasnysz[64] of an offence under Article 107 of the Fiscal Penal Code[65] in conjunction with Article 29a(1) and in connection with Article 2(1) of the *Act of 19 November 2009 on gambling games* (in the wording prior to 1 April 2017), consisting in the fact that between 2016 and 2017 he organised gambling games of a random nature on online platforms, in which the object of the winnings were the aforementioned skins. They are a type of feature used in the game C*ounter-Strike: Global Offensive* in the form of various types of weapons that the player can rent and in this way change the appearance of the artefacts used in the game[66]. Individuals who participated in the draw arranged by the accused submitted their skins to a virtual drum. These were then mixed and, depending on the rules of the platform in question, a randomly selected participant received the highest number of skins and the accused received a commission for organising the game.

In the wording prior to 1 April 2017, Article 2(1) of the Act on gambling games provided that (...) *games of chance are games, including those arranged via the Internet, for winnings in cash or in kind, the outcome of which depends in particular on chance*. Thus, the condition for the perpetrator to fulfil the elements of the offence was the court's recognition that the skin constitutes money or an object[67]. In the appeal filed against the conviction, the defendant's defence counsel argued that skin cannot be treated as money, as it is not issued by the National Bank of Poland, nor is it a tangible object, but only a piece of programming code, and therefore does not meet the definition of a thing under Article 45 of the Civil Code[68]. The Regional Court in Ostrołęka, 2nd Criminal Division[69], shared the argumentation

[64] Case file of the District Court in Przasnysz, 2nd Criminal Division, ref. no. II K 608/18.

[65] *Act of 10 September 1999 Fiscal Penal Code*.

[66] https://counterstrike.fandom.com/wiki/Skins [accessed: 17 II 2022].

[67] The charge in the indictment and judgment of the court of first instance states that "so-called skins - virtual keys that have a real monetary value in the real world and allow access to virtual weapons of varying strengths and attachments used in the battles of the 3D arcade game Counter-Strike Global Offensive (CS: GO for short) offered on the STEAM community platform owned by Valve Corporation based in Bellevue, Washington, USA" are at risk.

[68] *Act of 23 April 1964 – Civil Code*.

[69] Ref. no.: II Ka 40/20.

contained in the appeal and acquitted the accused of the alleged act in a judgement of 27 August 2020. In the justification for the verdict, the court indicated that the provisions of Article 2(1)(1) of the Act cannot be interpreted broadly and by analogy, and it is clear that skins do not have the status of things or objects, as they are virtual values[70].

In determining the legal status of a token, it is of fundamental importance to answer the question whether it constitutes a virtual currency, the legal definition of which is provided in Article 2(2)(26) of the AML/CFT Act. Carrying out such an assessment and providing an unambiguous answer as to whether a given asset is subject to the regime of the AML Act may prove very difficult, inter alia, because the aforementioned definition is very capacious and the phrases used therein are vague[71]. The classification of tokens as virtual currencies means that law enforcement authorities can enforce a number of obligations on an obliged institution dealing in such currency to provide information on suspicious persons and transactions. At the request of a law enforcement agency, the obliged institution should provide full data obtained during the first and subsequent client verification (KYC) and histories of the transactions performed by the client, news about possible reporting alerts to the GIFI on suspicious operations or a database of IP numbers that were used to commit a crime. Entities engaged in the business of providing services for exchanges between virtual currencies and means of payment or conversions between tokens themselves are furthermore required to submit, upon request by law enforcement authorities, the documentation set out in the AML Act, including, inter alia, the risk estimation procedure adopted and the attribution of the level of risk to a specific client[72]. A discussion of all

[70] Under the current state of the law, such behaviour would constitute an offence under Article 2(5) as amended by the *Act of 15 December 2016 amending the Act on gambling games and certain other acts* (Journal of Laws 2017, item 88), which reads: "Games on slot machines are also games on mechanical, electromechanical or electronic devices, including computer games, as well as games corresponding to the rules of slot machine games arranged via the Internet organised for commercial purposes, in which the player does not have the possibility of obtaining a prize in cash or in kind, but the game is of a random nature".

[71] For a detailed discussion of the various components of the definition of the term "virtual currencies", see: G. Ocieczek, P. Opitek, *Analiza definicji walut wirtualnych z ustawy*..., pp. 122–139.

[72] For a detailed discussion of the sources of evidence that law enforcement agencies may use in litigation and operational activities related to virtual currencies, see: J. Skała, *Uzyskiwanie przez prokuratora informacji i danych*...

the means and sources of evidence that can be used in a cryptocurrency investigation is beyond the scope of this paper, but what is certain is that the AML gives law enforcement agencies ample scope for action, which is poorly known among officers and too rarely used by them.

Operational work in the fight against cryptocurrency crime

Experience gained as a prosecutor shows that covert non-prosecution activities are an essential element in the successful fight against cryptocurrency crime. This is the case for several reasons. The perpetrators who commit such criminal acts are very cautious and usually operate in an environment of people at least as hermetic as organised drug trafficking groups or football hooligans. This is because the logistical facilities for trading cryptocurrencies are accessed remotely, so those using them operate in a virtual world, access to which may be irretrievably lost with the closing of their laptop matrix. This is one of the reasons why, in recent years, the methodology for conducting searches of places occupied by suspects and securing electronic equipment belonging to them has been re-evaluated. Previously, the indisputable rule was that an officer participating in a search which revealed a working computer unit should not search the memory of the device himself, as he would alter the data record on the laptop, which would negatively affect the evidentiary value of the traces obtained from it. Today, a search of a flat or an arrest of a person is not infrequently preceded by operational activities aimed at revealing and seizing the perpetrator's open computer at the time of their execution. This provides the opportunity to gain access to a lot of valuable information and data stored on the device's memory or the cloud resources to which it connects. In this way, it is possible to seize digital assets as collateral, obtain passwords to access applications used to commit crimes or to access an account on a cryptocurrency exchange, check which websites and web services were used by the perpetrator, find out the content of their instant messaging conversations. If the computer is shut down, it is likely that a computer forensics expert will not be able to break the password securing access to the device, and even if they do, data stored in elusive RAM or access to artefacts stored by the offender on other servers will be lost.

Actions taken to seize an open computer may range from deception (e.g. entering a flat "as a postman"), through a forensic trap (provoking a criminal to open a laptop in a public place in order to seize it), to the use of advanced operational and reconnaissance activities. This can be preceded by covert surveillance of people and places, property intelligence or cooperation with a network service provider to which the suspect is a subscriber. Operational control, controlled purchase and controlled delivery are also involved. There have been cases where law enforcement agencies have purchased bitcoins, set up their own darkmarket accounts and purchased drugs offered on the platform in order to establish the channels of transmission of prohibited substances, the method of their delivery and to obtain a quasi-forensic opinion on physicochemical testing, as well as to establish what drugs they are dealing with under the Act on counteracting drug addiction[73].

The effectiveness of covert operations in cyberspace aimed at combating cryptocurrency-related crime is confirmed by the experience of the US services. This includes the use of an undercover officer operating on the internet or determining the location and shutting down servers storing illegal content. The physical seizure of a server is a major success, as it contains traces that provide law enforcement agencies with valuable information on hundreds of individuals conducting illegal activities using IT infrastructure. However, such a takeover is no small challenge and is usually only possible through international cooperation. On 28 February 2023, German and Ukrainian police, with the support of Europol, Dutch police and the FBI, arrested members of a criminal group responsible for ransomware cyber attacks based on DoppelPaymer and Dridex software and targeting the critical infrastructure of private companies. The ransomware was distributed through various channels, including phishing and documents containing malicious JavaScript or VBScript code attached to spam emails. One of the most serious attacks was launched against the University Hospital in Düsseldorf, and in the US, victims paid at least €40 million in cryptocurrency to decrypt their data[74].

[73] *Act of 29 July 2005 on counteracting drug addiction.*

[74] *Germany and Ukraine hit two high-value ransomware targets*, Europol, https://www.europol.europa.eu/media-press/newsroom/news/germany-and-ukraine-hit-two-high-value-ransomware-targets [accessed: 6 IV 2023]. Elissa Slotkin, President of Intelligence and Counterintelligence for the US Congress, during testimony before Congress in 2021, spoke of the ransomware terrorist attacks in the US at the time, "which struck at

The characteristics of ransomware are likened to terrorist attacks in that they pose a serious threat to national security. Like terrorism, ransomware focuses on soft targets such as civilian critical infrastructure, but unlike terrorism it is primarily motivated by financial considerations[75]. However, it is sometimes difficult to draw a clear line between the two cyber threats. The North Korean government, for example, has been responsible for many major ransomware attacks on critical infrastructure around the world. In 2021, the US Department of Justice announced the indictment of three North Korean government officials suspected of carrying out some of the most dangerous cyber attacks, including WannaCry 2.0 (the ransom for decrypting data was paid in cryptocurrency), the hacking of the Sony Pictures database and the Bank of Bangladesh. The indictment alleges that the hackers are members of the Korean military intelligence service, linked to the hacker group called Lazarus, which has been involved in cyber operations for years[76]. The Korean lead was also attributed to a sophisticated and camouflaged cyber-attack on the Polish Financial Supervisory Authority's ICT system carried out in 2021. Although all the attackers' objectives are still not public today, one of them was to penetrate the trusted internal network of the banking systems, take control of the computers located there and establish communication between the victim's systems and the infrastructure controlled by the criminals[77].

---

the heart of everyday life in America, from gas pipelines and meat and plant processing to the operation of schools and hospitals", and at her meeting with constituents, "the first questions from farmers were about cyber attacks, cryptocurrency and what the government has done to protect them". See: *Statement of Chairwoman Elissa Slotkin*, p. 2.

[75] *Ransomware Attacks on Critical Infrastructure Sectors*, U.S. Department of Homeland Security, https://www.dhs.gov/sites/default/files/2022-09/Ransomware%20Attacks%20.pdf, p. i [accessed: 11 V 2023].

[76] M. Dugas, *The Latest North Korea Cyber Indictment Should Serve as a Model*, Just Security, 24 II 2021, https://www.justsecurity.org/74930/the-latest-north-korea-cyber-indictment-should-serve-as-a-model/ [accessed: 11 V 2023]. The indictment found that North Korea earned a total of more than $1.3 billion (the country's GDP is estimated at just $28 billion) through cyber-terrorism, i.e. bank hacking, cryptocurrency theft. The United Nations, meanwhile, estimated that in 2019 North Korea raised more than $2 billion in illicit financing from its cyber operations to fund its weapons programme.

[77] For more on the attack see: A. Maciąg, I. Tarnowski, *Atak teleinformatyczny na polski sektor finansowy* (Eng. ICT attack on the Polish financial sector), Rządowe Centrum Bezpieczeństwa, https://archiwum.rcb.gov.pl/atak-teleinformatyczny-na-polski-sektor-finansowy/ [accessed: 11 V 2023].

Effective action against organised crime groups operating on the Internet requires the formation of operational teams made up of representatives of various law enforcement services, and often international cooperation. In the United States, a special unit called J-CODE (Joint Criminal Opioid and Darknet Enforcement) has been created to combat cybercriminals, which is made up of seven institutions, including the FBI, HSI, the Department of Justice and The Postal Inspection Service. It follows that border guards, customs inspectors and the postal service have an invaluable role to play in combating the virtual trade in prohibited substances, as the delivery of goods ordered via the Internet is the point at which the virtual world of criminals meets the material world, and the resulting situation makes it possible not only to seize the illegal goods, but also to take other measures to identify and apprehend the criminals[78]. The state of affairs observed in one of the national services, in which the division dealing with asset recovery was separated from the units carrying out operational and exploratory and investigative activities, is therefore inadvisable. Effective combating of cryptocurrency crime, including the realisation of property seizure on digital tokens, requires constant cooperation and rapid flow of information between persons dealing with various aspects of combating crime, i.e. operational work, investigative work, asset recovery. *A contrario*, a person involved in the recovery of criminal assets will have serious difficulties in carrying out this task in relation to crypto-assets if he or she is not at all involved in the procedural activities of searching or interviewing a witness or does not have access to ongoing information from non-procedural arrangements.

The problem of the application of operational control in the form of obtaining and recording data contained in IT data carriers, telecommunication terminal devices, IT and ICT systems[79], i.e. control of the terminal device, is interesting. It can be stated with certainty that today's fight against cybercrime requires the use of such a method of operational work, as criminals mainly contact each other via devices that form the Internet. The law explicitly allows the obtaining of data recorded on the device's disk as one of the forms of operational control.

[78] P. Opitek, *Biegły z zakresu kryptowalut w sprawach karnych* ((Eng. Cryptocurrency expert in criminal cases), in: *Wokół kryminalistyki. Nauka i praktyka. Księga pamiątkowa dedykowana Profesorowi Tadeuszowi Widle*, D. Zienkiewicz (ed.), Toruń 2021, p. 434.

[79] This method of control is provided for in the laws governing the work of the police and the nine services.

At present, the efforts of the Police, as well as the Internal Security Agency and the Central Anticorruption Bureau, should focus on increasing the technical capabilities for operational control of the memory of a laptop, phone, modem or router in a passive manner, i.e. without modifying the digital traces present in the controlled object. Ideally, operational control of a hardware cryptocurrency wallet would be included, although technically this is a difficult task to achieve. This would make it possible, among other things, to know the entire transaction history, the current balance of bitcoins contained in the device or even the realisation of a property seizure on the disclosed cryptocurrencies[80]. Similar information would be provided by subjecting to control in the form of obtaining and recording the content of correspondence, including correspondence conducted via electronic means of communication, the so-called 'figurehead' account established on the exchange, to which additional data is sent, such as codes for withdrawing money at an ATM after the conversion of crypto into fiat money. It is true that on the basis of a letter or an order of the public prosecutor, the exchange administrator can be requested to submit the aforementioned data, but taking control of the account would help in obtaining up-to-date information and planning in advance the execution of tasks. Looking more broadly, it makes sense to introduce a new method of operational control in the form of uninterrupted ("on-the-fly") tracking of transfers of non-cash money, other means of payment or crypto-assets by establishing a new statutory form of operational work[81].

Traditional methods and forms of operational work are applied in the fight against cryptocurrency crime. For example, a police or secret service officer operating on an online platform under the guise of its real user is given the status of an undercover officer, with all the consequences this entails. Thus, an operational combination takes place in the form of, for example, the controlled purchase of drugs by an agent, followed

[80] The statement that the wallet contains units of virtual currency is a mental shortcut. This is because, in reality, the wallet contains the digital data to manage the altcoin units in the form of a so-called public and private key, but the tokens themselves are mapped to a ledger called a blockchain in the form of a digital data record.

[81] See in more detail: P. Opitek, *Kontrola transferów pieniądza bezgotówkowego w czasie rzeczywistym jako nowa forma czynności operacyjno-rozpoznawczych na przykładzie ustawy o Agencji Bezpieczeństwa Wewnętrznego (postulaty de lege ferenda)* ((Eng. Real-time control of non-cash money transfers as a new form of operational and reconnaissance activities on the example of the law on the Internal Security Agency (de lege ferenda postulates)), "Prokuratura i Prawo" 2021, no. 2, pp. 154–175.

by a controlled delivery. The aim is to unravel the environment of those involved in the online trafficking of illicit substances, to establish how the drugs are shipped and delivered to the customer, the chemical composition of the substances and how the buyer and seller communicate. The cryptocurrencies used to pay for the establishment of an account or to pay the price of goods will come from the service's operational fund, and the operations carried out with them are documented in detail until the costs of the actions taken are fully accounted for. These operations must be properly documented in the form of notes of the activities carried out at each stage of the special operation, accompanied by screen shots, and preferably a video recording, documenting what the undercover officer is doing in cyberspace. Snapshots of instant messaging conversations conducted by an agent with lawbreakers are important, as this is most often the form in which cybercriminals pass information to each other. Documents from the activities carried out, which constitute evidence of a suspected crime, should be made available in due course by the Chief of Police or the Head of a special service for criminal proceedings.

Investigation into cryptocurrency crime

2022 was a record year in terms of the number of trainings and conferences on virtual currencies organised by Polish law enforcement agencies. Most attention was devoted to the topic of property seizure on cryptocurrencies. It turns out, however, that the strictly procedural implementation of the security itself (i.e. the issuance of relevant decisions by the prosecutor) is easier than the disclosure of criminally derived bitcoins and the actual taking of their self-possession. Investigating cryptocurrency crime in cases of high gravity or where there is a real possibility of prosecuting specific individuals is an arduous detection process associated with the collection of extensive evidence. The success of this investigation depends on the knowledge and determination of those conducting it, and sometimes it is also determined by luck.

The criminal proceedings in question require skills in collecting digital traces and evidence not only from Polish and foreign providers of network services, such as cryptocurrency exchanges and bureaux de change, but also from Internet providers, telecommunications operators or financial institutions, led by banks. Administrators of industrial monitoring

systems (recordings of ATM withdrawals), national road administrators (registration of vehicle movements), carriers in air transport, entities operating the BLIK fast payments or administrators of online shopping platforms may also have valuable information for the investigation. Nevertheless, cryptocurrency exchanges remain the source of the largest amount of data. They can be requested to release information on:

- personal data of the exchange user, which is collected during the KYC procedure and can be changed during the customer's use of the platform (name, surname, date of birth, personal identification number, telephone number, home address, etc.);
- a scan of documents confirming his or her identity (identity card, driving licence, passport, etc.) and other documents submitted by the client in the course of using the services offered by the exchange (e.g. declaration of the source of funds invested);
- information on transactions carried out in virtual currencies and fiat money (list of transactions, their date, value of operations, beneficiary of funds received);
- the date of access to the exchange system by a potential perpetrator (submission of a summary of logins to the platform by persons of interest to law enforcement authorities, including any attributes in the form of IP addresses of ports with an indication of the exact time of log-in, BTS location, IMEI/MAC numbers of the device initiating Internet connections). In addition, check whether a new trusted device has been added for logins to the exchange account and the details of the devices from which logins occurred (operating system, system version, screen resolution, browser version);
- the history of the exchange user's account (codes sent to carry out ATM transactions, information and warnings received from the exchange administrator);
- information on whether transaction anomalies occurred during the course of the business relationship with the customer (e.g. a transaction was not completed because funds came from an address deemed to be suspicious, bank accounts or virtual currency addresses were blocked, transactions were stopped - if so, when and why);
- records of telephone or video conference calls made between exchange staff and the suspected person;

– reporting by the obliged institution to the GIFI, the prosecutor's office or another public authority on an exchange user (when and for what reason the report was issued);
– withdrawals of 'stolen' funds, notably the destination wallet address to which the funds were withdrawn and the transaction identifier (transaction *hash*).

The procedures and extent of data (e.g. logs) and information (transaction history) that can be obtained from exchanges depend on several factors, including the location of the exchange, the type and amount of data left on the platform by its user or the stage of the criminal proceedings. Law enforcement authorities and online service providers have developed a number of rules of cooperation. Sometimes obtaining the content requested by the prosecutor is done on the basis of a pleading. The request should indicate the officer and the unit conducting the case, the reference number of the proceedings, contain a brief description of the case indicating what offence the requested person is charged with. It should be sent electronically to the official contact point of the exchange, information about which is usually held by law enforcement authorities. The letter should be written in English or in the language of the country where the exchange operates. The main document should be a scan of the official letter and the attachment with the details should be sent in editable form so that it is possible to copy the data (e.g. cryptocurrency addresses) and further work on them. If the matter is of an urgent nature, this should be made clear in the letter. Importantly, as some exchanges inform their customers of an investigation against them, it is possible to stipulate in the request that the network service provider should refrain from doing so, and to justify this request.

There are, however, jurisdictions where obtaining information other than metadata (non-content data) will be conditional on a warrant being issued by the locally competent court. In such cases, requests for international legal assistance are made on the basis of agreements between sovereign states, which in practice significantly prolongs the process of collecting artefacts. This includes the United States, the territory with the largest number of network service provider companies. In Europe, the European Investigation Order commonly used by police officers and prosecutors is proving helpful. A person dealing with cryptocurrency crime must therefore be familiar with both the legal and practical aspects

of obtaining evidence, as the procedure involved depends on several factors:

- the company's headquarters and the location of the data server;
- the type of data in question: content data or non-content data (the latter are often made available in a deformalised manner);
- the procedure followed: "freezing" the data pending authorisation of its transfer, the procedure for obtaining the relevant data or the urgent obtaining of data in emergency cases);
- the internal policy of the entity obliged to provide information and data management.

Ultimately, if an exchange or other digital platform refuses to comply with the legally prescribed procedure for the release of data and information, or makes it significantly more difficult, one may consider seizing its server in order to extract the necessary artefacts or check that they have not been removed from it. Sometimes the vision of the inevitability of the seizure of the infrastructure leads to an opening for cooperation on the part of the service provider. Such actions are not possible with respect to darkmarket actors, where the location of their infrastructure is unknown, and in countries that do not cooperate with international legal assistance.

Another important piece of information for an investigation with a cryptocurrency thread is recorded on the electronic equipment used by end users of the Bitcoin protocol, most notably their phones and computers. There are artefacts on the secured evidentiary media to determine whether its user has used virtual currencies, connected to sites designed to handle them, and there may be traces or information (passwords, logins, etc.) in the computer's memory, including operational RAM, to authorise access to databases, i.e. applications, cloud resources or cryptocurrency wallets. If any system reveals data stating digital tokens and belonging to a suspect, it must be secured immediately for an ongoing investigation. To this end, the authors postulate that an operational and investigative group should be created in one of the leading special services in the area of the economic security of the Republic of Poland (e.g. the ISA) or the Police, consisting of officers who will have competences related to securing bitcoins and have the technological background to take possession of them. This refers to such skills as the visual inspection or search of the computer evidence system of the computer at the place of its disclosure, the handling of the electronic purse belonging to the perpetrators of the criminal act, but also to the possession by the formations fighting crime of their own hardware

wallet for accepting cryptocurrency, recognising the types of digital assets, generating addresses for them. Particularly important is the institution of property seizure on cryptocurrencies, as referred to in Article 291 § 1 of the Code of Criminal Procedure et seq. In Poland, such collateral has already been implemented for several years (the first one was executed in 2017), and the number is increasing every year. In order to seize bitcoin, police officers most often cooperated with online exchanges, which first froze the funds in the suspect's account and then created a special account for the prosecution and stored the object of the security there. There is also at least one known case of police officers generating a paper wallet, but it is most secure and practical for the services to have a hardware wallet such as Ledger or Trezor. The most difficult task in the course of operational or investigative activities seems to be to determine where the virtual currencies from the investigation are located and then to gain actual access to them with the possibility of transferring them to an address managed by the investigator. There are known cases in which, on the basis of criminal analysis of cryptocurrency transfers, addresses for storing significant amounts of tokens originating from crime, e.g. hacks on exchanges, were established, but they were not linked to any public Internet platforms, there were no findings regarding the persons managing these addresses and, consequently, the possibility of taking control over virtual funds. In such a situation, the only thing left to do is to flag such an address and thus monitor it in anticipation of the funds accumulated therein being transferred by someone to another, less anonymous address.

For bitcoin, which has already been seized by law enforcement, there are legal and factual difficulties with its storage. These are due to the fact that the price of virtual currencies is very liquid and subject to large exchange rate variations in short intervals, and that each wallet is vulnerable to hacking, mechanical or IT failure, and human error related to their handling may occur. In addition, Polish courts are not ready to seize cryptocurrencies that would be handed over with an indictment. A practical solution to these problems is the sale of secured assets during the investigation under Article 232 § 1 of the Code of Criminal Procedure. in conjunction with Article 236a of the Code of Criminal Procedure. They stipulate that items the storage of which would be connected with excessive difficulties or would cause a significant reduction in the value of the property may be sold according to the procedure specified for the competent authorities of the enforcement proceedings, and this

provision applies accordingly to digital tokens constituting IT data. The sale of the thing takes place in accordance with the provisions on enforcement proceedings in administration or those contained in the Code of Civil Procedure, depending on what was the basis for the seizure of the funds (Article 291 § 1, points 1-5 of the Code of Criminal Procedure). Another legal problem concerns the content of Article 295 § 1 of the Code of Criminal Procedure, which refers to movable property and bitcoin is not a thing within the meaning of Article 45 of the Civil Code. However, in practice, the institution of temporary seizure of movable property has already been effectively applied to virtual currencies and, moreover, Article 236b of the Code of Criminal Procedure, i.e. recognition of cryptocurrency as funds accumulated in an account and issuance of a decision on material evidence, may prove to be a solution in such a case.

Digital evidence relating to virtual currencies and, more generally, to the cybercrime committed should be properly collected, secured and then used in the investigation. The presentation of digital evidence in the course of criminal proceedings is based on the rule that it represents not only what can be seen, but also has metadata. This problem arose in the already mentioned case of the District Court in Przasnysz, in which the prosecutor, as evidence of the appearance and functioning of websites dedicated to skins, attached printouts of such websites to the indictment. In the pleading, the accused's defence counsel pointed out the unsuitability of evidence in the form of paper printouts of websites, which contained information which, according to the public prosecutor, constituted evidence of the commission of the offence charged against the accused. The accused's defence counsel argued that:

> (...) in the factual situation under examination, it is clearly the case that the taking of evidence indicated in the request for evidence cannot lead to the establishment of the circumstance indicated therein. The website is interactive in nature and a mere 'screenshot', printed on a piece of paper, does not reflect its essence and functioning. In the view of the defence counsel, the evidence of the circumstances referred to in the contested printouts of the websites should be carried out in such a way that the prosecutor, during the course of the evidence, reconstructs the functioning of the established websites. This is certainly technically possible (if only by saving the pages to

a permanent medium), but undoubtedly requires a little more effort on the part of the prosecutor[82].

The court shared the position of the defence and this, as well as many other mistakes made in the investigation, resulted in the acquittal of the accused. It follows that police officers should have had the knowledge, skills and due software for interactive visual inspection or web searches[83]. Particularly the latter activity, i.e. a cyber search, could be performed more often in the course of procedural activities, as it allows to obtain information and secure the most important evidence for the investigation, and yet the referents of criminal cases are either afraid to carry out such, in their opinion, difficult activities, or they do it without due diligence in the form of taking an official note, despite the fact that Article 143 § 1 (1) and (6) of the Code of Criminal Procedure requires a record to be made in this case.

Conclusions

The analysis of selected aspects of crime involving virtual currencies carried out leads to some basic conclusions. The role of cryptocurrencies in the activities of professional capital market players is steadily growing and more and more people are using this type of property. Cryptocurrencies are also used by criminals and the number of criminal cases related to cryptocurrency crime is increasing every year. Reports from public institutions and the authors' experience show that illegal activities involving crypto infrastructure can involve serious criminal acts harming the economic foundations of the state, serve to sponsor terrorism and espionage activities, corruption, circumvent sanctions, and therefore affect Poland's security and reputation internationally. This leads to the simple conclusion that law enforcement agencies, including the relevant special services, must have multifaceted capabilities (appropriately prepared people and logistical facilities) to work with cryptocurrencies, in both general (working with digital evidence, learning the essence of blockchain technology) and specific (the ability to use virtual wallets, redefining

[82] Case file of the District Court in Przasnysz, 2nd Criminal Division, ref. no. II K 608/18.

[83] See: P. Opitek, *Przeszukanie na odległość jako czynność procesowa (art. 236a k.p.k.)* (Eng. Remote search as a procedural act (Article 236a of the Code of Criminal Procedure)), "Prokuratura i Prawo" 2022, no. 9, pp. 100–128.

the work of an undercover officer in cyberspace, and perhaps creating an operational fund in the form of cryptoassets). It is obvious that not every officer of such an institution will be a specialist in cryptocurrencies, nevertheless they should immediately receive professional support when topics related to digital tokens arise in their proceedings. Furthermore, given that it is not always possible for a state security leader to cooperate with other law enforcement agencies specialised in fighting cybercrime, it is all the more reason for such an elite formation to have its own group (structure) of individuals specialised in the implementation of procedural and non-procedural activities related to cryptocurrencies (e.g. property seizure on bitcoin).

Looking more broadly, the Polish virtual currency market should be monitored for possible money laundering using binary values or circumventing sanctions imposed on Belarus and Russia. Instruments useful for the aforementioned tasks are offered by the AML/CFT Act. All the objectives regarding the minimisation of threats based on crypto-assets cannot be achieved without institutional cooperation between the ISA, the Public Prosecutor's Office, the GIFI and the FSA, as each of these institutions has specific legal tools and factual capabilities assigned only to it. Only their synergy offers the possibility to build an effective and comprehensive AML/CFT policy.

An analysis of the topic of cryptocurrencies has shown that they have also been used to support terrorist activities of a different nature - sponsorship of terrorist organisations using online crowdfunding, direct donations to a specific individual helping to organise or motivated to organise attacks, or cyber attacks targeting the ICT infrastructure of areas critical to the functioning of the state. According to information provided by an HSI representative, the number of criminal investigations involving cryptocurrencies in the US has increased from one in 2011 to more than 604 investigations in 2021. During this time, HSI has confiscated bitcoins and altcoins worth the equivalent of $79,825,606.65. This illustrates the increasing reliance of the perpetrators of the highest gravity of illegal acts on crypto-assets, and therefore implies the need for law enforcement agencies to gain competence to combat this type of terrorist financing[84]. And although the main sources of this financing still rely on traditional

[84] *Statement of John Eisert...*, pp. 14–16.

financial institutions[85] (it is estimated that cryptocurrency terrorist financing currently generates only 1 per cent of such transactions[86]), the problem is bound to grow. Perpetrators' modus operandi and approach to the virtual world are changing and evolving towards the most favourable solutions for them. Thanks to the successful actions of the US services against online platforms described in the article, the Izz ad-Din al-Qassam Brigades declared in April 2023 that it was suspending the collection of donations using bitcoin, citing an increase in 'hostile' activity towards donors. *This is out of concern for the safety of donors and to spare them any harm,* the Hamas announcement read[87]. At the same time they called for (...) *continued donations to Kassam and the resistance by all available means*[88].

Poland has been the subject of terrorist activities using the Internet infrastructure and cryptocurrencies. These include ransomware attacks targeting Poland or advertisements posted on the Darknet, which operates with bitcoin, encouraging the assassination of key named Polish politicians. Cryptocurrency issues are also linked to the activities of hostile intelligence organisations targeting Poland's security. It is therefore necessary for the most important state security services to increase their competence in the field of activity in the virtual world, the implementation of cyber operations and countering hostile IT attacks. This includes the ability to investigate cryptocurrency transfers, to secure such assets, but also to actively use them for their own purposes.

Bibliography

Chainalysis, *The 2022 Crypto Crime Report,* February 2022.

[85] *Risk Assessment. 2022 National Terrorist Financing...*

[86] *Statement of Ranking Member August Pfluger*, in: *Hearing before the Subcommittee on Intelligence and Counterterrorism...*, p. 3.

[87] N. Al-Mughrabi, *Hamas armed wing announces suspension of bitcoin fundraising,* Reuters, 28 IV 2023, https://www.reuters.com/world/middle-east/hamas-armed-wing-announces-suspension-bitcoin-fundraising-2023-04-28/ [accessed: 9 V 2023]; *Hamas armed wing to stop crypto fundraising over 'hostility' against donors,* i24NEWS, 30 IV 2023, https://www.i24news.tv/en/news/middle-east/palestinian-territories/1682688395-hamas-armed-wing-to-stop-crypto-fundraising-citing-hostility-against-donors [accessed: 9 V 2023].

[88] Ibid.

Ocieczek G., Opitek P., *Analiza definicji walut wirtualnych z ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* (Eng. Analysis of the definition of virtual currencies from the Act of 1 March 2018 on the prevention of money laundering and terrorist financing), "Consilium Iuridicum" 2022, no. 3–4, pp. 122–139.

Opitek P., *Biegły z zakresu kryptowalut w sprawach karnych* (Eng. Cryptocurrency expert in criminal cases), in: *Wokół kryminalistyki. Nauka i praktyka. Księga pamiątkowa dedykowana Profesorowi Tadeuszowi Widle*, D. Zienkiewicz (ed.), Toruń 2021, pp. 413–447.

Opitek P., *Funkcjonowanie instrumentów finansowych w oparciu o technologię blockchain* (Eng. Functioning of financial instruments based on blockchain technology), Łódź 2022.

Opitek P., *Kontrola transferów pieniądza bezgotówkowego w czasie rzeczywistym jako nowa forma czynności operacyjno-rozpoznawczych na przykładzie ustawy o Agencji Bezpieczeństwa Wewnętrznego (postulaty de lege ferenda)* (Eng. Real-time control of non-cash money transfers as a new form of operational and reconnaissance activities on the example of the law on the Internal Security Agency (de lege ferenda postulates)), "Prokuratura i Prawo" 2021, no. 2, pp. 154–175.

Opitek P., *Kryptowaluty w aspekcie czynności dochodzeniowo-śledczych Policji* (Eng. Cryptocurrencies in the aspect of police investigative activities), "Przegląd Policyjny" 2017, no. 2, pp. 138–158. https://doi.org/10.5604/01.3001.0013.6082.

Opitek P., *Przeciwdziałanie praniu pieniędzy z wykorzystaniem walut wirtualnych w świetle krajowych i międzynarodowych regulacji AML* (Eng. Anti-money laundering using virtual currencies in light of national and international AML regulations), "Prokuratura i Prawo" 2020, no. 12, pp. 41–70, Lex, https://sip.lex.pl/komentarze-i-publikacje/artykuly/przeciwdzialanie-praniu-pieniedzy-z-wykorzystaniem-walut-151383722.

Opitek P., *Przeszukanie na odległość jako czynność procesowa (art. 236a k.p.k.)* (Eng. Remote search as a procedural act (Article 236a of the Code of Criminal Procedure)), "Prokuratura i Prawo" 2022, no. 9, pp. 100–128.

Opitek P., *Wykorzystanie walut i serwisów wirtualnych do prania pieniędzy i finasowania terroryzmu* (Eng. Use of virtual currencies and services for money laundering and terrorist financing), Warszawa 2019 (diploma thesis written during post-graduate studies at the Warsaw School of Economics, unpublished, in the author's possession).

Prawo cywilne – część ogólna (Eng. Civil law - general part), M. Safjan (ed.), series: System Prawa Prywatnego, vol. 1, Warszawa 2007.

Przewłoka E., *Metodyka podstawowych czynności realizowanych przez funkcjonariusza Policji i związanych z przestępstwem „kradzieży" waluty wirtualnej* (Eng. Methodology of basic actions carried out by a police officer and related to the crime of "theft" of virtual currency), Bydgoszcz 2023 (Police internal methodology, in the author's posession).

Skała J., *Uzyskiwanie przez prokuratora informacji i danych od instytucji obowiązanych na podstawie ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* (Eng. Obtaining information and data by the public prosecutor from obliged institutions under the Act of 1 March 2018 on the prevention of money laundering and terrorist financing), "Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury" 2022, n. 3, pp. 83–100. https://doi.org/10.53024/4.3.47.2022.

Internet sources

Al-Mughrabi N., *Hamas armed wing announces suspension of bitcoin fundraising*, Reuters, 28 IV 2023, https://www.reuters.com/world/middle-east/hamas-armed-wing-announces-suspension-bitcoin-fundraising-2023-04-28/ [accessed: 9 V 2023].

Alnasaa M. et al., *Crypto, Corruption, and Capital Controls: Cross-Country Correlations*, International Monetary Fund, 25 III 2022, https://www.imf.org/en/Publications/WP/Issues/2022/03/25/Crypto-Corruption-and-Capital-Controls-Cross-Country-Correlations-515676 [accessed: 4 V 2023].

Anti-money laundering: Provisional agreement reached on transparency of crypto asset transfers, Council of the EU, 29 VI 2022, https://www.consilium.europa.eu/en/press/press-releases/2022/06/29/anti-money-laundering-provisional-agreement-reached-on-transparency-of-crypto-asset-transfers/ [accessed: 7 IV 2023].

Berton B., *The dark side of the web: ISIL's one-stop shop?*, European Union Institute for Security Studies, June 2015, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_30_The_Dark_Web.pdf [accessed: 23 VIII 2019].

Bitcoin wa Sadaqat al-Jihad, https://krypt3ia.files.wordpress.com/2014/07/btced-it-21.pdf [accessed: 20 I 2019].

CFTC Charges Binance and Its Founder, Changpeng Zhao, with Willful Evasion of Federal Law and Operating an Illegal Digital Asset Derivatives Exchange, CFTC, 27 III 2023, https://www.cftc.gov/PressRoom/PressReleases/8680-23 [accessed: 9 IV 2023].

Crypto-assets. Relevant provision: Article 5b(2) of Council regulation (EU) NO 833/2014, https://finance.ec.europa.eu/system/files/2023-03/faqs-sanctions-russia-crypto_en.pdf [accessed: 10 IV 2023].

Crypto exchanges Huobi, KuCoin enabled Russian sanction evasion. Binance also mentioned, Ledger Insights, 28 II 2023, https://www.ledgerinsights.com/russia-sanctions-crypto-exchanges-huobi-kucoin-binance/ [accessed: 10 IV 2023].

Dugas M., *The Latest North Korea Cyber Indictment Should Serve as a Model*, Just Security, 24 II 2021, https://www.justsecurity.org/74930/the-latest-north-korea-cyber-indictment-should-serve-as-a-model/ [accessed: 11 V 2023].

Farah D., Richardson M., *The Growing Use of Cryptocurrencies by Transnational Organized Crime Groups in Latin America*, Georgetown University, 20 III 2023, https://gjia.georgetown.edu/2023/03/20/the-growing-use-of-cryptocurrencies-by-transnational-organized-crime-groups-in-latin-america/ [accessed: 6 IV 2023].

Fight against money laundering and terrorist financing, European Council, https://www.consilium.europa.eu/en/policies/fight-against-terrorism/fight-against-terrorist-financing/ [accessed: 9 IV 2023].

Five Russian Nationals and Two Oil Traders Charged in Global Sanctions Evasion and Money Laundering Scheme, United States Attorney's Office, Eastern District of New York, 19 X 2022, https://www.justice.gov/usao-edny/pr/five-russian-nationals-and-two-oil-traders-charged-global-sanctions-evasion-and-money [accessed: 7 IV 2023].

Germany and Ukraine hit two high-value ransomware targets, Europol, https://www.europol.europa.eu/media-press/newsroom/news/germany-and-ukraine-hit-two-high-value-ransomware-targets [accessed: 6 IV 2023].

Global Disruption of Three Terror Finance Cyber-Enabled Campaigns, The United States Department of Justice, 13 VIII 2020, https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns [accessed: 9 V 2023].

Hamas armed wing to stop crypto fundraising over 'hostility' against donors, i24NEWS, 30 IV 2023, https://www.i24news.tv/en/news/middle-east/palestinian-territories/1682688395-hamas-armed-wing-to-stop-crypto-fundraising-citing-hostility-against-donors [accessed: 9 V 2023].

How Russians Use Tether to Evade Global Sanctions, Inca Digital, https://inca.digital/intelligence/how-russians-use-tether/ [accessed: 10 IV 2023].

https://counterstrike.fandom.com/wiki/Skins [accessed: 17 II 2022].

Illicit Finance Risk Assessment of Decentralized Finance, U.S. Department of the Treasury, April 2023, https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf [accessed: 14 IV 2023].

Living on the Edge, International Monetary Fund, October 2022, https://www.imf.org/en/Publications/REO/SSA/Issues/2022/10/14/regional-economic-outlook-for-sub-saharan-africa-october-2022 [accessed: 5 IV 2023].

Maciąg A., Tarnowski I., *Atak teleinformatyczny na polski sektor finansowy* (Eng. ICT attack on the Polish financial sector), Rządowe Centrum Bezpieczeństwa, https://archiwum.rcb.gov.pl/atak-teleinformatyczny-na-polski-sektor-finansowy/ [accessed: 11 V 2023].

MUFG's Progmat security token platform to become digital asset joint venture, Ledger Insights, 7 X 2021, https://www.ledgerinsights.com/mufg-progmat-security-token-digital-asset-joint-venture/ [accessed: 5 IV 2023].

MUFG, SBI share roadmap for Japanese security tokens, Ledger Insights, 7 X 2021, https://www.ledgerinsights.com/mufg-sbi-share-roadmap-for-japanese-security-token-platform/ [accessed: 27 III 2023].

National Strategy for Combating Terrorist and Other Illicit Financing 2020, https://home.treasury.gov/system/files/136/National-Strategy-to-Counter-Illicit-Financev2.pdf [accessed: 7 VII 2023].

O'Sullivan F., *Where Is Crypto Illegal in 2023? The Countries That Ban Cryptocurrency*, Cloudwards, 22 II 2023, https://www.cloudwards.net/where-is-crypto-illegal/ [accessed: 5 IV 2023].

Perez Y.B., *Bitcoin, Paris and Terrorism: What the Media Got Wrong*, CoinDesk, 6 III 2023, https://www.coindesk.com/bitcoin-paris-and-terrorism-what-the-media-got-wrong [accessed: 10 V 2023].

Preiss I., *Crypto AML rules passed by MEPs*, The Block, 28 III 2023, https://www.theblock.co/post/223215/crypto-aml-rules-passed-meps [accessed: 6 IV 2023].

Ransomware Attacks on Critical Infrastructure Sectors, U.S. Department of Homeland Security, https://www.dhs.gov/sites/default/files/2022-09/Ransomware%20Attacks%20.pdf [accessed: 11 V 2023].

Risk Assessment. 2022 National Terrorist Financing, Department of the Treasury, February 2022, https://home.treasury.gov/system/files/136/2022-National-Terrorist-Financing-Risk-Assessment.pdf [accessed: 10 V 2023].

SEC Charges Decentralized Finance Lender and Top Executives for Raising $30 Million Through Fraudulent Offerings, U.S. Securities and Exchange Commission, https://www.sec.gov/news/press-release/2021-145 [accessed: 24 III 2023].

Sigalos M., Goswami R., *Sam Bankman-Fried paid over $40 million to bribe at least one official in China, DOJ alleges in new indictment*, CNBC, 28 III 2023, https://www.cnbc.com/2023/03/28/sam-bankman-fried-paid-over-40-million-to-bribe-at-least-one-chinese-official-doj-alleges-in-new-indictment.html [accessed: 9 IV 2023].

Sutton S., Seligman L., *Two major crypto exchanges failed to block sanctioned Russians*, Politico, 24 II 2023, https://www.politico.com/news/2023/02/24/two-major-crypto-exchanges-failed-to-block-sanctioned-russians-00084391 [accessed: 10 IV 2023].

Terrorism and Digital Financing: How Technology is Changing the Threat. Hearing before the Subcommittee on Intelligence and Counterterrorism of the Committee On Homeland Security House of Representatives, https://www.congress.gov/117/chrg/CHRG-117hhrg45867/CHRG-117hhrg45867.pdf [accessed: 10 V 2023].

UK regulatory approach to cryptoassets and stablecoins: Consultation and call for evidence, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950206/HM_Treasury_Cryptoasset_and_Stablecoin_consultation.pdf [accessed: 9 IV 2023].

United States of America v. Samuel Bankman-Fried, https://storage.courtlistener.com/recap/gov.uscourts.nysd.590940/gov.uscourts.nysd.590940.80.0.pdf [accessed: 7 IV 2023].

United States of America v. Ali Shukri Amin, CRIMINAL NO. 1:15-CR-164, https://www.investigativeproject.org/documents/case_docs/2826.pdf [accessed: 10 V 2023].

Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing, FATF, https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html [accessed: 7 IV 2023].

White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets, The White House, 16 IX 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/ [accessed: 9 IV 2023].

Legal acts

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 EU L 156/43 of 19 June 2018).

COUNCIL REGULATION (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine (OJ EU L 229/1 of 31 July 2014).

Act of 30 March 2021 amending the Act on counteracting money laundering and terrorist financing and certain other acts (Journal of Laws 2021, item 815, as amended).

Act of 1 March 2018 on counteracting money laundering and terrorist financing (Journal of Laws 2023, item 1124, as amended).

Act of 19 November 2009 on gambling games (Journal of Laws 2023, item 227).

Act of 29 July 2005 on counteracting drug addiction (Journal of Laws 2023, item 172, of 2022, item 2600).

Act of 10 September 1999 Fiscal Penal Code (Journal of Laws 2023, item 654, as amended).

Act of 6 June 1997 Criminal Code (Journal of Laws 2022, item 1138, as amended).

Act of 23 April 1964 Civil Code (Journal of Laws 2022, item 1360, as amended).

Ensuring Responsible Development of Digital Assets, Executive Order 14067 of March 9, 2022, Federal Register. The Daily Journal of the United States Government, https://www.federalregister.gov/documents/2022/03/14/2022-05471/ensuring-responsible-development-of-digital-assets [accessed: 5 IV 2023].

Case law

Case file of the District Court in Przasnysz, 2nd Criminal Division, ref. no. II K 608/18.

Judgment of the District Court in Ostrołęka of 27 August 2020, ref. no. II Ka 40/20.

Judgment of the District Court for Kraków-Krowodrza, 2nd Criminal Division, of 3 August 2012, ref. no. II Ka 776/11/K.

Other documents

Markets in crypto-assets (MiCA), https://www.europarl.europa.eu [accessed: 9 IV 2023]. *Proposal for a regulation of the European Parliament and of the Council on markets in crypto-assets, and amending Directive (EU) 2019/1937*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593 [accessed: 9 IV 2023].

The views expressed in the article are the personal views of the authors and do not express the official position of the institution in which they are employed.

Paweł Opitek, PhD

Doctor of Law, Prosecutor of the District Prosecutor's Office in Kraków delegated to the National Prosecutor's Office.

Agnieszka Butor-Keler, PhD

Doctor in social sciences in the discipline of economics and finance, assistant professor in the Department of Management Accounting at the Warsaw School of Economics.

Karol Kanclerz

Legal trainee, chief specialist in the Legal Department of the Office of the Financial Supervision Authority.